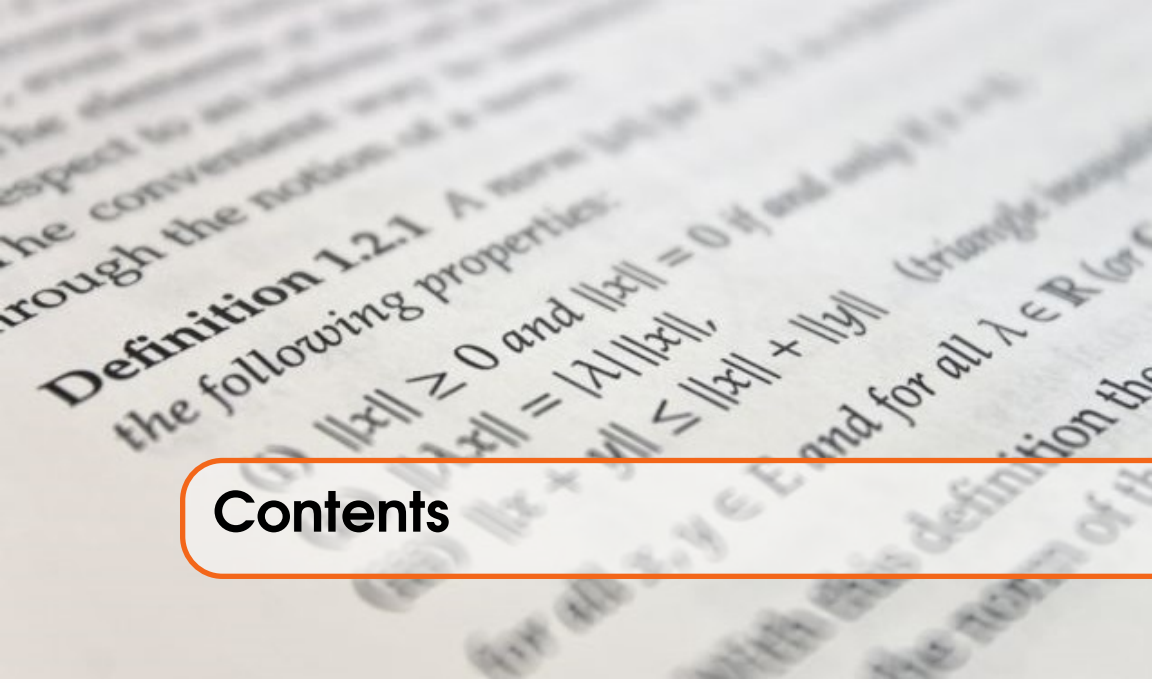
Linear Algebra

Jonathan Gleason

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Trigger warning: Row-reduction contained herein.



Contents

1 $\mathbb{K}$-modules and linear-transformations 1

1.1 Basic definitions 1

1.1.1 Morphism sets and bimodules 19

1.2 Basic concepts 25

1.2.1 Subspaces and quotient spaces 26

1.2.2 The (co)kernel and (co)image 31

1.3 Summary 33

2 Lin.-ind., span, bases, and dimension 34

2.1 Spanning and linear-independence 34

2.1.1 Linear-combinations and cofiniteness 34

2.1.2 Spanning 36

2.1.3 Linear-independence 37

2.2 Bases 44

2.2.1 Dimension 52

Rank of $\mathbb{K}$-modules 60

2.2.2 The Rank-Nullity Theorem 62

2.3 Summary 66

3 Coordinates, vectors, and matrices 67
3.1 Coordinates, vectors, and column vectors 67
3.2 Coordinates, lin.-trans., and matrices 72
3.2.1 Matrices 72
Row reduction 83
Matrix linear-transformations 95
3.2.2 Coordinates of linear-transformations 100
3.3 Summary 110

4 "Eigenstuff" 112
4.1 Motivation 112
4.2 Basic definitions 113
4.3 Diagonalization 127
4.3.1 Diagonalization of matrix linear-transformations . . 132
4.4 Jordan Canonical Form 135
4.4.1 Direct-sums 137
Coords. with respect to direct-sum decompositions . . . 147
The (external) direct-sum 159
4.4.2 Invariant subspaces 161
Indecomposability 167
4.4.3 Generalized "Eigenstuff" 170
A glimpse of generalized-eigenspaces 170
Nilpotent linear operators 173
More than a glimpse of generalized-eigenspaces 182
4.4.4 The Jordan Canonical Form Theorem 193
The theorem. Finally. 193
Jordan canonical form of matrix linear.-transformations 206
Similarity of linear operators 208
4.4.5 Summary 211
4.5 The minimal polynomial 211
4.6 The Jordan-Chevalley Decomposition 225
4.7 Summary 228
4.7.1 What now? 229

5 Multilinear algebra and tensors 230

5.1 Motivation 230
5.1.1 The derivative 230
5.1.2 Unification 231
5.1.3 Multilinear-transformations 231

5.2 Dual-pairs and dual-spaces 233
5.2.1 Dual-spaces 234
5.2.2 Dual-pairs 243
The definition and basic facts 243
The transpose 246
The orthogonal complement 249
The dual basis 255

5.3 The tensor product 257
5.3.1 The definition 257
5.3.2 Tensor products of linear-transformations 264
5.3.3 Basic properties 265
5.3.4 Natural-isomorphisms 268

5.4 Tensors and index notation 277
5.4.1 Tensors and the tensor algebra 277
5.4.2 Index notation 284
The definition 284
Constructions in index notation 287
5.4.3 Metrics 298
5.4.4 The physicists' definition 303
5.4.5 Summary 305

5.5 (Anti)symmetric tensors 305
5.5.1 The symmetric group 306
5.5.2 Basic definitions 308
5.5.3 The (anti)symmetric algebras 313

5.6 Extension of scalars 323
5.6.1 The definitions 324
5.6.2 The case of vector spaces 328

5.7 The determinant 331
5.7.1 The trace 331
5.7.2 The determinant 334
Properties of the determinant 337

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Determinants of matrices 342
The geometric interpretation of the determinant 356
The characteristic polynomial 359
5.8 Bilinear and quadratic forms 365
5.8.1 Basic definitions 366
5.8.2 Bilinear forms and matrices 368
5.8.3 Diagonalizable bilinear forms 370
5.8.4 Sylvester's Law of Inertia 376
5.9 Summary 377

6 Inner-product spaces 379
6.1 Motivation 379
6.2 Conjugate space 381
6.3 Basic definitions 385
6.3.1 Inner-products 385
6.3.2 The norm of an inner-product 391
Which norms come from inner-products? 394
6.4 Topological issues 398
6.4.1 Introduction 398
6.4.2 Conventions on sums 400
6.4.3 Hilbert spaces 404
"Sub-Hilbert spaces" 411
6.4.4 Miscellaneous 414
6.4.5 The justifications 415
6.5 Orthogonality 416
6.5.1 Basic definitions 416
6.5.2 Orthonormal bases 420
6.6 The projection onto a closed convex set 432
6.6.1 The result 432
6.6.2 The orthogonal complement decomposition 433
6.6.3 The adjoint 436
The Riesz Representation Theorem 437
The adjoint itself 442
6.6.4 Self-adjoint, nonnegative, unitary, and normal . . . 447
The function $\langle v|T(v)\rangle$ 457

6.6.5 Orthogonal-complements and projections 460
A return to orthogonal-complements 460
A return to projections 463
6.7 The Spectral Theorem 470
6.7.1 The theorem itself 470
6.7.2 Eigenvalues in inner-product spaces 474
6.8 Polar and singular value decompositions 479
6.8.1 The polar decomposition 479
6.8.2 The singular value decomposition 481
6.9 Summary 488

7 Applications 492

Appendices

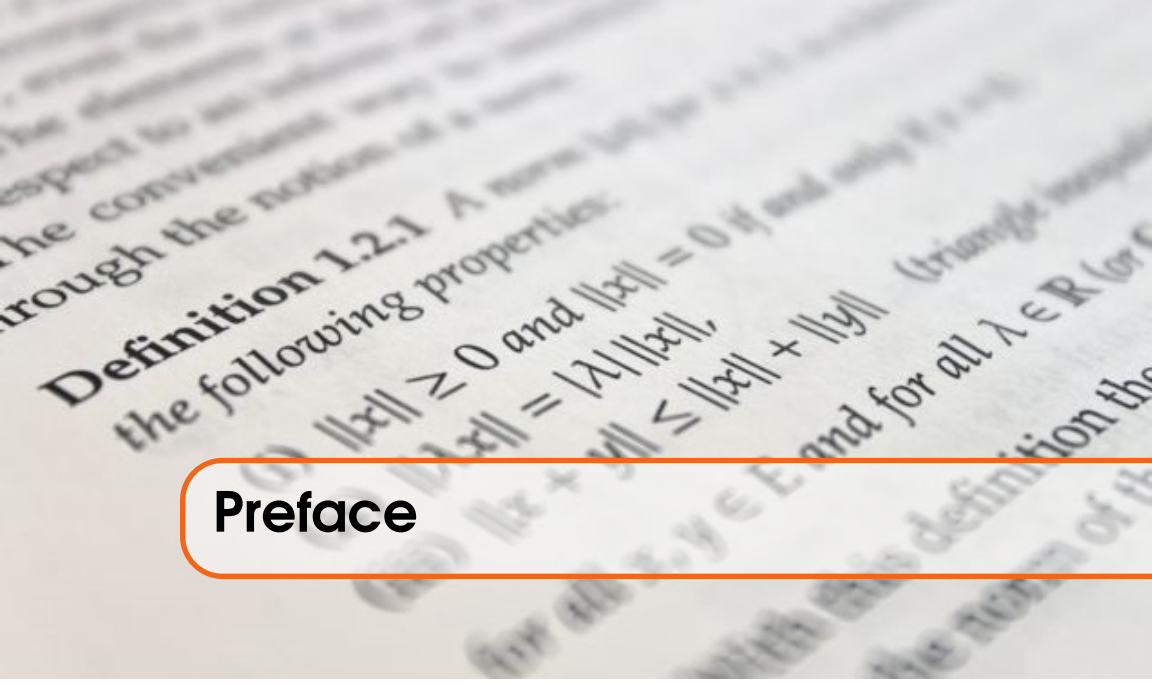
A Basic set theory 495
A.1 What is a set? 495
A.2 The absolute basics 498
A.2.1 Some comments on logical implication 498
A.2.2 A bit about proofs 501
Iff 502
The following are equivalent 503
For all. 503
The contrapositive and proof by contradiction 503
Without loss of generality. 506
If XYZ we are done, so suppose that ¬XYZ 506
Proving two sets are equal 507
Induction 507
A.2.3 Sets 510
A.3 Relations, functions, and orders 515
A.3.1 Arbitrary disjoint-unions and products 524
A.3.2 Equivalence relations 528
A.3.3 Preorders 533
A.3.4 Well-founded induction 537
A.3.5 Zorn's Lemma 538

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

A.4 Sets with algebraic structure 544
A.4.1 Quotient groups and quotient rngs 553
A.5 Cardinality, countability, and the naturals 559
A.5.1 Cardinality 560
A.5.2 The natural numbers 569
A.5.3 Countability 571

B Basic category theory 577
B.1 What is a category? 577
B.2 Some basic concepts 583
B.3 Functors and natural-transformations 589
B.3.1 Functors 589
B.3.2 Natural-transformations 594

C Results from ring theory 599
C.1 Prerequisites 599
C.2 Ideals and their quotients 604
C.2.1 Some properties of rings 605
C.2.2 Some properties of ideals 606
C.2.3 Their noncommutative variants 610
C.2.4 The dictionary 612
C.2.5 Summary 614
C.3 The integral closure 615
C.3.1 Associative algebras 617
C.3.2 Polynomials 622
Polynomials vs. polynomial functions 627
C.3.3 Algebraic and integral 631
C.3.4 Summary 645
C.4 Perfect fields 645
C.5 (Semi)simplicity 649



Preface

I started writing these notes in order to prepare to teach MATH 110 Linear Algebra at the University of California, Berkeley during Summer 2017. My obsessive-compulsive perfectionism and completionism turned them into what they are today.

At first, these notes were really just for me—I wanted to be sure I was ready to teach the class. As I'm sure you're aware if you've ever taught before, there is much more to being able to teach well than simply knowing all the material. For example, it is not enough to simply know Theorems 1 and 2. Among other things, for example, you have to know the order in which they come in the theory. Most of the motivation for starting these notes was to make sure I got all of that straight in my mind before I went up in front of a class.

A note to the reader

With the exception of specific examples,[1] the mathematics in these notes is developed "from the ground up". In particular, besides these exceptions, in principle, there are no prerequisites. That said, there is a modest amount of basic material that I cover sufficiently fast that it would be very helpful if you had at least passing familiarity

[1]For example, I need to assume that we know what the real numbers are to even talk about $\mathbb{R}^d$.

with. Essentially all of this 'prerequisite' material is given in the appendices.[2] I recommend you read these notes linearly, and refer to the appendices as needed when you come across concepts you are not familiar with. The notes are written in such a way that I would expect a student with no background to refer to the appendices *very often* in the beginning, but very little by the end.

Of all the statements which are true in these notes, they are roughly divided into two broad categories: the statements which are true by definition and the statements which are true because we can prove them. For the former, we have *definitions*; for the latter, we have *theorems*, *propositions*, *corollaries*, *lemmas*, and *claims*. We also have "meta" versions of (some of) these.

A definition is exactly what you think it is. A "meta-definition" is actually a whole collection of definitions—whenever you plug something in for XYZ, you get an actual definition. This explanation is probably not very lucid now, but I imagine it should be pretty obvious what I mean by this when you actually come to them. For the record, "meta-definition" is not a standard term (and I don't really think there is a standard term for this).[3] Similarly for "'meta-propositions", etc..

There is no hard and fast distinction between what I called theorems, propositions, corollaries, and lemmas. I tried to roughly adhere to the following conventions. If a result is used only in a proof of a single result and nowhere else, it is a *lemma*. If a result follows immediately or almost immediately from another result, it is a *corollary*. Results of particular significance are *theorems*. Everything else is a *proposition*. Claims, on the other hand, are distinct in that, not only only are they used in the proof of a single result like lemmas, but furthermore they wouldn't even make sense as stand-alone results (for example, if they use notation specific to the proof).

[2]Though there is also quite a bit of material there that I would not expect you to know.

[3]The closest I can think of is *axiom schema*, but "definition schema" sounds quite awkward to my ear.

In particular, note that the distinction between theorems and propositions has to do with the relative *significance*[4] of the *statement* of the result, and has nothing to to with the *difficulty* of the *proof*. Indeed, there are quite a few rather trivial results labeled as theorems simply because they are important.

There are also statements presented in blue boxes. The blue box is meant to draw attention to the fact contained therein, as it is particularly important for one reason or another. That said, the content in the blue box doesn't always contain the "full story", and is potentially a "watered-down" version of the truth. For example, we will very often omit stating what things are in the box itself and the reader will have to consult the surrounding context to gain the full meaning. This is by design—the boxes are supposed to highlight something important for convenience of the reader, not precise mathematics per se, and 'bogging it down' with details that are probably clear from context defeats the purpose of being quick and convenient.

I should mention that every now and then I give nonstandard names to results which would otherwise not have names. Part of the motivation for this is that I personally find this makes it easier to remember which result is which. For example, would you rather I refer to "Theorem 4.3.5" or the "Fundamental Theorem of Diagonalizability"? Just be warned that you shouldn't go up to other mathematicians, use these names, and expect them to know what you're talking about. (I will point it out when a name is nonstandard.)

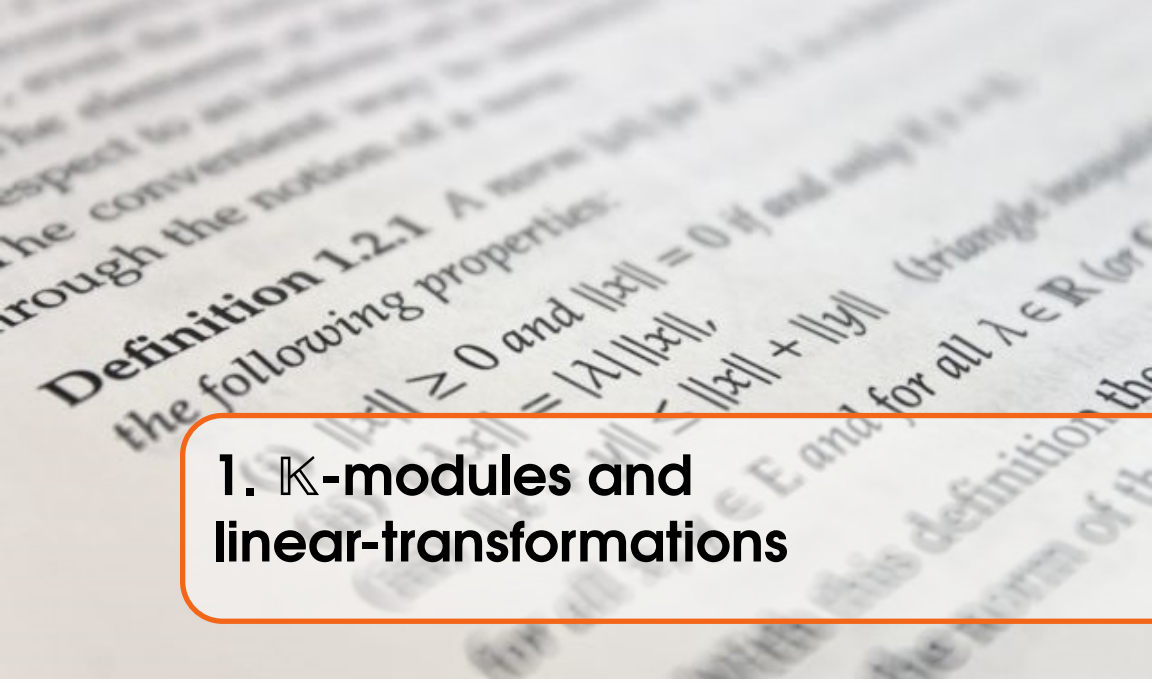
As an unimportant comment, I mention in case you're curious that I used double quotes when I am quoting something, usually a term or phrase either I or people in general use, and single quotes to indicate that the thing is quotes is not literally that thing. For example, mathematicians prove theorems and physicists prove 'theorems'.

Jonathan Gleason
Ph. D. Student, Department of Mathematics, University of California, Berkeley

[4]Obviously this is completely subjective and I would not expect any mathematician to pick out the exact same results which deserve the title of "theorem".

First draft (of preface): 18 June 2017
16 June 2017

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12



1. $\mathbb{K}$-modules and linear-transformations

1.1 Basic definitions

Linear algebra is the study of vector spaces.[1] A vector space is (i) a set, the elements of which are called *vectors*[2]; together with (ii) rules for adding and scaling the vectors.[3] This is the intuition anyways. In this way, the definition of vector spaces in general is an abstraction of the set of column vectors $\mathbb{R}^d$ that you know and love. As another example, the set of all continuous real-valued functions on $\mathbb{R}$ is a vector space, essentially because we can add and scale continuous functions (with the result being another continuous function).

To specify the scaling operation, however, we first need to say what the *scalars* are, that is, the thing by which we scale the vectors (in the two examples mentioned in the previous paragraph, the set of scalars it taken to be the real numbers $\mathbb{R}$). For vector spaces, the scalars are required to form what is called a *division ring*—see

[1] Or possibly *finite-dimensional* vector spaces if you prefer—it's not as if there is a strict definition of what the term "linear algebra" refers to.

[2] This is slightly unfortunate terminology, and I will elaborate on a possible confusion soon. In brief, one has to be careful not to confuse the term "vector" when used to describe elements of an 'abstract' vector space and the same term "vector" when used to describe column vectors in, e.g., $\mathbb{R}^d$.

[3] Subject to various axioms of course.

Definition A.4.23. That said, the axioms of a vector spaces makes just as much sense if you allow your division ring to be a more general (not necessarily division) *ring*—see Definition A.4.20. This is what is called a $\mathbb{K}$-*module*. As there is no reason to needlessly throw away this extra generality,[4] we present the definition in this form.

Definition 1.1.1 — $\mathbb{K}$-module Let $\mathbb{K}$ be a ring. Then, a ***$\mathbb{K}$-module*** is

(I). a commutative group $\langle V, +, 0, - \rangle$; together with
(II). a function $\cdot : \mathbb{K} \times V \to V$;

such that

(i). $(\alpha_1 \alpha_2) \cdot v = \alpha_1 \cdot (\alpha_2 \cdot v)$;
(ii). $1 \cdot v = v$;
(iii). $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v$; and
(iv). $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$;

for all $\alpha, \alpha_1, \alpha_2 \in R$ and $v, v_1, v_2 \in V$.

R $\mathbb{K}$ is called the ***ground ring***.

R In order to be less verbose, if every we say something like "Let V be a $\mathbb{K}$-module. . . ", it should be understood that $\mathbb{K}$ is a ring, even though we may not say so explicitly.

R Simply unraveling what it means for $\langle V, +, 0, - \rangle$ to be a commutative group, we see that this is equivalent to the following: V is a $\mathbb{K}$-module iff

(i). $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$;
(ii). $v_1 + v_2 = v_2 + v_1$;
(iii). $0 + v = v = v + 0$;
(iv). $v + (-v) = 0 = (-v) + v$;
(v). $(\alpha_1 \alpha_2) \cdot v = \alpha_1 \cdot (\alpha_2 \cdot v)$;
(vi). $1 \cdot v = v$;
(vii). $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v$; and
(viii). $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$

for all $\alpha, \alpha_1, \alpha_2 \in R$ and $v, v_1, v_2, v_3 \in V$.

[4] Except for perhaps, you know, pedagogy.

R See Theorem 1.1.6 for an equivalent slicker but less transparent definition. In general in mathematics, it is often the case that there are two (or more) ways to think of something—one is the conceptually concise, slick, but not very explicit way; and the other is not as elegant but easier to work with in practice. This definition is of the latter type and the statement in Theorem 1.1.6 of the former.

R In elementary linear algebra textbooks, this is often listed as eight (or more) axioms. This is quite a bit, and I think it is easy to remember them as follows: four of those axioms are simply equivalent to the statement that $\langle V, +, 0, - \rangle$ is a commutative group, two of them are distributive axioms, and the other two are natural "compatibility" axioms between the multiplication in $\mathbb{K}$ and $\cdot$.

R In fact, phrasing the definition in this way makes sense even more generally for rigs—see Theorem 1.1.6 for an explanation of why it is 'natural' to specialize to rings.

R This is sometimes referred to as a *left* $\mathbb{K}$-module because the "scalars" appear on the left. Of course, rewriting things a bit, it is easy enough to write down the definition of a *right* $\mathbb{K}$-module as well. There really isn't any serious difference between the two definitions, but one convention can be more convenient than the other in certain contexts.[a] Having a notion of both left and right modules is probably most useful when one wants to consider two different scalings on a set of vectors simultaneously—see Definition 1.1.1.5.

R It is more common to use "R" instead of "$\mathbb{K}$", in which case these would of course be called "R-modules". The reason we use "$\mathbb{K}$" instead of "R" is because we are primarily interested in vector spaces and "$\mathbb{K}$" is more suggestive that the ring we are working over is a division ring, or at the very least, commutative. That said, we will on occasion use "R" instead of "$\mathbb{K}$" when it feels more natural to do so.

[a] This is not unlike how it is sometimes convenient to write composition in ***postfix notation***: $f \cdot g := g \circ f$.

Our first order of business is to give another equivalent definition of a $\mathbb{K}$-module (Theorem 1.1.6). You should note, however, that while this is the most logical place to put this material, it's not of a particularly high priority, and so if this is your first time through the subject you should feel free to skip to the definition of a vector space (Definition 1.1.25). Before getting to this equivalent definition itself, however, we must prove some basic facts about $\mathbb{K}$-modules that follow immediately from the axioms (as well as Proposition 1.1.3).

Exercise 1.1.2 Let V be a $\mathbb{K}$-module.

(i). Show that $0 = 0 \cdot v$ for all $v \in V$.
(ii). Show that $-v = (-1) \cdot v$ for all $v \in V$.

Proposition 1.1.3 Let V be a commutative group. Then, $\langle \mathrm{End}_{\mathbf{Grp}}(V), +, 0, -, \circ, \mathrm{id}_V \rangle$ is a ring.

R Recall that (Definition B.2.2 and Example B.1.5) $\mathrm{End}_{\mathbf{Grp}}(V)$ is the set of all group homomorphisms (Definition A.4.11) from V to itself.

R $+$ is defined "pointwise", that is, $[\phi + \psi](v) := \phi(v) + \psi(v)$. Similarly, 0 here denotes the *function* that is 0 for all v.

Proof. $\langle \mathrm{End}_{\mathbf{Grp}}(V), +, 0, - \rangle$ is a commutative group because $\langle V, +, 0, - \rangle$ is (write out the verification of the axioms yourself if you don't believe me). $\langle \mathrm{End}_{\mathbf{Grp}}(V), \circ, \mathrm{id}_V \rangle$ is a monoid by Proposition B.2.11. From the definition of a ring Definition A.4.12, we see that it only remains to check that $\circ$

distributes over +, and so, we check.

$$\begin{aligned}
[\phi \circ (\psi + \chi)](v) &:= \phi([\psi + \chi](v)) \\
&:= \phi(\psi(v) + \chi(v)) \\
&= {}^{a}\phi(\psi(v)) = \phi(\chi(v)) \\
&=: [\phi \circ \psi](v) + [\phi \circ \chi](v) \\
&=: [\phi \circ \psi + \phi \circ \chi](v).
\end{aligned} \tag{1.1.4}$$

As this is true for all v, in fact, the functions themselves must be equal, that is $\phi \circ (\psi + \chi) = \phi \circ \psi + \phi \circ \chi$. Similarly,

$$\begin{aligned}
[(\psi + \chi) \circ \phi](v) &:= [\psi + \chi](\phi(v)) \\
&:= \psi(\phi(v)) + \chi(\phi(v)) \\
&=: [\psi \circ \phi](v) + [\chi \circ \phi](v) \\
&=: [\psi \circ \phi + \chi \circ \phi](v),
\end{aligned} \tag{1.1.5}$$

as desired. ■

[a] Because ϕ is a homomorphism.

Theorem 1.1.6. Let R be a ring.

(i). Let V be a commutative group and let $\rho\colon R \to \mathrm{End}_{\mathbf{Grp}}(V)$ be a ring homomorphism. Then, $\langle V, \cdot_\rho \rangle$ is an R-module, where $\cdot_\rho\colon R \times V \to V$ is defined by

$$\alpha \cdot_\rho v := \rho_\alpha(v).^{a} \tag{1.1.7}$$

(ii). Let $\langle V, \cdot \rangle$ be an R-module. Then, $\rho_\cdot\colon R \to \mathrm{End}_{\mathbf{Grp}}(V)$, defined by

$$[\rho_\cdot]_\alpha(v) := \alpha \cdot v, \tag{1.1.8}$$

is a ring homomorphism.

Furthermore, these two constructions are inverse to each other, that is, $\cdot_{\rho_\cdot} = \cdot$ and $\rho_{\cdot_\rho} = \rho$.

R This remark is more important than usual so pay attention. This result is the precise statement of the fact that we could have equivalently defined an R-module to be a pair $\langle V, \rho \rangle$, where V is a commutative group and $\rho\colon R \to \mathrm{End}_{\mathbf{Grp}}(V)$ is a ring homomorphism. This is hugely important as it says that, in language which you will eventually encounter (though not in these notes), *R-modules are 'the same' as "representations" of R.*[b]

R Note that $\mathrm{End}_{\mathbf{Grp}}(V)$ is in fact a ring by the previous result.

R Note that, by Proposition 1.1.3, $\mathrm{End}_{\mathbf{Grp}}(V)$ is a *ring*, not just a *rig*, and so it is natural to require that R likewise be a ring, not just a rig.

[a] We have writen $\rho_\alpha(v) \coloneqq [\rho(\alpha)](v)$, as I find this notation more transparent—for each α, you obtain a group homomorphism called $\rho_\alpha\colon V \to V$, and so $\rho_\alpha(v)$ is the value of that group homomorphism at $v \in M$. We use similar notation throughout.

[b] In fact, "ρ" is for *representation*.

Proof. (i) For the sake of brevity, we shall simply write $\cdot \coloneqq \cdot_\rho$. We must verify the four axioms in Definition 1.1.1. So, let $\alpha, \alpha_1, \alpha_2 \in R$ and $v, v_1, v_2 \in V$. Then,

$$\begin{aligned}(\alpha_1\alpha_2) \cdot v &\coloneqq \rho_{\alpha_1\alpha_2}(v) = {}^{a}[\rho_{\alpha_1} \circ \rho_{\alpha_2}](v) \\ &\coloneqq \rho_{\alpha_1}\left(\rho_{\alpha_2}(v)\right) \\ &\coloneqq \rho_{\alpha_1}(\alpha_2 \cdot v) \coloneqq \alpha_1 \cdot (\alpha_2 \cdot v).\end{aligned} \tag{1.1.9}$$

As $\rho_1 = \mathrm{id}_V$ (as it is a ring homomorphism, it must "preserve" the multiplicative identity), we have that $1 \cdot v \coloneqq \rho_1(v) = \mathrm{id}_V(v) = v$. As for the first distributive axiom, we have

$$\begin{aligned}(\alpha_1 + \alpha_2) \cdot v &\coloneqq \rho_{\alpha_1+\alpha_2}(v) = {}^{b}[\rho_{\alpha_1} + \rho_{\alpha_2}](v) \\ &\coloneqq \rho_{\alpha_1}(v) + \rho_{\alpha_2}(v) \\ &=: \alpha_1 \cdot v + \alpha_2 \cdot v.\end{aligned} \tag{1.1.10}$$

Finally, for the second distributive axiom, we have

$$\begin{aligned} \alpha \cdot (v_1 + v_2) &:= \rho_\alpha(v_1 + v_2) = {}^c\rho_\alpha(v_1) + \rho_\alpha(v_2) \\ &=: \alpha \cdot v_1 + \alpha \cdot v_2. \end{aligned} \tag{1.1.11}$$

(ii) For the sake of brevity, we shall simply write $\rho := \rho_\cdot$. First of all, note that each ρ_α is in fact a group homomorphism because $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$ for all $v_1, v_2 \in V$. We first check that ρ preserve addition.

$$\begin{aligned} \rho_{\alpha_1+\alpha_2}(v) &:= (\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v \\ &=: \rho_{\alpha_1}(v) + \rho_{\alpha_2}(v) =: [\rho_{\alpha_1} + \rho_{\alpha_2}](v), \end{aligned} \tag{1.1.12}$$

and so $\rho_{\alpha_1+\alpha_2} = \rho_{\alpha_1} + \rho_{\alpha_2}$. Similarly, ρ preserves the additive identity and additive inverses by Exercise 1.1.2. Likewise, ρ preserves multiplication as $(\alpha_1\alpha_2) \cdot v = \alpha_1 \cdot (\alpha_2 \cdot v)$. Finally, ρ preserves the multiplicative identity as $1 \cdot v = v$.

It remains to check that these constructions are inverse to each other. This is quite easy and is just a matter of unraveling the definitions.

$$\alpha \cdot_{\rho_\cdot} v := [\rho_\cdot]_\alpha(v) := \alpha \cdot v, \tag{1.1.13}$$

and so $\alpha_{\rho_\cdot} = \cdot$. Similarly,

$$[\rho_{\cdot_\rho}]_\alpha(v) := \alpha \cdot_\rho v := \rho_\alpha(v), \tag{1.1.14}$$

and hence $[\rho_{\cdot_\rho}]_\alpha = \rho_\alpha$ for all $\alpha \in R$, and hence $\rho_{\cdot_\rho} = \rho$. ■

[a] As ρ is a ring homomorphism, it "preserves" multiplication.
[b] As ρ is a ring homomrphism, it "preserves" addtion.
[c] Becasue ρ_α itself is a group homomorphism.

Now that we've seen two equivalent definitions of $\mathbb{K}$-module, it's time we present what is perhaps the most important example (at least for us) of $\mathbb{K}$-modules.

▪ **Example 1.1.15 — Column vectors** Let $\mathbb{K}$ be a ring and let $d \in \mathbb{N}$. Then, $\mathbb{K}^d$ is a $\mathbb{K}$-module with "componentwise" addition and scaling. Explicitly,

$$\langle v^1, \ldots, v^d \rangle + \langle w^1, \ldots, w^d \rangle := \langle v^1 + w^1, \ldots, v^d + w^d \rangle$$
$$\alpha \cdot \langle v^1, \ldots, v^d \rangle := \langle \alpha v^1, \ldots, \alpha v^d \rangle.$$

Elements of $\mathbb{K}^d$ are ***column vectors*** with entries or elements in $\mathbb{K}$.

R Note the superscripts here. v^k simply indicates the k^{th} component of the vector $v := \langle v^1, \ldots, v^d \rangle$. The reason we use the superscript instead of a subscript is because we will want to use subscripts to denote lists of *different vectors*. For example, we might have two vectors v_1 and v_2. Then, $[v_1]^2$ and $[v_2]^5$ would respectively denote 2^{nd} component of v_1 and 5^{th} component of v_2.

In practice, this doesn't cause any confusion with exponentiation, but just in case, we will try not to make use of exponents and simply indicate multiplication explicitly, for example, $\alpha \cdot \alpha$ instead of α^2.

Exercise 1.1.16 Check that $\mathbb{K}^d$ is indeed a $\mathbb{K}$-module.

R For what it's worth, the "d" is for *dimension*.

▪ **Example 1.1.17 — $\mathbb{K}$** Taking $d = 1$ in the previous example, we note that every ring can be viewed as a module over itself. This might seem trivial, and I suppose in some sense it is, but it's actually relatively important, if for no other reasons than it allows us to apply results and definitions we know about modules to rings. For example, you will learn at some point in your mathematical life that a ring is left(resp. right) *Noetherian* (by definition) iff is is Noetherian when regarded as a left (resp. right) module over itself.

▪ **Example 1.1.18 — $\mathbb{K}^\infty$** Let $\mathbb{K}$ be a ring and define

$$\mathbb{K}^\infty := \left\{ v \in \mathbb{K}^\mathbb{N} : m \mapsto v^m \text{ is eventually } 0. \right\} . \quad (1.1.19)$$

Note that $\mathbb{K}^\mathbb{N}$ is a countably-infinite Cartesian product of $\mathbb{K}$, that is,

$$\mathbb{K}^\mathbb{N} := \left\{ \langle v^0, v^1, v^2, \ldots \rangle : v^k \in \mathbb{K} \right\} . \quad (1.1.20)$$

To clarify, "$m \mapsto v^m$ is eventually 0" is equivalent to the statement that only finitely many v^ms are nonzero. So, for example,

$$\langle 1, 1, 1, \ldots \rangle \notin \mathbb{K}^\infty \quad (1.1.21)$$

(though it *is* an element of $\mathbb{K}^\mathbb{N}$).

$\mathbb{K}^\infty$ is a $\mathbb{K}$-module with componentwise addition and scaling (just as $\mathbb{K}^\mathbb{N}$ is).

▪ **Example 1.1.22 — Commutative groups are $\mathbb{Z}$-modules** Let $\langle V, +, 0, - \rangle$ be a commutative group, and for $n \in \mathbb{Z}$, define

$$n \cdot v := \operatorname{sgn}(n)(\underbrace{v + \cdots + v}_{|n|}). \quad (1.1.23)$$

Exercise 1.1.24 Check that indeed $\langle V, +, 0, -, \mathbb{Z}, \cdot \rangle$ is a $\mathbb{Z}$-module.

R In fact, every $\mathbb{Z}$-module also determines a commutative group, simply by "forgetting" about the scaling operation. These constructions, from commutative groups to $\mathbb{Z}$-modules and from $\mathbb{Z}$-modules to commutative groups, are inverse to one another. (The intuition is that the group structure determines the scaling operation by integers, and so adding the additional structure of a $\mathbb{Z}$-module gives nothing new.)

For this reason, one often does not distinguish between commutative groups and $\mathbb{Z}$-modules, and you may freely change how you think about things depending on what is most convenient to the objective at hand.

And finally, the definition of a vector space.

Definition 1.1.25 — Vector space A ***vector space*** over $\mathbb{F}$ is an $\mathbb{F}$-module where $\mathbb{F}$ is a division ring.

R Elements of $\mathbb{F}$ are called ***scalars***. Elements of V are called ***vectors***. $0 \in V$ is the ***origin***.[a]

I can't guarantee that I won't use the terms "scalar" and "vector" in the context of $\mathbb{K}$-modules, $\mathbb{K}$ not-necessarily-a-field, though this is not standard.

R If $\mathbb{F} = \mathbb{Q}$, V is a ***rational vector space***. If $\mathbb{F} = \mathbb{R}$, V is a ***real vector space***. If $\mathbb{F} = \mathbb{C}$, V is a ***complex vector space***. If $\mathbb{F} = \mathbb{H}$, V is a ***quaternionic vector space***.

R Often times people require that $\mathbb{F}$ be a field (that is, a commutative division ring) instead of just a division ring. While the vast majority of the concrete examples we will be interested are over fields and not division rings, most of the general theory works just as well for division rings.[b]

[a] Note that we abuse notation and use the same symbol for $0 \in \mathbb{F}$. I can't say I ever recall this causing any confusion.

[b] Contrast this with general R-modules where things really break down.

■ **Example 1.1.26 — $\mathbb{K}$-modules that are not vector spaces** Let $m, d \in \mathbb{N}$, take $\mathbb{K} := \mathbb{Z}/m\mathbb{Z}$, and define $V := (\mathbb{Z}/m\mathbb{Z})^d$ to be the set of d-component column vectors with entries in $\mathbb{Z}/m\mathbb{Z}$. As $\mathbb{Z}/m\mathbb{Z}$ is a field iff m is prime,

V constitute an example of a $\mathbb{K}$-module that is not a vector space if m is not prime.

These are important in that they are perhaps the simplest such examples, and so, if you think a certain property of vector spaces might fail more generally, you might consider checking the $(\mathbb{Z}/m\mathbb{Z})^d$s first.

▪ **Example 1.1.27 — Polynomials** Let $\mathbb{K}$ be a ring. Then, $\mathbb{K}[x]$ is the set of all polynomials with coefficients in $\mathbb{K}$ (Proposition C.3.2.1). Addition and scaling are just ordinary addition and scaling of polynomials.

For $m \in \mathbb{N}$, we shall write $\mathbb{K}[x]_m$ for the set of all polynomials in $\mathbb{K}[x]$ of degree *at most* m.

R Note that this notation is nonstandard—I am not aware of any universally accepted notation for this.

▪ **Example 1.1.28 — $C^\infty(O)$** Let $O \subseteq \mathbb{R}^d$ be open. Then, $C^\infty(O)$ is the set of smooth complex-valued functions on O.[a] $C^\infty(O)$ is then a vector space over $\mathbb{C}$.

[a] This means that the function has infinitely-many continuous derivatives.

▪ **Example 1.1.29 — An algebraic number field** Define $\mathbb{F} := \mathbb{Q}$ and $V := \mathbb{Q}(\sqrt{2})$.[a] Explicitly,

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \in \mathbb{C} : a, b \in \mathbb{Q} \right\}. \tag{1.1.30}$$

This is a two-dimensional vector space over $\mathbb{Q}$.

R In general, extensions of $\mathbb{Q}$ that are finite-dimensional over $\mathbb{Q}$ are known as *algebraic number fields*, and constitute the primary objects of interest in *algebraic number theory*.[b]

[a] Recall that (Proposition C.3.3.44) $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of the algebraic-closure of $\mathbb{Q}$ that contains $\sqrt{2}$.

[b] Recall that (Definition C.3.1.21) an *extension* of a ring $\mathbb{K}$ is an associative algebra over $\mathbb{K}$ in which $\mathbb{K}$ is a subset.

▪ **Example 1.1.31 — The same set of vectors over different fields** Define $V := \mathbb{C}^2$. Addition is done componentwise, as usual. Now take $\mathbb{F} := \mathbb{C}$, $\mathbb{F} := \mathbb{R}$, or $\mathbb{F} := \mathbb{Q}$. Either way, scaling $\mathbb{F} \times V \to V$ is done componentwise as usual, however, *these are all different scaling operations* because the *domains are different*. We thus have *three different vector spaces*. While we haven't defined dimension yet, hopefully your intuition suggests that V should be 2 dimensional over $\mathbb{C}$, 4 dimensional over $\mathbb{R}$, and infinite dimensional over $\mathbb{Q}$.

The point:

> *The same set of vectors over different division rings are considered to be different vector spaces.*

R Thus, we technically always need to specify the ring we are working over. However, most of the time, it will be clear from context, and we will not state this explicitly. For example, even for $V := \mathbb{C}^2$, it should be assumed that we are working over $\mathbb{C}$ unless otherwise stated.

I mentioned before that the term "vector" for elements in an "abstract" vector space can potentially be confusing for n00bs. The reason this is potentially confusing is because *the elements of V are not necessarily 'actual vectors'*. For example, the set of real-valued functions on a set can be made into a vector space, and certainly functions themselves are not traditionally thought of as "vectors". Thus, to avoid any possible confusion or ambiguity, I will be careful to make the following distinction.

Elements of a general vector space will simply be referred to as *vectors*. Elements of the specific vector space $\mathbb{R}^d$ will be referred to as *column vectors*.[a]

[a] More precisely, we will use this terminology when regarding $\mathbb{R}^d$ as an object in $\mathbf{Vect}_{\mathbb{R}}$, the category of vector spaces over $\mathbb{R}$—see Example 1.1.57.

Of fundamental importance in linear algebra is the relationship between the abstract and the concrete. Of course, the set of all column vectors (with a fixed number of components) forms a vector space, and matrices define linear-transformations. In the other direction, given a vector space V,[5] for every choice of a basis $\mathcal{B}$ of V, there is a unique isomorphism $V \to \mathbb{R}^d$ that satisfies such and such properties. Thus, having fixed a basis, one can associate *column vectors to vectors* and *matrices to linear-transformations*. I mention this now only to help solidify the distinction between vectors (in a general vector space) and column vectors (and also to foreshadow one of the more important results in elementary linear algebra)—you are not supposed to know what any of this precisely means just yet. In brief:

Vectors are to column vectors as linear-transformations are to matrices.

Having defined a type of mathematical object, we are now morally obligated to specify what the relevant notion of morphism is.

Definition 1.1.32 — Linear-transformation Let V and W be $\mathbb{K}$-modules, and let $T : V \to W$ be a function. Then, T is a ***$\mathbb{K}$-linear-transformation*** iff

(i). $T : V \to W$ is a group homomorphism; and
(ii). $T(\alpha \cdot v) = \alpha \cdot T(v)$ for all $\alpha \in \mathbb{K}$ and $v \in V$.

R Explicitly, (i) means that $T(v_1 + v_2) = T(v_1) + T(v_2)$ for all $v_1, v_2 \in V$.

[5] Over $\mathbb{R}$, for the moment.

R Informally, a function which satisfies (i) is said to *preserve addition*. Similarly, a function which satisfies (ii) is said to *preserve scaling* or *preserve scalar multiplication*.

R It's worth noting that there is an important result that allows one to easily define linear-transformations, though it will have to wait until we first discuss bases—see Theorem 2.2.25.

R If $\mathbb{K}$ is clear from context as it often is, we shall simply say ***linear-transformation***.

R A synonym for "linear-transformation" is ***module homomorphism***.

R Another synonym for "linear-transformation" is ***linear operator***, though this is probably more commonly used when the domain and codomain are the same, $T: V \to V$.[a]

[a] I use a dash in "linear-transformation" but not in "linear operator" because the term "transformation" by itself is meaningless in this context, whereas the term "operator" is used in related contexts in its own right (indeed, *nonlinear operators* are definitely a thing, whereas no one talks about "nonlinear transformations").

Notation 1.1.33 — Composition denoted by juxtaposition If S and T are composable linear-transformations, then we may sometimes write

$$ST := S \circ T \tag{1.1.34}$$

for clarity.

Exercise 1.1.35 — Sum and composition of linear maps is linear Let $\mathbb{K}$ be a ring.

(i). For $T_1, T_2 : V \to W$ linear maps of $\mathbb{K}$-modules, show that $T_1 + T_2$ is another linear map.
(ii). For $S : U \to V$ and $T : V \to W$ linear maps of $\mathbb{K}$-modules, show that $T \circ S$ is linear.
(iii). For $T : V \to W$ a linear map of $\mathbb{K}$-modules and $\alpha \in \mathbb{K}$, show that $\alpha \cdot T$ is linear *if* $\mathbb{K}$ *is commutative*.

R Warning: (iii) will *fail* if $\mathbb{K}$ is not commutative—see Example 3.2.1.37. We will return to fix this problem the best we can in Subsection 1.1.1.

R To clarify,

$$[T_1 + T_2](v) \coloneqq T_1(v) + T_2(v) \tag{1.1.36}$$

and

$$[\alpha \cdot T](v) \coloneqq \alpha \cdot T(v). \tag{1.1.37}$$

▪ **Example 1.1.38 — Identity** For any ring $\mathbb{K}$ and $\mathbb{K}$-module V, the identity function $\mathrm{id}_V : V \to V$ is a linear-transformation.

▪ **Example 1.1.39 — Zero** For any ring $\mathbb{K}$ and $\mathbb{K}$-modules V and W, the constant function $V \ni v \mapsto 0 \in W$ is a linear-transformation, the *zero linear-transformation*.

▪ **Example 1.1.40 — Scaling** Let $\mathbb{K}$ be a cring, let V be a $\mathbb{K}$-module, and let $\alpha \in \mathbb{K}$. Then, scaling by α, $V \ni v \mapsto \alpha \cdot v \in V$, is a linear-transformation.

Notation 1.1.41 In general (for any $\mathbb{K}$, not necessarily commutative) for $\alpha \in \mathbb{K}$, if the map $V \ni v \mapsto \alpha \cdot v \in V$ is linear, then we shall denote it by

$$\alpha := \alpha \, \mathrm{id}_V \, . \tag{1.1.42}$$

Thus, for example, we may write expressions like $T - \alpha$, T a linear-transformation—a priori this wouldn't make sense, but this should now be understood to be shorthand for the linear-transformation $T - \alpha \cdot \mathrm{id}$.

R In fact, the identity and zero linear-transformations are respectively the special cases in which $\alpha = 1$ and $\alpha = 0$.

R Warning: This makes use of commutativity! For example, take $\mathbb{K} := \mathbb{H}$ and $V := \mathbb{H}$. Then, scaling by $\mathrm{i} \in \mathbb{H}$ is not linear because it doesn't preserve scaling. Taking $\alpha := \mathrm{j} \in \mathbb{K}$ and $v := 1 \in V$, we see that

$$\mathrm{i} \cdot (\alpha \cdot v) := \mathrm{ij} = -\mathrm{ji} \neq \alpha \cdot (\mathrm{i} \cdot v). \tag{1.1.43}$$

Indeed, this is perhaps the most important pathology that occurs in the noncommutative case: scaling need no longer be linear!

▪ **Example 1.1.44 — Rotation** For any angle θ, rotation about the origin in $\mathbb{R}^2$ is a linear-transformation $\mathbb{R}^2 \to \mathbb{R}^2$.

▪ **Example 1.1.45 — Permutation** Let $\mathbb{K}$ be a ring, let $d \in \mathbb{N}$ and let $\sigma \colon \{1, \ldots, d\} \to \{1, \ldots, d\}$ be any bijection (though

of as a permutation of the indices). Then,

$$\mathbb{K}^d \ni \begin{bmatrix} v^1 \\ \vdots \\ v^d \end{bmatrix} \mapsto \begin{bmatrix} v^{\sigma(1)} \\ \vdots \\ v^{\sigma(d)} \end{bmatrix} \in \mathbb{K}^d. \tag{1.1.46}$$

is a linear-transformation.

To see an explicit example, consider the bijection $\sigma\colon \{1,2,3\} \to \{1,2,3\}$ defined by $\sigma(1) := 3$, $\sigma(2) := 1$, $\sigma(3) := 2$. Then, the corresponding linear-transformation is defined by

$$\begin{bmatrix} v^1 \\ v^2 \\ v^3 \end{bmatrix} \mapsto \begin{bmatrix} v^3 \\ v^1 \\ v^2 \end{bmatrix}. \tag{1.1.47}$$

▪ **Example 1.1.48 — Shift operators** Let $\mathbb{K}$ be a ring. Then, the ***left-shift operator*** $L\colon \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$ and ***right-shift operator*** $R\colon \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$ are defined respectively by

$$L\left(\langle v^0, v^1, v^2, \ldots\rangle\right) := \langle v^1, v^2, v^3, \ldots\rangle. \tag{1.1.49}$$

and

$$R\left(\langle v^0, v^1, v^2, \ldots\rangle\right) := \langle 0, v^0, v^1, \ldots\rangle \tag{1.1.50}$$

R There are similar variants of these shift operators on $\mathbb{K}^{\mathbb{Z}}$.

▪ **Example 1.1.51 — Differentiation** For any open subset $O \subseteq \mathbb{R}$, differentiation defines a linear-transformation $C^\infty(O) \to C^\infty(O)$, $f \mapsto f'$.

Similarly, for *any* ring $\mathbb{K}$, differentiation defines a linear-transformation $\mathbb{K}[x] \to \mathbb{K}[x]$.[a] Likewise, differentiation defines a different[b] linear-transformation $\mathbb{K}[x]_m \to \mathbb{K}[x]_m$ for any $m \in \mathbb{N}$.

In fact, we can be even fancier than this. More complex "differential operators", e.g. $\frac{\mathrm{d}^2}{\mathrm{d}x^2} + 1$, define linear-transformations in the obvious way (in this example, $C^\infty(\mathbb{R}) \ni f \mapsto f'' + f \in C^\infty(\mathbb{R})$).

[a] While the limit definition of differentiation won't make sense for arbitrary $\mathbb{K}$, the power rule still does, and so we can still "formally" differentiation polynomials with coefficients in any ring.

[b] It must be different because the domain and codomain are not the same!

▪ **Example 1.1.52 — Integration** Integration likewise defines a linear-transformation:

$$C^\infty(\mathbb{R}) \ni f \mapsto (x \mapsto \int_0^x \mathrm{d}t\, f(t)). \tag{1.1.53}$$

R To clarify, this linear-transformation sends the function f to the function whose value at x is $\int_0^x \mathrm{d}t\, f(t)$.

R Note that the "dt" on the left side of the integral, instead of the right side, is just a different convention—this expression means the same thing as $\int_0^x f(t)\,\mathrm{d}t$.

Similarly as before, "formal" integration defines a linear-transformation on polynomials.

▪ **Example 1.1.54** As in Example 1.1.29, take $\mathbb{F} := \mathbb{Q}$, and $V := \mathbb{Q}(\sqrt{2})$. Then, for any $a, b \in \mathbb{Q}$, $T : V \to V$ defined by

$$T(x) := (a + b\sqrt{2})x \tag{1.1.55}$$

is a linear-transformation.

With a working notion of morphism in hand, we obtain corresponding categories.

▪ **Example 1.1.56 — The category of $\mathbb{K}$-modules** Let $\mathbb{K}$ be a ring. Then, the category of $\mathbb{K}$-modules is the concrete category $\mathbb{K}$-**Mod**

(i). whose collection of objects $\mathrm{Obj}(\mathbb{K}\text{-}\mathbf{Mod})$ is the collection of all $\mathbb{K}$-modules; and
(ii). with morphism set $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$ precisely the set of all linear-transformations from V to W.

R Just as we have the category of left $\mathbb{K}$-modules $\mathbb{K}$-**Mod**, we also have the category of right $\mathbb{K}$-modules **Mod**-$\mathbb{K}$ defined similarly.

▪ **Example 1.1.57 — The category of vector spaces** Let $\mathbb{F}$ be a division ring. Then, the category of vector spaces over $\mathbb{F}$ is the category $\mathbf{Vect}_{\mathbb{F}} := \mathbb{F}\text{-}\mathbf{Mod}$.

R If $\mathbb{F}$ is clear from context or not relevant, we may only write $\mathbf{Vect} := \mathbf{Vect}_{\mathbb{F}}$.

1.1.1 Morphism sets and bimodules

In fact, we would like the morphism sets $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$ themselves to furnish examples of $\mathbb{K}$-modules. Unfortunately, if $\mathbb{K}$ is not commutative, we can't quite do this. To see this, we would need to be able to define a notion of scaling of linear-transformations, and essentially the only thing one could write down is

$$[\alpha \cdot T](v) := \alpha \cdot T(v). \tag{1.1.1.1}$$

Unfortunately, however, this is not linear in general:

$$\begin{aligned}[\alpha \cdot T](\beta \cdot v) &:= \alpha \cdot T(\beta \cdot v) = \alpha\beta \cdot T(v) \neq \beta \cdot (\alpha \cdot T(v)) \\ &=: \beta \cdot [\alpha \cdot T](v).\end{aligned} \tag{1.1.1.2}$$

In order for what we have written as an inequality to be an equality, we would need to know that $\mathbb{K}$ is commutative.[6] There is a silly way to fix this, however—instead, let us try scaling T *on the right*:

$$[T \cdot \alpha](\beta \cdot v) \coloneqq T(\beta \cdot v) \cdot \alpha = \beta \cdot T(v) \cdot \alpha = \beta \cdot [T \cdot \alpha](v), \quad (1.1.1.3)$$

and so $T \cdot \alpha$ is again $\mathbb{K}$-linear (on the left).[7]

This situation is one in mathematics where it is easier to keep things straight in the most general situation, even though one (or at least us) will never actually need that amount of generality. Specifically, we are going to now consider sets of vectors equipped with *two* scaling operations, one on the left and one on the right.

R The material on bimodules is of relatively low priority, and so if you find it confusing the first time through, you needn't worry. What you *should* remember, however, is that when $\mathbb{K}$ is *commutative*, $\mathrm{End}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$ is another $\mathbb{K}$-module with the "obvious" definitions of addition and scaling

$$[T_1 + T_2](v) \coloneqq T_1(v) + T_2(v) \quad (1.1.1.4a)$$
$$[\alpha \cdot T](v) \coloneqq \alpha \cdot T(v). \quad (1.1.1.4b)$$

It is only for $\mathbb{K}$ noncommutative that one must go to the trouble of worrying about bimodules.

Definition 1.1.1.5 — $\mathbb{K}$-$\mathbb{L}$-bimodule Let $\mathbb{K}$ and $\mathbb{L}$ be rings. Then, a $\mathbb{K}$-$\mathbb{L}$-***bimodule*** is

(I). a left $\mathbb{K}$-module $\langle V, +, 0, -, \mathbb{K}, \cdot \rangle$; and
(II). a right $\mathbb{L}$-module $\langle V, +, 0, -, \mathbb{L}, \cdot \rangle^a$

such that

$$(\alpha \cdot v) \cdot \zeta = \alpha \cdot (v \cdot \zeta) \quad (1.1.1.6)$$

for all $v \in V$, $\alpha \in \mathbb{K}$, and $\zeta \in \mathbb{K}$.

R Similarly as we may view commutative groups as $\mathbb{Z}$-modules (Example 1.1.22), we may view any left

[6] See Example 3.2.1.37 for a concrete counter-example.

[7] Note that the scaling in W has to be written on the right in order for this to make sense.

$\mathbb{K}$-module as a $\mathbb{K}$-$\mathbb{Z}$ bimodule, and likewise, we may view any right $\mathbb{L}$-module as a $\mathbb{Z}$-$\mathbb{L}$ bimodule.

[a] Of course, the two scaling operations here are not the same, even those we abuse notation and simply write "$\cdot$" for both.

The following example of a bimodule is one of the most important, and it would likely help your intuition to keep in in the make of your mind in a similar way you might think of $\mathbb{K}^d$ even when doing "abstract" linear algebra.

▪ **Example 1.1.1.7 — The $\mathbb{K}$-$\mathrm{End}_{\mathbb{K}\text{-}\mathbf{Mod}}(V)$ bimodule** V et V be a left $\mathbb{K}$-module. For $T\colon V \to V$ a $\mathbb{K}$-linear-transformation, let us define

$$v \cdot T := T(v). \tag{1.1.1.8}$$

Exercise 1.1.1.9 Check that this does indeed make V into a right $\mathrm{End}_{\mathbb{K}\text{-}\mathbf{Mod}}(V)$ module.

As for the bimodule property, we simply check

$$\alpha \cdot (v \cdot T) := \alpha \cdot T(v) = T(\alpha \cdot v) =: (\alpha \cdot v) \cdot T. \tag{1.1.1.10}$$

Another important fact to note is that every ring can be thought of as a bimodule over itself.

▪ **Example 1.1.1.11 — The R-R-bimodule** R Let R be a ring. Writing $V := R$ to keep conceptually straight which Rs are being thought of as rings and which ones are being thought of as bimodules, the left scaling $R \times V \to V$ is defined by $\langle r, v\rangle \mapsto r \cdot v$ and the right scaling $V \times R \to V$ is defined by $\langle v, r\rangle \mapsto v \cdot r$. That is, left (right) scaling is just given by multiplication on the left (right).

We mentioned before briefly that one needn't introduce the complication of bimodules if the ground ring is commutative. One can see this from the following example.

▪ **Example 1.1.1.12 — 𝕂-modules over crings** Let $\mathbb{K}$ be a cring and let V be a $\mathbb{K}$-module. Then in fact we can view V as a $\mathbb{K}$-$\mathbb{K}$-bimodule by defining

$$v \cdot \alpha \coloneqq \alpha \cdot v. \tag{1.1.1.13}$$

Exercise 1.1.1.14 Check that this does indeed make V into a $\mathbb{K}$-$\mathbb{K}$-bimodule.

R Note how this requires commutativity.

Thus, if $\mathbb{K}$ is commutative, left $\mathbb{K}$-modules are 'the same as' $\mathbb{K}$-$\mathbb{K}$-bimodules are 'the same as' right $\mathbb{K}$-modules, and so in this case, there is no need to really distinguish.

We motivated the introduction of bimodules because we wanted to turn morphism sets themselves into modules. Now that we have bimodules, however, we are again morally obligated to introduce the new relevant of morphism.

Definition 1.1.1.15 — Linear-transformation (of bimodules) Let $\mathbb{K}$ and $\mathbb{L}$ be rings, let V and W be $\mathbb{K}$-$\mathbb{L}$ bimodules, and let $T\colon V \to W$ be a function. Then, T is a $\mathbb{K}$-$\mathbb{L}$-***linear-transformation*** iff

(i). T is a $\mathbb{K}$-linear-transformation; and
(ii). T is an $\mathbb{L}$-linear-transformation.

R Explicitly, this means that (i) $T(v_1 + v_2) = T(v_1) + T(v_2)$, (ii) $T(\alpha \cdot v) = \alpha \cdot T(v)$, and (iii) $T(v \cdot \zeta) = T(v) \cdot \zeta$.

R If $\mathbb{K}$ and $\mathbb{L}$ are clear from context, we shall simply say ***Linear-transformation***.

R If T only satisfies (i), then we may say that T is ***left linear*** or ***linear on the left***. Likewise, if T only satisfies (ii), we may say that T is ***right linear*** or ***linear on the right***. In this context, we may say that T is ***two-sided linear*** if T satisfies both (i) and (ii) for emphasis to distinguish between just "left-linear" and "right-linear".

R A synonym for "linear-transformation of bimodules" is ***bimodule-homomorphism***.

R Warning: Don't use the term "bilinear-transformation" for this. That means something else—see Definition 5.1.3.1.

Again, having defined a new type of object as well as the relevant notion of morphism, we obtain a corresponding category.

▪ **Example 1.1.1.16 — The category of $\mathbb{K}$-$\mathbb{L}$-bimodules** Let $\mathbb{K}$ and $\mathbb{L}$ be rings. Then, the category of $\mathbb{K}$-$\mathbb{L}$-bimodules is the concrete category $\mathbb{K}$-**Mod**-$\mathbb{L}$

(i). whose collection of objects $\mathrm{Obj}(\mathbb{K}\text{-}\mathbf{Mod}\text{-}\mathbb{L})$ is the collection of all $\mathbb{K}$-$\mathbb{L}$-bimodules; and

(ii). with morphism set $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}\text{-}\mathbb{L}}(V, W)$ precisely the set of all linear-transformations from V to W.

We now turn to the issue of equipping morphism sets of *bimodules* with another bimodule structure. As we can view any $\mathbb{K}$-module V as a $\mathbb{K}$-$\mathbb{Z}$-bimodule, this will allow us to equip $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$ with the structure of a bimodule. We will find, however, that the bimodule structure on $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$ is not just that of a left $\mathbb{K}$-module—if it were that simple, we wouldn't have needed to take this excursion on bimodules in the first place.

▪ **Example 1.1.1.17 — $\mathrm{Mor}_{R\text{-}\mathbf{Mod}}(V,W)$ is an S-T-bimodule** Let R, S, and T be rings, and let V be an R-S-bimodule and let W be an R-T-bimodule. Then, as V and W are both left R-modules, and so while we cannot speak of linear-transformations, we can speak of left linear-transformations. In fact, $\mathrm{Mor}_{R\text{-}\mathbf{Mod}}(V,W)$ can be given the structure of an S-T-bimodule:[a]

$$[s \cdot T \cdot t](v) \coloneqq T(v \cdot s) \cdot t. \tag{1.1.1.18}$$

Exercise 1.1.1.19 Check that $s \cdot T \cdot t$ is still left linear.

Exercise 1.1.1.20 Check that $\mathrm{Mor}_{R\text{-}\mathbf{Mod}}(V,W)$ is an S-T-bimodule.

[a] Addition is defined pointwise. We don't mention this explicitly because addition is always pointwise and the sum of two linear-transformations is always again linear.

▪ **Example 1.1.1.21 — $\mathrm{Mor}_{\mathbf{Mod}\text{-}S}(V,W)$ is a T-R-bimodule** Let R, S, and T be rings, let V be an R-S-bimodule and let W be a T-S-bimodule.[a] Thus, in this case, we can speak of the *right* linear-transformations. In fact, $\mathrm{Mor}_{\mathbf{Mod}\text{-}S}(V,W)$ can be given the structure of a T-R-bimodule:

$$[t \cdot T \cdot r](v) \coloneqq t \cdot T(r \cdot v). \tag{1.1.1.22}$$

Exercise 1.1.1.23 Check that $t \cdot T \cdot t$ is still right linear.

Exercise 1.1.1.24 Check that $\mathrm{Mor}_{\mathbf{Mod}\text{-}S}(V,W)$ is an T-R-bimodule.

[a]Note that V is still an R-S-bimodule as in the previous example, but now W is a T-S-bimodule (before it was an R-T-bimodule).

While this might seem complicated, there is actually a relatively simple mnemonic to keep this straight. You can remember these respectively as

$$(R\text{-}S)^{\mathrm{co}} \times (R\text{-}T) \mapsto S\text{-}T \tag{1.1.1.25}$$

and

$$(R\text{-}S)^{\mathrm{co}} \times (T\text{-}S) \mapsto T\text{-}R. \tag{1.1.1.26}$$

(The common Rs and Ss 'annihilate' each other, similar to the mnemonic for the dimensions for multiplication of matrices.) That is, the morphism set[8] from a R-S-bimodule to a R-T-bimodule is and S-T-bimodule, and the morphism set from a R-S-bimodule to a T-S-bimodule is a T-R-bimodule.

Finally, let us return to the important special case where the ring we are working over is commutative. So, let $\mathbb{K}$ be a cring, and let V and W be $\mathbb{K}$-modules. On account of Example 1.1.1.12, we can view both of these as $\mathbb{K}$-$\mathbb{K}$-bimodules, and so according to the general case we just discussed, both $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V,W)$ and $\mathrm{Mor}_{\mathbf{Mod}\text{-}\mathbb{K}}(V,W)$ have the structure of $\mathbb{K}$-$\mathbb{K}$-bimodules. Again, by Example 1.1.1.12, we don't think of these as bimodules, but just simply $\mathbb{K}$-modules. Anyways, the TL;DR version is: if $\mathbb{K}$ is commutative, then $\mathrm{Mor}_{\mathbb{K}}(V,W)$ is a $\mathbb{K}$-module with addition and scaling defined by

$$[T_1 + T_2](v) \coloneqq T_1(v) + T_2(v) \tag{1.1.1.27a}$$

$$[\alpha \cdot T](v) \coloneqq \alpha \cdot T(v). \tag{1.1.1.27b}$$

1.2 Basic concepts

In the previous section, we gave two equivalent definitions of $\mathbb{K}$-modules, and likewise gave the definition of a linear-transformation. We now turn to the basic theory $\mathbb{K}$-modules and linear-transformations.

[8]Note how it only makes sense to speak of the left linear transformations, and so I there is no ambiguity as to what morphism set I could possibly be referring to.

1.2.1 Subspaces and quotient spaces

If you've studied linear algebra before, you're almost certainly familiar with the concept of a *subspace*. Intuitively, you should think of subspaces of a vector space as lines, planes, etc. that contain the origin.

Definition 1.2.1.1 — Subspace Let $\langle V, \cdot \rangle$ be an $\mathbb{K}$-module. Then, a ***subspace*** of V is a subset $W \subseteq V$ such that $\langle W, \cdot \rangle$ is an $\mathbb{K}$-module.

R That is, a subspace is a subset that is also a $\mathbb{K}$-module (with respect to the same scaling operation).

R Warning: It is incredibly uncommon to use the term "subspace" in the context of more general R-modules, in which case the term ***submodule*** is usually used instead. Because the focus is on vector spaces, I will be using the terminology that is standard in that context, even when I'm not working over a division ring. This applies throughout, though I will try to mention when there is terminology that is more common in the context of R-modules.

A priori, to show that $\langle W, \cdot \rangle$ is a subspace, there are quite a few axioms one would have to check. Fortunately, in practice, it is relatively easy to check whether or not something is a subspace.

Proposition 1.2.1.2 Let V be a $\mathbb{K}$-module and let $W \subseteq V$. Then, W is a subspace iff

(i). $0 \in W$;
(ii). $v_1, v_2 \in W$ implies $v_1 + v_2 \in W$; and
(iii). $v \in W$ implies $\alpha \cdot v \in W$ for all $\alpha \in \mathbb{K}$.

R The first condition here is just to excluded the stupid case of the empty-set. Thus, in other words, a nonempty subset of V is a subspace iff it is closed under addition and scaling.

Proof. We leave this as an exercise.

Exercise 1.2.1.3 Prove this yourself.

■

▪ **Example 1.2.1.4 — 0 and V** Every $\mathbb{K}$-module V has two subspace:[a] 0 and V. Note that we are writing

$$0 := \{0\}, \tag{1.2.1.5}$$

that is, we abuse notation and write 0 for the subspace whose only element is the 0 vector.

I won't even bother making it an exercise, but you should quickly convince yourself that these are in fact subspaces.

[a] Well, they might coincide in the trivial case $V = 0$.

▪ **Example 1.2.1.6 — Polynomials and smooth functions** $\mathbb{R}[x]$ is[a] a subspace of $C^\infty(\mathbb{R})$, which in turn is a subspace of $\mathrm{Mor}_{\mathbf{Set}}(\mathbb{R}, \mathbb{R})$.[b]

[a] Technically, I should say "embeds as". The reason for this technicality is because polynomials are not quite the same as polynomial functions—see Equation (C.3.2.12). In any case, this is not a huge deal, and if it confuses you, you should ignore this technicality.

[b] See Appendix B for an explanation, but "$\mathrm{Mor}_{\mathbf{Set}}(X, Y)$" is just fancy notation for the set of all functions from X to Y.

Exercise 1.2.1.7 — $\mathbb{K}^\infty$ Let $\mathbb{K}$ be a ring. Show that $\mathbb{K}^\infty$ is a subspace of $\mathbb{K}^{\mathbb{N}}$.

R See Example 1.1.18 to recall the definition of $\mathbb{K}^\infty$ (and $\mathbb{K}^{\mathbb{N}}$).

Exercise 1.2.1.8 — $\mathbb{K}[x]_m$ Let $\mathbb{K}$ be a ring and let $m \in \mathbb{N}$.

(i). Show that $\mathbb{K}[x]_m$ is a subspace of $\mathbb{K}[x]$.

(ii). Explain why the set of all polynomials of degree exactly equal to m, together with the 0 polynomial, do not necessarily form a subspace of $\mathbb{K}[x]$.

R Recall that $\mathbb{K}[x]$ is the vector space of all polynomials with coefficients in $\mathbb{K}$, and $\mathbb{K}[x]_m$ is the subset of polynomials with degree at most m—see Example 1.1.27.

'Dual' to the concept of subspace is that of *quotient space*, something you likely did not encounter in a first course on linear algebra. We won't have much use for this concept, but it feels wrong to talk about subspaces with no mention of quotient spaces. That said, I recommend you skip this topic unless you know you need to know it.

Quotient objects are actually relatively difficult the first time one encounters them. However, the intuition is essentially always the same—whether for quotient groups, quotient rings, quotient spaces, etc.—and we have already discussed this intuition before Proposition A.4.1.1, and so don't repeat this intuition here. Finally, I want to add that the ratio of difficulty to usefulness (for us) regarding the material on quotient spaces here is pretty large, and so I might even go so far as to recommend you skip the quotient stuff—it's really here for the sake of completeness, not pedagogy.[9]

Proposition 1.2.1.9 — Cosets (in $\mathbb{K}$-modules) Let V be a $\mathbb{K}$-module, let $W \subseteq V$, and define

$$v_1 \cong v_2 \,(\mathrm{mod}\, W) \text{ iff } -v_2+v_1 \in N \text{ for } v_1, v_2 \in V. \quad (1.2.1.10)$$

Then, $\cong \,(\mathrm{mod} W)$ is an equivalence relation iff $\langle W, +, 0, - \rangle$ is a subgroup of $\langle V, +, 0, - \rangle$.

[9] In fact, I would not expect anyone to be able to fully understand this material from what little I have written about it, but that's okay, because that's not why it's here.

Furthermore, in the case this is an equivalence relation,

$$[v]_{\cong \,(\mathrm{mod}\, W)} = v + W. \tag{1.2.1.11}$$

R To clarify, $[v]_{\cong\,(\mathrm{mod}\,W)}$ is the equivalence class of v with respect to $\cong \pmod{W}$ and $v + W := \{v + w : w \in W\}$.

R The equivalence class of v with respect $\cong \pmod{W}$ is the ***left W-coset***. The set of all left W-cosets is denoted by $V/W := V/{\sim_{\cong\,(\mathrm{mod}\,W)}} = \{v + W : v \in M\}$.

R By changing the definition of the equivalent relation to "... iff $v_1 - v_2 \in W$", then we obtain the corresponding definition of ***right W-cosets***, given explicitly by $W + v$. In this case, however, the binary operation in question $(+)$ is commutative, and so $v + W = W + v$, that is, the left and right cosets coincide, and so we can simply say ***coset***. In particular, there is no need to talk about the set of right W-cosets, which would have been denoted $W\backslash V$.

R Note how this result itself says nothing about the action of $\mathbb{K}$. The action of $\mathbb{K}$ itself will definitely play a role in the next definition, however, when we attempt to make the set of cosets V/W itself into an $\mathbb{K}$-module.

Definition 1.2.1.12 — Quotient space Let $\langle V, \cdot \rangle$ be a $\mathbb{K}$-module, let $W \subseteq \langle V, 0, +, - \rangle$ be a subgroup, and let $v, v_1, v_2 \in V$ and $\alpha \in \mathbb{K}$. Define

$$(v_1 + W) + (v_2 + W) := (v_1 + v_2) + W \tag{1.2.1.13}$$

and

$$\alpha \cdot (v + W) := \alpha \cdot v + W. \tag{1.2.1.14}$$

W is an ***ideal*** iff both of these operations are well-defined. In this case, V/W is the ***quotient space*** of V modulo W.

R The term "ideal" is never used in this context. This is because, by the the following result, this condition is equivalent to being a subspace, and so people use only term the "subspace".

R By now, as we've seen the concepts of subobject and quotient object of algebraic structures pop up on several occasions, you might be wondering whether one can develop theory that would generalize and be capable of tackling all these cases at once (so that we don't have to separately define "quotient group", "quotient rng", "quotient space", etc.). Of course the answer is "Yes, there is such a generalization.", and this generalization is known as *general algebra* or *universal algebra*. As this is an introductory linear algebra text, it would be insane to develop any of this theory at all. Indeed, all of the algebra we're doing is being done for tangential reasons as it is.

R For us, one of the most important properties of the quotient space is that

$$\dim(V/W) = \dim(V) - \dim(W), \quad (1.2.1.15)$$

at least when V is a finite-dimensional vector space. Of course, we don't know what dimension is yet, but for now you can just take note of the fact is that this is one reason in the future we might care. For example, the Rank-Nullity Theorem (Theorem 2.2.2.2) can be understood to follow from this fact.

Exercise 1.2.1.16 Let V be a $\mathbb{K}$-module, and let $W \subseteq V$ be a subset. Show that W is an ideal iff it is a subspace.

R Hereafter, we shall adhere to the standard convention and only use the term "subspace" in this context.

1.2.2 The (co)kernel and (co)image

A fact with which you are likely familiar is that, to each linear-transformation, are associated two subspaces, a subspace of the domain and a subspace of the codomain. A fact with which you are unlikely familiar is that there are likewise two *quotient* modules associated to each linear-transformation as well. One of the subspaces is just the image, something you (hopefully) are already quite comfortable with. The other three, however, we should probably define. Note again that the concepts of coimage and cokernel can likely safely be skipped for the time being.

Definition 1.2.2.1 — Kernel (of a linear-transformation) Let $T: V \to W$ be a linear-transformation. Then, the ***kernel*** of T, $\mathrm{Ker}(T)$, is defined by

$$\mathrm{Ker}(T) := \{v \in V : T(v) = 0\}\,. \tag{1.2.2.2}$$

R If the term "kernel" is unfamiliar to you, perhaps the term ***null-space*** is. While I prefer to try to reserve the term "null-space" for matrices and "kernel" for linear-transformations, they are essentially the same thing. Similarly, the term is essentially the same as the image of a linear-transformation, though, again, this terminology is more appropriate in the context of matrices. When I do use this terminology, however, I shall write $\mathrm{Null}(A)$ for the null-space and $\mathrm{Col}(A)$ for the column-space.

R Note the *capital* "K" in "Ker". I don't promise you that everyone will be strict about this, but it is common to use a capital letter to refer to the kernel as an object (set) and to use a lowercase letter to refer to the corresponding map $\mathrm{Ker}(T) \xrightarrow{\ker(T)} M$. In this context, this distinction is a pedantic one, but it's a distinction that will matter as you progress in your studies.

Proposition 1.2.2.3 Let $T\colon V \to W$ be a linear-transformation. Then,

(i). $\mathrm{Ker}(T) \subseteq V$ is a subspace; and
(ii). $\mathrm{Im}(T) \subseteq W$ is a subspace.

Proof. We leave this as an exercise.

Exercise 1.2.2.4 Prove this yourself.

■

We now turn to the two quotient spaces.

Definition 1.2.2.5 — Coimage Let $T\colon V \to W$ be a linear-transformation. Then, the ***coimage*** of T, $\mathrm{Coim}(T)$ is defined by

$$\mathrm{Coim}(T) \coloneqq V/\mathrm{Ker}(T). \tag{1.2.2.6}$$

Definition 1.2.2.7 — Cokernel Let $T\colon V \to W$ be a linear-transformation. Then, the ***cokernel*** of T, $\mathrm{Coker}(T)$ is defined by

$$\mathrm{Coker}(T) \coloneqq W/\mathrm{Im}(T). \tag{1.2.2.8}$$

Thus, to each linear-transformation is associated a subspace of the domain and a subspace of the codomain (the kernel and image respectively). Quotienting by these respective subspaces gives you a quotient of the domain and a quotient of the codomain (the coimage and cokernel respectively).

One application of these concepts is that they give us alternative methods to test for injectivity and surjectivity, though we wait to state the results until we can speak of *dimension*—see Propositions 2.2.1.25 and 2.2.1.27.

1.3 Summary

So far, we've covered 32 pages worth of material, but not all of it is equally important. For example, things like the coimage and bimodules can safely be ignored on a first reading. We recall here things covered in the chapter that you really must absolutely know.

(i). The definition of $\mathbb{K}$-*modules* (Definition 1.1.1) and *vector spaces* (Definition 1.1.25).
(ii). The definition of *linear-transformations* (Definition 1.1.32).
(iii). The definition of *subspaces* (Definition 1.2.1.1) and the criterion to test whether a subset is in fact a subspace (Proposition 1.2.1.2).
(iv). Each linear-transformation has a *kernel*, a subspace of the domain (Proposition 1.2.2.3).
(v). Each linear-transformation has an *image*, a subspace of the codomain (Proposition 1.2.2.3).

2. Linear-independence, spanning, bases, and dimension

2.1 Spanning and linear-independence

If you've studied linear algebra before, you'll almost certainly recall that the concepts of linear-independence, spanning, and basis are of fundamental importance. We next turn to the study of these concepts. Before we discuss any of these, however, we must first discuss some preliminaries.

2.1.1 Linear-combinations and cofiniteness

Let V be a $\mathbb{K}$-module, let $\mathcal{I}$ be an indexing set, and for every $i \in \mathcal{I}$ let $v_i \in V$. In the course of these notes, you will eventually see us write something like the following.

$$\sum_{i \in \mathcal{I}} v_i. \tag{2.1.1.1}$$

If $\mathcal{I} = \{1, \ldots, m\}$ is finite, there is no worry about what this might mean:

$$\sum_{i \in \mathcal{I}} v_i := v_1 + \cdots + v_m. \tag{2.1.1.2}$$

However, if $\mathcal{I}$ is infinite, the corresponding sum is infinite, and it a priori has no meaning. If we wanted to give such an infinite sum

meaning, we would have to define a notion of convergence. For us, however, it will be most convenient to use the following convention.[1]

Definition 2.1.1.3 — Cofinite Let X be a set and let $S \subseteq X$. Then, S is ***cofinite*** in X iff $X \setminus S$ is finite.

Convention 2.1.1.4 Whenever a sum that is not necessarily finite appears, it should be assumed that cofinitely many terms are 0.

R We will see later (Proposition 6.4.2.3) that this is just the statement that, unless otherwise stated, we assume the sum converges in the discrete topology. In fact, when it becomes relevant, this convention will be superseded by the more general Convention 6.4.2.8.

Thus, if ever we write down a sum as in (2.1.1.1), you should pretend that the sum comes suffixed with the clause "... where cofinitely many v_is are 0.". This essentially had to be the case in order for the sum to make sense, and not having to explicitly say this every time will cut down on the verbosity.

Our first experience with this convention appears in the following fundamental definition.

Definition 2.1.1.5 — Linear-combination Let V be a $\mathbb{K}$-module and let $S \subseteq V$. Then, a ***linear-combination*** of elements of S is an element in V of the form

$$\sum_{v \in S} \alpha_v \cdot v \tag{2.1.1.6}$$

for $\alpha_v \in \mathbb{K}$.

R We will find that many concepts are most clearly illustrated in the finite case, and the definition of linear-combination is no exception: If $S = \{v_1, \ldots, v_m\}$, then a linear-combination of $v_1, \ldots, v_m$ is an element

[1] For what it's worth, this convention is equivalent to the notion of convergence defined by the *discrete topology*, whatever that means.

in V of the form

$$\alpha_1 \cdot v_1 + \cdots + \alpha_m \cdot v_m \tag{2.1.1.7}$$

for $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$.

2.1.2 Spanning

If we have a collection of vectors, then we can generate a bunch of other vectors by taking linear-combinations of the ones we started with. The collection of all such linear-combinations will be a subspace, and in fact, the *smallest* subspace containing our original collection. This subspace has a name: the *span*.

Theorem 2.1.2.1 — Span. Let V be a $\mathbb{K}$-module and let $S \subseteq V$. Then, there is a unique subspace of V, the ***span*** of S, $\mathrm{Span}(S)$, such that

(i). $S \subseteq \mathrm{Span}(S)$; and
(ii). if $W \subseteq V$ is another subspace containing S, it follows that $\mathrm{Span}(S) \subseteq W$.

Furthermore, explicitly, $\mathrm{Span}(S)$ is the set of all linear-combinations of elements of S.

R Thus, if $S = \{v_1, \ldots, v_m\}$, we have that

$$\begin{aligned} \mathrm{Span}(v_1, \ldots, v_m) &:= \mathrm{Span}(S) \\ &= \{\alpha_1 \cdot v_1 + \cdots + \alpha_m \cdot v_m : \\ &\qquad \alpha_k \in \mathbb{K}\}. \end{aligned} \tag{2.1.2.2}$$

R In the context of R-modules, this is usually referred to as the subspace ***generated*** by S.

Proof. We leave this as an exercise.

Exercise 2.1.2.3 Prove this yourself.

■

Exercise 2.1.2.4 What is Span($\emptyset$)?

Definition 2.1.2.5 — Spanning Let V be a $\mathbb{K}$-module and let $S \subseteq V$. Then, S is ***spanning*** iff Span$(S) = V$.

R Synonymously, we also say that S ***spans*** V.

R In other words, this means that every vector in V can be written as a linear combination of elements of S.

2.1.3 Linear-independence

Given a collection of vectors, we can take the set of all linear-combinations to form the span. A question we might ask is "Can we obtain a single vector in this way from two distinct linear-combinations?", or less precisely, "Is our collection of vectors 'redundant' in some sense?". There is a term for this "redundancy": *linear-dependence*.

Definition 2.1.3.1 — Linear-independence Let V be a $\mathbb{K}$-module and let $S \subseteq M$. Then, S is ***linearly-independent*** iff whenever

$$\sum_{v \in S} \alpha_v \cdot v = 0 \tag{2.1.3.2}$$

for $\alpha_v \in \mathbb{K}$, it follows that $\alpha_v = 0$ for all $v \in S$.

S is ***linearly-dependent*** iff it is not linearly-independent.

R In words, S is linearly-independent iff the only way to obtain 0 by taking linear-combinations of elements of S is with the trivial linear combination.

R If $S = \{v_1, \ldots, v_m\}$ is finite, this definition is equivalent to the statement that S is linearly-independent iff

$$\alpha_1 \cdot v_1 + \cdots + \alpha_m \cdot v_m \tag{2.1.3.3}$$

implies that $\alpha_1 = 0, \ldots, \alpha_m = 0$.

Furthermore, even if S is not necessarily finite, you may prefer to use the equivalent definition: "S is linearly-independent iff for every $m \in \mathbb{N}$ and $v_1, \ldots, v_m \in S$

$$\alpha_1 \cdot v_1 + \cdots + \alpha_m \cdot v_m = 0 \tag{2.1.3.4}$$

implies

$$\alpha_1 = 0, \ldots, \alpha_m = 0. \tag{2.1.3.5}$$

R Explicitly, S is linearly-dependent iff there are $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ *not all zero* and $v_1, \ldots, v_m \in S$ such that

$$\alpha_1 \cdot s_1 + \cdots + \alpha_m \cdot s_m = 0. \tag{2.1.3.6}$$

R Proposition 2.1.3.7 is probably a more intuitive way to understand linear-dependence. However, we do not take it as a definition because (i) it is not the right, or at least standard, notion for general $\mathbb{K}$-modules; and (ii) in practice, it is easiest to check whether a collection of vectors is linearly-independent using this definition.

R Note that S is automatically linearly-dependent if $0 \in S$.[a]

[a] Why?

What follows is arguably a more intuitive way to think about linear (in)dependence.

Proposition 2.1.3.7 Let V be a vector space and let $v_1, \ldots, v_m \in V$. Then, $\{v_1, \ldots, v_m\}$ is linearly-dependent iff there is some $1 \leq k \leq m$ such that

$$v_k \in \mathrm{Span}(v_1, \ldots, v_{k-1}), \tag{2.1.3.8}$$

in which case

$$\mathrm{Span}(v_1, \ldots, v_{k-1}) = \mathrm{Span}(v_1, \ldots, v_k). \tag{2.1.3.9}$$

R That is, a set is linearly-independent iff one of the vectors is a linear-combination of the others.

R Warning: Note that this is *not* true for $\mathbb{K}$-modules in general—see Example 2.1.3.24.[a] Instead, what is true is that linear-dependence is equivalent to the statement that some nonzero scalar multiple of some v_k can be written as a linear-combination of the other v_is.

[a] If you think of the proof, you'll note that at some point you'll have to *divide* by one of the coefficients.

Proof. We leave this as an exercise.

Exercise 2.1.3.10 Prove this yourself.

■

Exercise 2.1.3.11 Let V be a vector space and let $v_1, v_2 \in V$. Show that $\{v_1, v_2\}$ is linearly-*dependent* iff v_2 is a scalar multiple of v_1 or v_1 is a scalar multiple of v_2.

Proposition 2.1.3.12 Let V be a $\mathbb{K}$-module, and let $S \subseteq V$. Then, S is linearly-independent iff for every $w \in \mathrm{Span}(S)$ there

are unique $w^v \in \mathbb{K}$ such that

$$w = \sum_{v \in S} w^v \cdot v. \tag{2.1.3.13}$$

R The significant thing here is the *uniqueness*. We of course know automatically that there exist some coefficients for which this works from the definition of Span (Theorem 2.1.2.1)—the linear-independence of S tells us that these coefficients are *unique*.

R If $S = \{v_1, \ldots, v_m\}$ is finite, then this is equivalent to the statement that for every $w \in \mathrm{Span}(S)$ there are unique $w^1, \ldots, w^m \in \mathbb{K}$ such that

$$w = w^1 \cdot v_1 + \cdots + w^m \cdot v_m. \tag{2.1.3.14}$$

Proof. ($\Rightarrow$) Suppose that S is linearly-independent. Let $w \in \mathrm{Span}(S)$. From Theorem 2.1.2.1, the definition of Span, it follows that there are $w^v \in \mathbb{K}$ such that

$$w = \sum_{v \in S} w^v \cdot v. \tag{2.1.3.15}$$

We wish to show that this linear-combination is unique. So, suppose also that

$$w = \sum_{v \in S} \alpha^v \cdot v \tag{2.1.3.16}$$

for $\alpha^v \in \mathbb{K}$. Subtracting (2.1.3.16) from (2.1.3.15), we find

$$0 = \sum_{v \in S} (w^v - \alpha^v) \cdot v. \tag{2.1.3.17}$$

The definition of linear-independence then implies that $w^v - \alpha^v = 0$, that is, $w^v = \alpha^v$.

Suppose that for every $w \in \mathrm{Span}(S)$ there are unique $w^v \in \mathbb{K}$ such that

$$w = \sum_{v \in S} w^v \cdot v. \tag{2.1.3.18}$$

Suppose that

$$0 = \sum_{v \in S} \alpha_v \cdot v \tag{2.1.3.19}$$

for $\alpha_v \in \mathbb{K}$. As we also have

$$0 = \sum_{v \in S} 0 \cdot v, \tag{2.1.3.20}$$

by uniqueness, we have that $\alpha_v = 0$. Hence, by definition, S is linearly-independent. ■

▪ **Example 2.1.3.21** The set of functions

$$\left\{x \mapsto \cos(x), x \mapsto \sin(x), x \mapsto \mathrm{e}^{\mathrm{i}x}, x \mapsto \mathrm{e}^{-\mathrm{i}x}\right\} \tag{2.1.3.22}$$

is linearly-*dependent* in $C^\infty(\mathbb{R})$ regarded as a complex vector space. However, they are linearly-*independent* when $C^\infty(\mathbb{R})$ is regarded a a real vector space.

Exercise 2.1.3.23 Check both of these claims.

R Hint: Euler's Formula.

▪ **Example 2.1.3.24** Take $R := \mathbb{Z}$, $V := \mathbb{Z}$, and $m \cdot n := mn$. Then, the set $\{2, 3\}$ is linearly-*dependent* as $3 \cdot 2 + (-2) \cdot 3 = 0$, but yet 2 is not a linear-combination of other elements of $\{2, 3\}$: this would mean that 2 is a multiple of 3, but of course it's not.

▪ **Example 2.1.3.25** [a] Define

$$L := \left\{ \sqrt{p} \in \mathbb{R} : p \in \mathbb{Z}^+ \text{ is prime.} \right\}. \tag{2.1.3.26}$$

We claim that L is linearly-independent in $\mathbb{R}$ over $\mathbb{Q}$. To show that, it suffices to show that every finite subset of L is linearly-independent. So, let $p_1, \ldots, p_m \in \mathbb{Z}^+$ be prime. Denote by

$$\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}) \tag{2.1.3.27}$$

the smallest subfield of $\mathbb{R}$ that contains each $\sqrt{p_k}$. Note that this is a vector space over $\mathbb{Q}$ (in fact, a subspace of R over $\mathbb{Q}$).

Exercise 2.1.3.28 Show that

$$\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}) = \operatorname{Span}\left(\left\{ \sqrt{\prod_{k \in S} p_k} : S \subseteq \{1, \ldots, m\} \right\} \right).$$

R To clarify, among the elements appearing inside the Span, 1 is in this list, each $\sqrt{p_k}$ is in this list, each $\sqrt{p_i p_j}$ for $i < j$ is in this list, each $\sqrt{p_i p_j p_k}$ for $i < j < k$ is in this list, etc..

Thus, if we can show that

$$\dim\left(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}\right) = 2^m, \tag{2.1.3.29}$$

it must be the case that

$$\left\{ \sqrt{\prod_{k \in S} p_k} : S \subseteq \{1, \ldots, m\} \right\} \tag{2.1.3.30}$$

is linearly-independent over $\mathbb{Q}$, and in particular $\{\sqrt{p_1}, \ldots, \sqrt{p_m}\}$ is linearly-independent over $\mathbb{Q}$. We prove (2.1.3.29) by induction.

Exercise 2.1.3.31 Do the initial step by proving

$$\dim\left(\mathbb{Q}(\sqrt{p_1})\right) = 2. \tag{2.1.3.32}$$

For the inductive step, suppose that we have proven that

$$\dim\left(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})\right) = 2^k \tag{2.1.3.33}$$

for all $k < m$. Define

$$\mathbb{F} := \mathbb{Q}\left(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{m-2}})\right). \tag{2.1.3.34}$$

By the inductive hypothesis, we have that $\dim_{\mathbb{Q}}(\mathbb{F}) = 2^{m-2}$.

Exercise 2.1.3.35 Show that

(i).

$$\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}) = \mathbb{F}(\sqrt{p_{m-1}}, \sqrt{p_m});$$

and

(ii).

$$\dim_{\mathbb{Q}}\left(\mathbb{F}(\sqrt{p_{m-1}}, \sqrt{p_m})\right) = \dim_{\mathbb{F}}\left(\mathbb{F}(\sqrt{p_{m-1}}, \sqrt{p_m})\right) \dim_{\mathbb{Q}}(\mathbb{F}).$$

R To clarify, $\mathbb{F}(\sqrt{p_{m-1}}, \sqrt{p_m})$ is the smallest subfield of $\mathbb{R}$ that contains $\mathbb{F}$, $\sqrt{p_{m-1}}$, and $\sqrt{p_m}$. It is a vector space over $\mathbb{F}$, and hence may also be regarded as a vector space over $\mathbb{Q}$.

Exercise 2.1.3.36 Show that

$$\dim_{\mathbb{F}}\left(\mathbb{F}(\sqrt{p_{m-1}}, \sqrt{p_m})\right) = 4. \tag{2.1.3.37}$$

Putting the results of the previous to exercises together, we find that

$$\dim_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_m})\right) = 4\cdot 2^{m-2} = 2^m, \quad (2.1.3.38)$$

as desired.

[a] Adapted from math.stackexchange.

2.2 Bases

We have now defined two properties that a collection of vectors may or may not have, *spanning* and *linear-independence*. If a collection of vectors satisfies both such properties, it is called a *basis*.

Definition 2.2.1 — Basis Let V be a $\mathbb{K}$-module, and let $\mathcal{B}\subseteq V$. Then, $\mathcal{B}$ is a ***basis*** of V iff for every $v\in V$ there are unique $v^b\in\mathbb{K}$ such that

$$v=\sum_{b\in\mathcal{B}} v^b\cdot b. \quad (2.2.2)$$

R In words, $\mathcal{B}$ is a basis iff every vector can be written as a *unique* linear-combination of elements of $\mathcal{B}$.

Proposition 2.2.3 Let V be a $\mathbb{K}$-module, and let $\mathcal{B}\subseteq V$. Then, $\mathcal{B}$ is a basis of V iff $\mathcal{B}$ is linearly-independent and spans V.

Proof. ($\Rightarrow$) Suppose that $\mathcal{B}$ is a basis of V. By definition, every element of V is a linear-combination of elements of $\mathcal{B}$, and so $\mathcal{B}$ spans V. It is linearly-independent by Proposition 2.1.3.12.

($\Leftarrow$) Suppose that $\mathcal{B}$ is linearly-independent and spans V. Let $v \in V$. As $\mathcal{B}$ spans V, there are $v^b \in \mathbb{K}$ such that

$$v = \sum_{b \in \mathcal{B}} v^b \cdot b. \tag{2.2.4}$$

As $\mathcal{B}$ is linearly-independent, by Proposition 2.1.3.12, this is the unique such linear-combination, and so $\mathcal{B}$ is a basis by definition. ■

▪ **Example 2.2.5 — Standard basis of $\mathbb{K}^d$** Let $\mathbb{K}$ be a ring and let $d \in \mathbb{N}$. Then, $\mathbb{K}^d$ has a canonical basis, the ***standard basis***, which is given by

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right\}. \tag{2.2.6}$$

▪ **Example 2.2.7** $\{1, x, x^2, \ldots\}$ is a basis for $\mathbb{K}[x]$.

If we start with a collection of linearly-independent vectors, adding more vectors to our collection runs of the risk of making our collection linearly-*dependent*. In the other direction, if we start with a collection of vectors which span the vector space, removing vectors from our collection runs the risk of obtaining a collection that fails to span. Likewise, adding vectors makes it easier to span and removing vectors makes it easier to be linearly-independent. A basis is an exact middle ground between spanning and linear-independence in the following sense.

Proposition 2.2.8 Let V be a vector space and let $\mathcal{B} \subseteq V$. Then, the following are equivalent.

(i). $\mathcal{B}$ is a basis.
(ii). $\mathcal{B}$ is a maximal linearly-independent set.

(iii). $\mathcal{B}$ is a minimal spanning set.

R Intuitively, "maximal linearly-independent set" means that if you add any new vector at all to $\mathcal{B}$, the resulting set must fail to be linearly-independent. Similarly, "minimal spanning set" means that if you remove any vector at all from $\mathcal{B}$, the resulting set must fail to span. See Definition A.3.5.3 for the precise definitions of maximal and minimal.

R Warning: This fails over general R-modules—see Examples 2.2.22 and 2.2.23. That said, (i) implies both (ii) and (iii) no matter what.

Proof. Denote the ground division ring by $\mathbb{F}$.

$((i) \implies (ii))$ Suppose that $\mathcal{B}$ is a basis. $\mathcal{B}$ is linearly-independent by Proposition 2.2.3, so it only remains to show maximality. Let $C \subseteq V$ be linearly-independent and such that $C \supseteq \mathcal{B}$. We wish to show that $\mathcal{B} = C$, that is, that $C \subseteq \mathcal{B}$. So, let $c \in C$. If $c \in \mathcal{B}$, we're done, so suppose $c \notin \mathcal{B}$. As $\mathcal{B}$ spans by Proposition 2.2.3 again, there are unique $c^b \in \mathbb{K}$ such that

$$c = \sum_{b \in \mathcal{B}} c^b \cdot b. \tag{2.2.9}$$

It follows that

$$\sum_{b \in \mathcal{B}} c^b \cdot b - 1 \cdot c = 0, \tag{2.2.10}$$

and so as each $b \in C$ and C is linearly-independent, it follows that $1 = 0$,[a] and so $\mathbb{F} = 0$. But then the only linear-combinations of elements of $\mathcal{B}$ is 0, and so $V = 0$, in which case we must have $\mathcal{B} = \emptyset = C$.

$((ii) \implies (i))$ $\mathcal{B}$ is a maximal linearly-independent set. It remains to show that $\mathcal{B}$ spans. So, let $v \in V$. If $v \in \mathcal{B}$, of

course $v \in \text{Span}(\mathcal{B})$. Otherwise, $\mathcal{B} \cup \{v\}$ is strictly larger than $\mathcal{B}$, and so as $\mathcal{B}$ is a maximal linearly-independent set, it must be the case that $\mathcal{B} \cup \{v\}$ is linearly-dependent, so that there are $\alpha^b, \alpha \in \mathbb{F}$, not all 0, such that

$$\sum_{b \in \mathcal{B}} \alpha^b \cdot b + \alpha \cdot v = 0. \tag{2.2.11}$$

If $\alpha = 0$, linear-independent of $\mathcal{B}$ implies that every $\alpha^b = 0$ as well, which is impossible (not all of these coefficients are 0). Therefore, $\alpha \neq 0$. Rearranging and multiplying by α^{-1} yields

$$v = -\alpha^{-1} \sum_{b \in \mathcal{B}} \alpha^b \cdot b \in \text{Span}(\mathcal{B}). \tag{2.2.12}$$

$((i) \implies (iii))$ Suppose that $\mathcal{B}$ is a basis. Let $C \subseteq V$ be a spanning set such that $C \subseteq \mathcal{B}$. We wish to show that $\mathcal{B} \subseteq C$. So, let $b \in \mathcal{B}$. If $b \in C$, we're done, so suppose that $b \notin C$. As C is a spanning set, there are $b^c \in \mathbb{F}$ such that

$$b = \sum_{c \in C} b^c \cdot c. \tag{2.2.13}$$

It follows that

$$\sum_{c \in C} b^c \cdot c - b = 0, \tag{2.2.14}$$

and so, as each $c \in \mathcal{B}$ and $\mathcal{B}$ is linearly-independent, it follows in particular that $1 = 0$, so that $\mathbb{F} = 0$, and hence $V = 0$, and hence $\mathcal{B} = \emptyset = C$.

$((iii) \implies (i))$ Suppose that $\mathcal{B}$ is a minimal spanning set. We wish to show that $\mathcal{B}$ is linearly-independent. So, suppose that

$$0 = \sum_{b \in \mathcal{B}} \alpha_b \cdot b \tag{2.2.15}$$

for $\alpha_b \in \mathbb{K}$. If every $\alpha_b = 0$, we're done, so suppose this is not the case. Then, there is some $b_0 \in \mathcal{B}$ such that $\alpha_{b_0} \neq 0$. Then, we can rearrange this to find

$$b_0 = -\alpha_{b_0}^{-1} \sum_{\substack{b \in \mathcal{B} \\ b \neq b_0}} \alpha_b \cdot b \in \mathrm{Span}(\mathcal{B}). \tag{2.2.16}$$

It then follows that $\mathcal{B} \setminus \{b_0\}$ is again a spanning set, which contradicts minimality. ■

[a] This implicitly uses the fact that $c \not\in \mathcal{B}$, for otherwise we might have, for example, $c = b_1$, in which case we would instead deduce that $c^1 = 1$.

We mentioned before that if we start adding vectors to a linearly-independent set, it's becomes more likely to span but we run the risk of making our set linearly-dependent. In the other direction, if we start removing vectors from a spanning set, it becomes more likely to be linearly-independent but we run the risk of having our set fail to span. One might then ask the questions "Can I always add vectors to a linearly-independent set to get a spanning set without ruining my linear-independence, that is, can I obtain a basis in this way?" and "Can I always remove vectors from a spanning set to obtain a linearly-independent set without losing the property of being spanning?". Fortunately, it turns out that the answer to both of these questions is "Yes.".

Proposition 2.2.17 Let V be a vector space and let $S \subseteq V$.

(i). If S is spanning, then there is a subset of S that is a basis.

(ii). If S is linearly-independent, then there is a superset of S that is a basis.

R Warning: This fails over general R-modules—see Examples 2.2.22 and 2.2.23.

Proof. Denote the ground division ring by $\mathbb{F}$.

(i)[a] Suppose that S is spanning. Define

$$\mathscr{S} := \{A \subseteq V : A \subseteq S \text{ and } A \text{ is linearly-independent.}\}.$$

$\mathscr{S}$ a partially-ordered set with respect to the usual inclusion $\subseteq$ partial-order. We wish to show that $\langle \mathscr{S}, \subseteq \rangle$ has a maximal element, which will be a basis by Proposition 2.2.8. To show that $\langle \mathscr{S}, \subseteq \rangle$ has a maximal element, we apply Zorn's Lemma (Theorem A.3.5.9).

So, let $\mathscr{T} \subseteq \mathscr{S}$ be a totally-ordered subset and define

$$T_0 := \bigcup_{T \in \mathscr{T}} T. \tag{2.2.18}$$

Certainly, if indeed $T_0 \in \mathscr{S}$, it will be an upper-bound of $\mathscr{T}$, whence Zorn's Lemma will imply the existence of a maximal element, as desired. To show that $T_0 \in \mathscr{S}$, we wish to show that T_0 is linearly-independent. So, let $v_1, \ldots, v_m \in T_0$ and suppose that

$$\alpha_1 \cdot v_1 + \cdots + \alpha_m \cdot v_m = 0 \tag{2.2.19}$$

for $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$. For each v_k, there is some $T_k \in \mathscr{T}$ such that $v_k \in T_k$. As $\mathscr{T}$ is in particular totally-ordered, there is some T_k that contains the rest. But then, as T_k is linearly-independent, (2.2.19) implies that every $\alpha_k = 0$, so that T_0 is linearly-independent, as desired.

Thus, there is a maximal element $\mathcal{B} \in \mathscr{S}$. It is linearly-independent and maximal with this property *among subsets of* S, but we don't yet know that it is a maximal linearly-independent set *period* (that is, among all subsets of V). Instead of proving that $\mathcal{B}$ is a method using this technique, we simply show that $\mathcal{B}$ spans. As S spans, it suffices to show that $s \in \mathrm{Span}(\mathcal{B})$ for every $s \in S$. So, let $s \in S$. If $s \in \mathcal{B}$, of course $s \in \mathrm{Span}(\mathcal{B})$, so suppose this is not the case. Then,

$\mathcal{B} \cup \{s\} \subseteq S$ is strictly larger than $\mathcal{B}$, and so if it were linearly-independent, we would have a contradiction of the maximality of $\mathcal{B}$. Thus, s can be written as a linear-combination of elements of $\mathcal{B}$, as desired.

(ii) Suppose that S is linearly-independent. Define

$$\mathscr{S} := \{A \subseteq V : A \supseteq S \text{ and } A \text{ is linearly-independent.}\}.$$

A maximal element of $\mathscr{S}$ will be a maximal linearly-independent set, and hence a basis by Proposition 2.2.8. To show that $\mathscr{S}$ has a maximal element, we apply Zorn's Lemma (Theorem A.3.5.9).

So, let $\mathscr{T} \subseteq \mathscr{S}$ be a totally-ordered subset and define

$$T_0 := \bigcup_{T \in \mathscr{T}} T. \tag{2.2.20}$$

Certainly, if indeed $T_0 \in \mathscr{S}$, it will be an upper-bound of $\mathscr{T}$, whence Zorn's Lemma will imply the existence of a maximal element, as desired. To show that $T_0 \in \mathscr{S}$, we wish to show that T_0 is linearly-independent. So, let $v_1, \ldots, v_m \in T_0$ and suppose that

$$\alpha_1 \cdot v_1 + \cdots + \alpha_m \cdot v_m = 0 \tag{2.2.21}$$

for $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$. For each v_k, there is some $T_k \in \mathscr{T}$ such that $v_k \in T_k$. As $\mathscr{T}$ is in particular totally-ordered, there is some T_k that contains the rest. But then, as T_k is linearly-independent, (2.2.21) implies that every $\alpha_k = 0$, so that T_0 is linearly-independent, as desired. ■

[a] Proof adapted from [Con17].

■ **Example 2.2.22 — A maximal linearly-independent set which is not a basis** Define $\mathbb{K} := \mathbb{Z}$ and $V := \mathbb{Z}$. V is then a $\mathbb{K}$-module with the usual operations. $\{2\} \subseteq V$ is a

linearly-independent set, for if $n \cdot 2 = 0$, we must of course have that $n = 0$. In fact, it is indeed a *maximal* linearly-independent set, for if $m \in V$ is any other integer, we have $(-2) \cdot n + n \cdot 2 = 0$, and so $\{2, n\}$ is not linearly-independent. On the other hand, it is not a basis as $1 \notin \text{Span}(\{2\})$.

Note that this also furnishes an example of a linearly-independent set for which no superset is a basis.

▪ **Example 2.2.23 — A minimal spanning set which is not a basis** Define $\mathbb{K} := \mathbb{Z}$ and $V := \mathbb{Z}$. V is then a $\mathbb{K}$-module with the usual operations. $\{2, 3\} \subseteq V$ spans V, for if $n \in V$, we have that

$$n = n \cdot 3 - n \cdot 2 \in \text{Span}(\{2, 3\}). \tag{2.2.24}$$

In fact, it is indeed a *minimal* spanning set, for neither $\{2\}$ nor $\{3\}$ span V. On the other hand, it is not a basis because it is not linearly-independent: $(-3) \cdot 2 + 2 \cdot 3 = 0$.

Note that this also furnishes an example of a spanning set for which no subset is a basis.

Bases are incredibly important in the theory of vector spaces for at least three reasons: they provide a convenient way to define linear-transformations (Theorem 2.2.25), they allow us to define *dimension* (Theorem 2.2.1.1 and Definition 2.2.1.20), and they allow us to define *coordinates* (Definition 3.1.1 and Theorem 3.2.2.1). We start with the first.

Theorem 2.2.25 — Linear-transformations and basis of domain. Let V and W be $\mathbb{K}$-modules, let $\mathcal{B}$ be a basis for V, and for every $b \in \mathcal{B}$ let $w_b \in W$ be some vector in W. Then, there exists a unique linear-transformation $T : V \to W$ such that $T(b) = w_b$ for all $b \in \mathcal{B}$.

R In words, you can define a linear-transformation by specifying where elements of a given basis are mapped to.

Proof. Let $v \in V$. Then, there are unique $m \in \mathbb{N}$, nonzero $v^1, \dots, v^m \in \mathbb{K}$, and $b_1, \dots, b_m \in \mathcal{B}$ such that

$$v = v^1 \cdot b_1 + \cdots + v^m \cdot b_m. \tag{2.2.26}$$

Define $T : V \to W$ by

$$T(v) := v^1 \cdot w_{b_1} + \cdots + v^m \cdot w_{b_m}. \tag{2.2.27}$$

Certainly, $T(b) = w_b$ by definition.

Exercise 2.2.28 Check that T is in fact linear.

Finally, linearity dictated that this was the only possible choice for $T(v)$ if we required that b be mapped to w_b, and so T is the unique such linear-transformation. ■

2.2.1 Dimension

Intuitively, the dimension of a vector space is the number of scalars required to uniquely specify any element in that vector space. For example, I can uniquely specify any element of $\mathbb{R}^3$ with three real numbers. The definition of a basis (Definition 2.2.1) says that, if the basis has d elements, then any element in the vector space can be uniquely specified by d scalars. Thus, the idea is to define the dimension to be the cardinality of a given basis.[2] This presents a couple of potential problems: What if the vector space doesn't have a basis? What if two different bases have a different number of elements? For example, if my vector space has one basis with 2 elements and another basis with 3? Should the dimension be 2 or 3? Fortunately, the next result tells us that these pathologies cannot happen.

[2] Intuitively, just the number of elements in the basis—see Appendix A.5.1.

Theorem 2.2.1.1 — Fundamental Theorem of Dimension. Let V be a vector space.

(i). V has a basis.

(ii). Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be bases of V. Then, $\mathcal{B}_1$ and $\mathcal{B}_2$ have the same cardinality.

R Warning: $\mathbb{K}$-modules in general need not have a basis—see Example 2.2.1.21.

R In fact, those $\mathbb{K}$-modules which do have a basis are called ***free modules***—see Definition 2.2.1.29.[a] However, even when $\mathbb{K}$-modules do have bases, distinct bases need not have the same cardinality—see Example 2.2.1.22. On the other hand, if $\mathbb{K}$ is commutative, then distinct bases do have the same cardinality—see Theorem 2.2.1.31.

R "Fundamental Theorem of Dimension" is not a standard name for this result (it doesn't have a standard name), so don't expect other people to know what you're talking about if you decide to use it.

[a] Using this terminology, (i) becomes the statement that modules over division rings are free.

Proof. STEP 1: INTRODUCE NOTATION

Denote the ground division ring by $\mathbb{F}$. To simplify notation by getting rid of some subscripts, let us instead write $\mathcal{B} := \mathcal{B}_1$ and $C := \mathcal{B}_2$.

STEP 2: PROVE (I)

The idea of the proof is to show that V has a maximal linearly-independent set. This will be a basis by Proposition 2.2.8. The reason this is the strategy is because we have a result that asserts the existence of maximal things—*Zorn's Lemma (Theorem A.3.5.9)*.

So, define

$$\mathscr{B} := \{S \subseteq V : S \text{ is linearly-independent.}\}. \quad (2.2.1.2)$$

We consider $\mathscr{B}$ as a partially-ordered set with respect to the relation of inclusion. As just explained, a maximal element of $\mathscr{B}$ will be a basis. Furthermore, Zorn's Lemma states that $\mathscr{B}$ will have a maximal element if every well-ordered subset of $\mathscr{B}$ has an upper-bound in $\mathscr{B}$, and so it suffices to show this.

So, let $\mathscr{S} \subseteq \mathscr{B}$ be a well-ordered subset of $\mathscr{B}$. Define

$$\mathcal{B} := \bigcup_{S \in \mathscr{S}} S \quad (2.2.1.3)$$

This certainly contains every element of $\mathscr{S}$, and so it only remains to check that $\mathcal{B} \in \mathscr{B}$, that is, we need to check that $\mathcal{B}$ is linearly-independent. So, let $b_1, \ldots, b_m \in \mathcal{B}$ and suppose that

$$\alpha_1 \cdot b_1 + \cdots + \alpha_m \cdot b_m = 0 \quad (2.2.1.4)$$

for $\alpha_k \in \mathbb{F}$. As $b_k \in \mathcal{B}$, there is some $S_k \in \mathscr{S}$ such that $b_k \in S_k$. As $\mathscr{S}$ is totally-ordered, some S_k contains all the others. Without loss of generality, suppose that $S_1 \supseteq S_1, \ldots, S_m$. It follows that $b_k \in S_1$ for all $1 \leq k \leq m$, and so as S_1 is linearly-independent, we find that each $\alpha_k = 0$, as desired.

Step 3: Prove that if $\mathcal{B}$ is finite, then C is finite

Suppose that $\mathcal{B}$ is finite. Write $\mathcal{B} =: \{b_1, \ldots, b_d\}$. For each $b_k \in \mathcal{B}$, there is a nonempty finite subset $C_k \subseteq C$ such that $b_k \in \mathrm{Span}(C_k)$. Thus,

$$\{b_1, \ldots, b_d\} \subseteq \mathrm{Span}\left(\bigcup_{k=1}^{d} C_k\right), \quad (2.2.1.5)$$

and hence

$$\begin{aligned} V &= \mathrm{Span}(b_1, \ldots, b_d) \\ &\subseteq \mathrm{Span}\left(\bigcup_{k=1}^{d} C_k\right) \subseteq \mathrm{Span}(C) = V, \end{aligned} \quad (2.2.1.6)$$

and so all of these inclusions must be equalities. In particular,

$$\text{Span}\left(\bigcup_{k=1}^{d} C_k\right) = V. \tag{2.2.1.7}$$

However, as C is a basis, it is a minimal spanning set, and so

$$C = \bigcup_{k=1}^{d} C_k, \tag{2.2.1.8}$$

and so C is finite.

STEP 4: PROVE (II) IN THE CASE ONE IS FINITE
Without loss of generality, suppose that $\mathcal{B}$ is finite. By the previous step, C must also be finite. Write $\mathcal{B} = \{b_1, \ldots, b_d\}$ and $C = \{c_1, \ldots, c_e\}$. We wish of course to show that $d = e$. Without loss of generality, suppose that $d \leq e$.

$b_1 \in \text{Span}(C)$, so we may write

$$b_1 = b^1{}_1 \cdot c_1 + \cdots + b^e{}_1 \cdot c_e \tag{2.2.1.9}$$

for $b^k{}_1 \in \mathbb{F}$. Not all of these coefficients can be 0, so without loss of generality, suppose that $b^1{}_1 \neq 0$. Then, rearranging, we see that $c_1 \in \text{Span}(b_1, c_2, \ldots, c_e)$, and hence

$$V = \text{Span}(c_1, \ldots, c_e) = \text{Span}(b_1, c_2, \ldots, c_e). \tag{2.2.1.10}$$

Exercise 2.2.1.11 Verify that $\{b_1, c_2, \ldots, c_e\}$ is still linearly-independent.

We thus have a new basis $\{b_1, c_2, \ldots, c_e\}$ with exactly e elements. In particular, $b_2 \in \text{Span}(b_1, c_2, \ldots, c_e)$, and so we can write

$$b_2 = a^1{}_2 \cdot b_1 + b^2{}_2 \cdot c_2 + \cdots + b^e{}_2 \cdot c_e. \tag{2.2.1.12}$$

We can't have all of the ${b^k}_2 = 0$, for then $\{b_1, b_2\}$ would be linearly-dependent. Thus, again, without loss of generality, ${b^2}_2 \neq 0$, and so $c_2 \in \mathrm{Span}(b_1, b_2, c_3, \ldots, c_e)$. Proceeding as before, we find that $V = \mathrm{Span}(b_1, b_2, c_3, \ldots, c_e)$.

Proceeding inductively, we may replace the c_ks with the corresponding b_ks to obtain bases, and eventually we find that

$$\{b_1, \ldots, b_d, c_{d+1}, \ldots, c_e\} \tag{2.2.1.13}$$

is a basis, and in particular, is a linearly-independent set that contains $\{b_1, \ldots, b_d\}$. As $\{b_1, \ldots, b_d\}$ is maximal linearly-independent, it follows that

$$\{b_1, \ldots, b_d\} = \{b_1, \ldots, b_d, c_{d+1}, \ldots, c_e\}, \tag{2.2.1.14}$$

and hence $d = e$, as desired.

STEP 5: PROVE (II) IN THE CASE BOTH ARE INFINITE

Now suppose that the cardinalities of both $\mathcal{B}$ and C are infinite. We wish to show that $|\mathcal{B}| \leq |C|$. If we can show this, then by $\mathcal{B} \leftrightarrow C$ symmetry, the same argument can be used to show that $|C| \leq |\mathcal{B}|$, whence we will have $|\mathcal{B}| = |C|$ by the Bernstein-Cantor-Schröder Theorem (Theorem A.5.1.9), as desired.

So, we would like to show that $|\mathcal{B}| \leq |C|$. Let $c \in C$. As $\mathcal{B}$ spans V, there are $b_1, \ldots, b_m \in \mathcal{B}$ and $c^1, \ldots, c^m \in \mathbb{F}$ nonzero such that

$$c = c^1 \cdot b_1 + \cdots + c^m \cdot b_m. \tag{2.2.1.15}$$

Define $\mathcal{B}_c := \{b_1, \ldots, b_m\}$, and for $F \subseteq \mathcal{B}$ finite, define

$$C_F := \{c \in C : \mathcal{B}_c = F\}. \tag{2.2.1.16}$$

We have that

$$C = \bigcup_{\substack{F \subseteq \mathcal{B} \\ F \text{ finite}}} C_F. \tag{2.2.1.17}$$

By Proposition A.5.2.2, the cardinality of the collection of finite subsets of $\mathcal{B}$ is just $|\mathcal{B}|$, and so the above is a union of $|\mathcal{B}|$ many nonempty finite sets, and hence $|C| \leq |\mathcal{B}|$ by Proposition A.5.2.5. ■

Corollary 2.2.1.18 Let V be a vector space, let $L \subseteq V$ be linearly-independent, and let $S \subseteq V$ be spanning. Then, $|L| \leq |S|$.

Proof. By Proposition 2.2.17, there are bases $\mathcal{B}$ and C such that $L \subseteq \mathcal{B}$ and $C \subseteq S$. It follows from the previous result that

$$|L| \leq |\mathcal{B}| = |C| \leq |S|. \tag{2.2.1.19}$$

■

Definition 2.2.1.20 — Dimension Let V be a vector space. Then, the *dimension* of V, $\dim(V)$, is the cardinality of a basis of V.

R Of course, this makes sense and is well-defined by Theorem 2.2.1.1. Indeed, in some sense, that was the entire point of this theorem.

R Sometimes we will want to consider the same set of vectors as a vector space over different division rings. In such a case, we will write $\dim_{\mathbb{F}}(V)$ to clarify what ground division ring we mean to work over. For example, we have $\dim_{\mathbb{C}}(\mathbb{C}) = 1$ but $\dim_{\mathbb{R}}(\mathbb{C}) = 2$.

▪ **Example 2.2.1.21 — A $\mathbb{K}$-module without a basis** Define $V := \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{K} := \mathbb{Z}$. V is then a $\mathbb{K}$-module. Furthermore, every subset of V is linearly-dependent: the only subset

of V that doesn't contain the 0 vector is $\{1\}$, and this itself is linearly-dependent as $2 \cdot 1 = 0$. Thus, V cannot have a basis.

▪ Example 2.2.1.22 — A $\mathbb{K}$-module with two bases of distinct cardinalities

R Warning: This example technically requires a knowledge of matrices, which we haven't yet discussed—see Subsection 3.2.1. Feel free to come back to this later if you like—the details aren't particularly important.

Define

$$\mathbb{K} := \left\{ \langle A^i{}_j : i, j \in \mathbb{N} \rangle \in \mathbb{R}^{\mathbb{N}\times\mathbb{N}} : \text{for every } j \in \mathbb{N}, \right.$$
$$\left. A^i{}_j = 0 \text{ for cofinitely many } i \in \mathbb{N}. \right\}.$$

Intuitively, $\mathbb{K}$ is thought of as infinite-dimensional square matrices (with rows and columns indexed by $\mathbb{N}$) such that each column only has finitely many nonzero entries. $\mathbb{K}$ is regarded as a ring with the usual definition of matrix addition and multiplication.[a]

Define $V := \mathbb{K}$ and $W := \mathbb{K}^2$ and regard these as $\mathbb{K}$-modules. We claim that there is an isomorphism of $\mathbb{K}$-modules $V \to W$. As V has a basis with 1 element and W has a basis of 2 elements, this isomorphism shows in particular that both V and W each have distinct bases with 1 and 2 elements.

We define a map $V \to W$ as follows. Given a matrix $M \in V$, we wish to define two matrices $\langle M_0, M_1 \rangle \in W$. Let M_0 be the matrix whose columns are exactly the even columns of M and M_1 be the matrix whose columns are exactly the odd columns of M (in the same order of course from left to right).

Exercise 2.2.1.23 Verify that this map is indeed an isomorphism.

[a]The condition that the columns have only finitely many nonzero entries guarantees that the sum involved in the definition of matrix multiplication is just a finite sum, and so makes sense.

Exercise 2.2.1.24 Let V be a vector space and let $W \subseteq V$ be a subspace.

(i). Show that $\dim(W) \leq \dim(V)$.
(ii). Show that if $\dim(W) = \dim(V)$ is finite, then $W = V$.
(iii). Find a counter-example to the previous part in infinite-dimensions.

We mentioned awhile back that the subspace associated to a linear-transformation can be used to detect injectivity and surjectivity, though we wanted to state the result until we had talked about dimension. It is time we return to this.

Proposition 2.2.1.25 Let $T: V \to W$ be a linear-transformation of $\mathbb{K}$-modules. Then, the following are equivalent.

(i). T is injective.
(ii). $\mathrm{Ker}(T) = 0$.
(iii). $\mathrm{Coim}(T) = V$.
(iv). $\dim(\mathrm{Ker}(T)) = 0$.
(v). $\dim(\mathrm{Coim}(T)) = \dim(V)$.

R The most important of these is the second, which, concretely, says that T is injective iff $T(v) = 0$ implies $v = 0$.

Proof. We leave this as an exercise.

Exercise 2.2.1.26 Prove this yourself.

■

Proposition 2.2.1.27 Let $T: V \to W$ be a linear-transformation of $\mathbb{K}$-modules. Then, the following are equivalent.

(i). T is surjective.
(ii). $\mathrm{Im}(T) = W$.
(iii). $\mathrm{Coker}(T) = 0$.
(iv). $\dim(\mathrm{Im}(T)) = \dim(W)$.
(v). $\dim(\mathrm{Coker}(T)) = 0$.

R Unlike the analogous result for injectivity, there really isn't much content here. Indeed, that (i) is equivalent to (ii) is essentially the definition of surjectivity. Nevertheless, we list it here in order to note the 'duality' with the corresponding result for injectivity.

Proof. We leave this as an exercise.

Exercise 2.2.1.28 Prove this yourself.

■

In elementary linear algebra, injectivity and surjectivity are often talked of in the context of solving systems of equations. For example, let $T: V \to W$ be a linear map, fix $w_0 \in W$, and consider the equation $T(x) = w_0$ in which x is the "unknown". Then, T is surjective iff for every $w_0 \in W$, there is a solution to this equation; T is injective iff, whenever there is a solution, that solution is unique.

Rank of $\mathbb{K}$-modules

R This subsubsection is tangential, and can safely be skipped on a first reading.

We saw above that every vector space has a basis, and furthermore, any two bases must have the same cardinality. We also saw how both of these results can fail if the ground ring is not a division ring. Despite this, for any ring $\mathbb{K}$, there are important classes of $\mathbb{K}$-modules for which we still have bases and a notion dimension (usually called *rank* in the context of $\mathbb{K}$-modules).

Definition 2.2.1.29 — Free module Let V be a $\mathbb{K}$-module. Then, V is ***free*** iff V has a basis.

The ***rank*** of a free module is the smallest cardinality of a basis.

R If V is a vector space, then it has a rank and its rank is the same as its dimension (by definition). The reason the term "rank" is used in this context instead of "dimension" is that it would likely give misleading intuition in some cases, though not in any case we will encounter.

R I suppose if you like you could define the rank of a module that is not free to be $-\infty$, but I've never seen this done.

We saw before in Example 2.2.1.22 that two bases in a $\mathbb{K}$-module need not have the same number of elements, which is why we needed to say "smallest cardinality" in the above definition. This allows us to make sense of the rank of any free module, but it would still be nice to know when any two bases have the same cardinality so that we need not worry about checking whether a basis we find is the smallest.

Definition 2.2.1.30 — Invariant-basis-number property Let V be a $\mathbb{K}$-module.

(i). V has the ***invariant-basis-number property*** iff V is free and any two bases of V have the same cardinality.

(ii). $\mathbb{K}$ has the ***invariant-basis-number property*** iff every free $\mathbb{K}$-module has the invariant-basis-number property.

R The reason we require V be free is because otherwise this condition would be vacuously satisfied.

Theorem 2.2.1.31. Let V be a $\mathbb{K}$-module. Then, if $\mathbb{K}$ is commutative, V has invariant-basis-number.

Proof. We leave this as an exercise.

Exercise 2.2.1.32 Prove this yourself.

R Hint: This really shouldn't be an exercise. It's only an exercise because I haven't yet had time to write the proof down myself—feel free to look it up.

■

2.2.2 The Rank-Nullity Theorem

Having discussed dimension, we can finally present what is arguably the most important result of elementary linear algebra: the *Rank-Nullity Theorem*.[3]

Definition 2.2.2.1 — Rank Let V and W be vector spaces and let $T: V \to W$ be a linear-transformation. Then, the ***rank*** of T is the dimension of the image of T.

Theorem 2.2.2.2 — Rank-Nullity Theorem. Let V and W be vector spaces and let $T: V \to W$ be a linear-transformation. Then,

$$\dim(V) = \dim(\mathrm{Ker}(T)) + \dim(\mathrm{Im}(T)). \tag{2.2.2.3}$$

R $\dim(\mathrm{Im}(T))$ is of course the rank of T. Presumably then, $\dim(\mathrm{Ker}(T))$ should probably be the ***nullity*** of T, though I can't say I've ever heard that term used on its own.

R In terms of matrices, this can be understood as follows. If A is a $e \times d$ matrix that defines a

[3] Indeed, Axler [Axl15] refers to this instead as the *Fundamental Theorem of Linear Maps*.

linear-transformation from $V := \mathbb{F}^d$ to $W := \mathbb{F}^e$, then $\dim(V) = d$ is the *number of columns* of A. $\dim(\mathrm{Ker}(T_A))$ is the *number of free-variables* of A and $\dim(\mathrm{Im}(T_A))$ is the *number of pivots* of A. Thus, for a matrix linear-transformation, this equation reads

$$\#\,\text{columns} = \#\,\text{free-variables} + \#\,\text{pivots}, \quad (2.2.2.4)$$

which is in some sense obvious since every column either corresponds to a free-variable or is a pivot column.

R While this itself is not true for $\mathbb{K}$-modules, what is true is the following: If $T\colon V \to W$ is a linear-transformation of $\mathbb{K}$-modules, then $V/\mathrm{Ker}(T) \to \mathrm{Im}(T)$ is an isomorphism—Definition 1.2.1.12 for the meaning of $V\,\mathrm{Ker}(T)$. This is an example of what is called the *First Isomorphism Theorem* in the subject known as *general algebra* or *universal algebra*.

Proof. Denote the ground division ring by $\mathbb{F}$. Let $\mathcal{B}$ be a basis of $\mathrm{Ker}(T)$ and let C be a basis of V with $C \supseteq \mathcal{B}$. Define $\mathcal{A} := C \setminus \mathcal{B}$, so that C is the disjoint union of $\mathcal{A}$ and $\mathcal{B}$, and hence

$$\dim(V) := |C| = |\mathcal{A}| + |\mathcal{B}| =: |\mathcal{A}| + \dim(\mathrm{Ker}(T)). \quad (2.2.2.5)$$

Thus, it suffices to show that $\dim(\mathrm{Im}(T)) = |\mathcal{A}|$. First, note that,

$$\mathcal{A} \ni a \mapsto T(a) \in T(\mathcal{A}) \quad (2.2.2.6)$$

is a bijection,[a] and hence $|\mathcal{A}| = |T(\mathcal{A})|$. Thus, it suffices to show that $|T(\mathcal{A})| = \dim(\mathrm{Im}(T))$. To do this, we show that $T(\mathcal{A})$ is a basis for $\mathrm{Im}(T)$.

We first check that $T(\mathcal{A})$ is linearly-independent. So, suppose that

$$\alpha_1 \cdot T(a_1) + \cdots + \alpha_m \cdot T(a_m) = 0 \quad (2.2.2.7)$$

for $\alpha_k \in \mathbb{F}$ and $a_k \in \mathcal{A}$. By linearity, it follows that

$$T(\alpha_1 \cdot a_1 + \cdots + \alpha_m \cdot a_m) = 0, \tag{2.2.2.8}$$

and hence

$$\alpha_1 \cdot a_1 + \cdots + \alpha_m \cdot a_m \in \mathrm{Ker}(T). \tag{2.2.2.9}$$

However, as $\mathcal{B}$ is a basis for $\mathrm{Ker}(T)$, this means that the above linear-combination of elements of $\mathcal{A}$ can be written as a linear-combination of elements of $\mathcal{B}$:

$$\alpha_1 \cdot a_1 + \cdots + \alpha_m \cdot a_m = \beta_1 \cdot b_1 + \cdots + \beta_n \cdot b_n \tag{2.2.2.10}$$

for $\beta_k \in \mathbb{F}$ and $b_k \in \mathcal{B}$. However, as

$$\{a_1, \ldots, a_m, b_1, \ldots, b_n\} \subseteq C, \tag{2.2.2.11}$$

this set is in particular linearly-independent, whence we find that $\alpha_k = 0 = \beta_k$ for all k, as desired.

Finally, we check that $\mathrm{Im}(T) = \mathrm{Span}(T(\mathcal{A}))$. Let $T(v) \in \mathrm{Im}(T)$. As $C = \mathcal{A} \cup \mathcal{B}$ is a basis for V, we can write

$$v = \alpha_1 \cdot a_1 + \cdots + \alpha_m \cdot a_m + \beta_1 \cdot b_1 + \cdots + \beta_n \cdot b_n \tag{2.2.2.12}$$

for $\alpha_k, \beta_k \in \mathbb{F}$, $a_k \in \mathcal{A}$, and $b_k \in \mathcal{B}$. As $b_k \in \mathrm{Ker}(T)$, it follows that

$$T(v) = \alpha_1 \cdot T(a_1) + \cdots + \alpha_m \cdot T(a_m) \in T(\mathcal{A}), \tag{2.2.2.13}$$

and so indeed $T(\mathcal{A})$ spans $\mathrm{Im}(T)$, as desired. ■

[a] Why?

This result has a number of important corollaries.

Corollary 2.2.2.14 Let V and W be vector spaces and $T : V \to W$ be a linear-transformation. Then, if V and W are finite-

dimensional with the same dimension, then the following are equivalent.

(i). T is injective.
(ii). T is surjective.
(iii). T is bijective.

R Warning: This is *false* in infinite-dimensions—see the following counter-example.

Proof. Suppose that V and W are finite-dimensional with the same dimension.

$((i) \Rightarrow (ii))$ Suppose that T is injective. Then, $\text{Ker}(T) = 0$, and so $\dim(\text{Ker}(T)) = 0$, and so $\dim(V) = \dim(\text{Im}(T))$. As we are assuming $\dim(V) = \dim(W)$, it follows that $\dim(W) = \dim(\text{Im}(T))$, and hence $W = \text{Im}(T)$, that is, T is surjective.

$((ii) \Rightarrow (iii))$ Suppose that T is surjective. Then, $\text{Im}(T) = W$, an so $\dim(\text{Im}(T)) = \dim(W) = \dim(V)$. As $\dim(V)$ is finite, we can subtract this from the equation $\dim(V) = \dim(\text{Ker}(T))+ \dim(\text{Im}(T))$ to obtain $0 = \dim(\text{Ker}(T))$, and hence $\text{Ker}(T) = 0$, and hence T is injective. We already knew it was surjective, and so T is bijective.

$((iii) \Rightarrow (i))$ This is immediate from the definition of bijectivity. ■

▪ **Example 2.2.2.15 — A surjective linear operator that is not injective** Define $D\colon \mathbb{R}[x] \to \mathbb{R}[x]$ by $D(p) := p'$.

Exercise 2.2.2.16 Check that D is surjective but not injective.

R Note that this does not contradict the preceding corollary as this vector space is infinite-dimensional.

We mentioned three particularly important applications of bases: they allow us to define linear-transformations (Theorem 2.2.25), they allow us to define dimension (Definition 2.2.1.20), and they allow us to define coordinates. We've covered the first two. The third, however, we postpone until the next chapter.

2.3 Summary

Though you should likely know a higher percentage of the material than in the previous chapter, there are again some things that can safely be skipped on a first study (rank of $\mathbb{K}$-modules, for example). For convenience, we again list some of the big concepts in this chapter you really need to know.

(i). The definition of span (Theorem 2.1.2.1) and spanning (Definition 2.1.2.5).
(ii). The definition of linear-independence (Definition 2.1.3.1).
(iii). The definition of basis (Definition 2.2.1).
(iv). Every linearly-independent set can be 'enlarged' to a basis and every spanning set can be 'shrunk' to a basis (Proposition 2.2.17).
(v). One may define linear-transformations by specifying what it does to a basis (Theorem 2.2.25).
(vi). The definition of dimension (Definition 2.2.1.20).
(vii). The Rank-Nullity Theorem (Theorem 2.2.2.2).
(viii). Linear-transformations between vector spaces of the same dimension are injective iff they are surjective iff tey are bijective (Corollary 2.2.2.14).

3. Coordinates, column vectors, and matrices

We now turn to the second important use of bases: coordinates.

3.1 Coordinates, vectors, and column vectors

Definition 3.1.1 — Coordinates (of a vector) Let V be a $\mathbb{K}$-module, let $\mathcal{B}$ be a basis of V, let $v \in V$, and write

$$v = \sum_{b \in \mathcal{B}} v^b \cdot b \tag{3.1.2}$$

for unique $v^b \in \mathbb{K}$. Then, the ***coordinates*** of v with respect to the basis $\mathcal{B}$, $[v]_{\mathcal{B}}$, are defined by

$$[v]_{\mathcal{B}} := \langle v^b : b \in \mathcal{B} \rangle \in \mathbb{K}^{\mathcal{B}}. \tag{3.1.3}$$

R Recall that (Definition A.3.1.6 and Exercise A.3.1.12) this is suggestive notation for what is technically a function $\mathcal{B} \ni b \mapsto v^b \in \mathbb{K}$. Thinking of things like this, however, is often not helpful—for example, we usually don't think of sequences as being functions

on $\mathbb{N}$, even though that's exactly what they are. In this case, I like to think of $\langle v^b : b \in \mathcal{B}\}$ as a list of scalars indexed by elements in the basis. If $\mathcal{B}$ is finite, this list is often written as a *column vector*—see the following remark.

R In this level of generality, it is a bit difficult to understand, so let us consider the important special case in which $\mathcal{B}$ is *finite*. Write $\mathcal{B} = \{b_1, \dots, b_d\}$. As $\mathcal{B}$ is a basis, there are unique $v^1, \dots, v^d \in \mathbb{K}$ such that

$$v = v^1 \cdot b_1 + \cdots + v^d \cdot b_d. \tag{3.1.4}$$

Then, the coordinates of v are given by the column vector

$$[v]_{\mathcal{B}} := \begin{bmatrix} v^1 \\ \vdots \\ v^d \end{bmatrix} \in \mathbb{K}^d. \tag{3.1.5}$$

Note that, when we do this, it is implicit that the first coordinate corresponds to the coefficient of b_1, etc.. Thus, if someone said instead to take the coordinates with respect to "$\{b_2, b_1, b_3, \dots, b_d\}$", at least in terms of the notation, it is implicit that the first coordinate now corresponds to the coefficient of b_2, the second coordinate now corresponds to the coefficient of b_1, etc., and so in this case one would instead write

$$[v]_{\mathcal{B}} := \begin{bmatrix} v^2 \\ v^1 \\ v^3 \\ \vdots \\ v^d \end{bmatrix} \in \mathbb{K}^d. \tag{3.1.6}$$

Thus, if we are working in a vector space V, a *choice of basis* $\mathcal{B}$ allows us to assign column vectors to all vectors in V.[1] It turns out that this is an isomorphism[2], at least in finite dimensions.

Proposition 3.1.7 — $[\cdot]_{\mathcal{B}}$ is linear and injective (and surjective in finite dimensions) Let V be a $\mathbb{K}$-module, and let $\mathcal{B}$ be a basis of V. Then,

$$V \ni v \mapsto [v]_{\mathcal{B}} \in \mathbb{K}^{\mathcal{B}} \tag{3.1.8}$$

is linear and injective with image

$$\left\{ \langle v^b : b \in \mathcal{B} \rangle : v^b = 0 \text{ for cofinitely many } b \in \mathcal{B}. \right\}. \tag{3.1.9}$$

R In particular, if $\mathcal{B}$ is finite (with $|\mathcal{B}| = d$), this map is surjective, and so this gives an *isomorphism* $V \to \mathbb{K}^d$ onto $\mathbb{K}^d$.

R Explicitly, that this map is linear means that

$$[v_1 + v_2]_{\mathcal{B}} = [v_1]_{\mathcal{B}} + [v_2]_{\mathcal{B}} \tag{3.1.10}$$

and

$$[\alpha \cdot v]_{\mathcal{B}} = \alpha \cdot [v]_{\mathcal{B}}. \tag{3.1.11}$$

R Note that a corollary of this is that any two vector spaces with the same dimension are isomorphic. Thus, in this sense, vector spaces aren't terribly interesting.

[1] At least if $\mathcal{B}$ is finite—we can of course do essentially the same thing no matter the cardinality of $\mathcal{B}$, but calling an infinite list a "column vector" is slightly dubious.

[2] See Definition B.2.3 for the definition of isomorphism. In this context, "isomorphism" is effectively synonymous with "invertible linear map".

Proof. We first prove that it is in fact linear. Let $v_1, v_2 \in V$ and write

$$v_1 = v_1^{b_1} \cdot b_1 + \cdots + v_1^{b_m} \cdot b_m \tag{3.1.12}$$

and

$$v_2 = v_2^{b_1} \cdot b_1 + \cdots + v_2^{b_m} \cdot b_m, \tag{3.1.13}$$

so that

$$v_1 + v_2 = (v_1^{b_1} + v_2^{b_1}) \cdot b_1 + \cdots + (v_1^{b_m} + v_2^{b_m}) \cdot b_m. \tag{3.1.14}$$

$[v_1]_{\mathcal{B}}$ is the function $\mathcal{B} \to \mathbb{K}$ that sends b_k to $v_1^{b_k}$ and every other basis element to 0. Similarly for $[v_2]_{\mathcal{B}}$. Hence, $[v_1]_{\mathcal{B}} + [v_2]_{\mathcal{B}}$ is the function that sends b_k to $v_1^{b_k} + v_2^{b_k}$ (and everything else to 0). However, from (3.1.14), we see that this is exactly the same as $[v_1 + v_2]_{\mathcal{B}}$, as desired. Similarly, for $\alpha \in \mathbb{K}$, we have

$$\alpha \cdot v_1 = \alpha v_1^{b_1} \cdot b_1 + \cdots + \alpha v_1^{b_m} \cdot b_m, \tag{3.1.15}$$

which says that the $[\alpha \cdot v_1]_{\mathcal{B}}$ is the function $\mathcal{B} \to \mathbb{K}$ that sends b_k to $\alpha v_1^{b_k}$ (and everything else to 0). This, of course, is the same as the function $\alpha \cdot [v_1]_{\mathcal{B}}$, as desired.

We now check injectivity. As it is linear, it suffices to show that the kernel is 0. So, suppose that $[v]_{\mathcal{B}} = 0$. As, by definition, the coordinates are the coefficients of the basis elements when writing v as a linear-combination of elements of $\mathcal{B}$, if all the coordinates are 0, then v itself has to be 0, and so indeed the kernel vanishes. As for the image, if $\mathcal{B} \ni b \mapsto v^b \in \mathbb{K}$ is a function such that $v^b \neq 0$ for only finitely many $b \in \mathcal{B}$, we can enumerate those elements $\{b_1, \ldots, b_m\} \subseteq \mathcal{B}$ (that is, $v^b = 0$ unless $b \in \{b_1, \ldots, b_m\}$). Now, let us define

$$v := v^{b_1} \cdot b_1 + \cdots + v^{b_m} \cdot b_m. \tag{3.1.16}$$

By construction, we have that $[v]_{\mathcal{B}} = (b \mapsto v^b)$, as desired. ∎

So, given a choice of basis, we can associate column vectors to 'abstract' vectors. But what happens if the "abstract" vectors were

column vectors themselves? Fortunately, the answer is as nice as one could hope.

Proposition 3.1.17 — Coordinates of column vectors Let $v \in \mathbb{K}^d$, and let $\mathcal{S}$ denote the standard basis of $\mathbb{K}^d$. Then,

$$[v]_{\mathcal{S}} = v. \tag{3.1.18}$$

Proof. We leave this as an exercise.

Exercise 3.1.19 Prove the result yourself.

■

▪ **Example 3.1.20** Define $T\colon C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$ by

$$T(f) \coloneqq f'' + f. \tag{3.1.21}$$

Then,

$$\mathcal{B} \coloneqq \{x \mapsto \mathrm{e}^{\mathrm{i}x}, x \mapsto \mathrm{e}^{-\mathrm{i}x}\} \tag{3.1.22}$$

and

$$C \coloneqq \{x \mapsto \cos(x), x \mapsto \sin(x)\} \tag{3.1.23}$$

are both bases for $\mathrm{Ker}(T)$.

Using Euler's Formula

$$\mathrm{e}^{\mathrm{i}x} = \cos(x) + \mathrm{i}\sin(x), \tag{3.1.24}$$

we see that

$$[\mathrm{e}^{\mathrm{i}x}]_C = \begin{bmatrix} 1 \\ \mathrm{i} \end{bmatrix} \text{ and } [\mathrm{e}^{-\mathrm{i}x}]_C = \begin{bmatrix} 1 \\ -\mathrm{i} \end{bmatrix}.^a \tag{3.1.25}$$

Note that, if we had used the different order (first sin then cos), we would instead have

$$[\mathrm{e}^{\mathrm{i}x}]_C = \begin{bmatrix} \mathrm{i} \\ 1 \end{bmatrix} \text{ and } [\mathrm{e}^{-\mathrm{i}x}]_{\mathcal{B}} = \begin{bmatrix} -\mathrm{i} \\ 1 \end{bmatrix}. \tag{3.1.26}$$

Technically, the order doesn't really matter as the function $\mathcal{B} \to \mathbb{C}$ doesn't depend on this; however, in practice, we need to keep the order in mind because changing the order in which we write things implicitly changes the function from $\mathcal{B}$ to $\mathbb{C}$ we mean to indicate. Loosely speaking, while the mathematics doesn't care about the order, the notation does. If this technicality doesn't quite make sense, don't worry—I promise this is a subtle and unimportant detail.

Exercise 3.1.27 Compute $[\cos(x)]_{\mathcal{B}}$ and $[\sin(x)]_C$.

[a] Technically, I should be writing $x \mapsto e^{ix}$ and $x \mapsto e^{-ix}$, though being this pedantic all the time becomes tiresome. I trust you know what I mean and will make similar abuse of notation throughout.

3.2 Coordinates, linear-transformations, and matrices

We can also define the coordinates of linear-transformations. We just saw that the coordinates of a vector in an ('abstract') vector space is a column vector. On the other hand, it turns out that the coordinates of a linear-transformation is a *matrix*, and so first, I suppose, it would help to actually define what a matrix is.

3.2.1 Matrices

While there is a good chance you are already familiar with matrices, if you think about it, a priori, matrices are sort of an awkward thing. Put numbers in a rectangular grid? What? Why? Well, I think the best answer to this question is given by Theorem 3.2.2.1, the result that tells us how we actually associate matrices to linear-transformations. From a mathematician's perspective, it is linear-transformations that we care about a priori—we then care about matrices because they help us understand linear-transformations using the correspondence explained in Theorem 3.2.2.1. What a priori seems like an awkward definition is justified a posteriori because it makes Theorem 3.2.2.1 work. Of course, however, we can't actually state the correspondence

if we don't know what matrices are, which means we need to define them here.

We begin with some heuristic motivation. Let $T\colon V \to W$ be a linear-transformation between finite-dimensional vector spaces, and let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ and $C =: \{c_1, \ldots, c_e\}$ be bases for V and W respectively. Given $v \in V$, I can write

$$v = v^1 \cdot b_1 + \cdots + v^d \cdot b_d \tag{3.2.1.1}$$

for unique $v^j \in \mathbb{F}$. As we just learned, these are the *coordinates* of v with respect to the basis $\mathcal{B}$. Apply T to this equation, and use linearity to find

$$T(v) = v^1 \cdot T(b_1) + \cdots + v^d \cdot T(b_d). \tag{3.2.1.2}$$

Each $T(b_i) \in W$, and so for each $b_i \in \mathcal{B}$, we can write

$$T(b_i) = T^1{}_j \cdot c_1 + \cdots + T^e{}_i \cdot c_e \tag{3.2.1.3}$$

for unique $T^j{}_i \in \mathbb{F}$. Substituting this back into (3.2.1.2), we find

$$T(v) = \left(\sum_{i=1}^{d} v^i T^1{}_i\right) \cdot c_1 + \cdots + \left(\sum_{i=1}^{d} T^e{}_i\right) \cdot c_e. \tag{3.2.1.4}$$

From this, we see that the collection of scalars $\{T^j{}_i : 1 \leq i \leq d, 1 \leq j \leq e\}$ determines the linear-transformation T: using the above equation, if you hand me v, I can compute $T(v)$. This is where the idea of "putting numbers in a rectangular grid" comes from.

Definition 3.2.1.5 — Matrix Let $\mathbb{K}$ be a ring, and let m and n be sets. Then, an $m \times n$ ***matrix*** with entries in $\mathbb{K}$ is a function from $m \times n$ into $\mathbb{K}$.

Notation 3.2.1.6 If $A\colon m \times n \to \mathbb{K}$ is a matrix, we generally write $A^i{}_j := A(i,j)$. Often times you'll also see $A_{ij} := A(ij)$, but the former is quite advantageous, something that will likely only be obvious when you learn Penrose's abstract index notation for tensors.

If $n =: \{*\}$ is a singleton, we write $A^i := A^i{}_*$. Similarly, if $m =: \{*\}$ is a singleton, we write $A_j := A^*{}_j$.

R $\langle m, n\rangle$, often written $m\times n := \langle m, n\rangle$, is the ***dimension*** of A.

R Note that we do allow m and n to be *any set*. To obtain the case you are most likely familiar with where $m, n \in \mathbb{Z}^+$, we think of these as corresponding to the sets $\{1,\dots,m\}$ and $\{1,\dots,n\}$ respectively. Indeed, we will be sloppy and say that A is an $m \times n$ matrix even though we technically mean it is a $\{1,\dots,m\} \times \{1,\dots,n\}$ matrix.

R For convenience, if we ever say "Let A be an $m \times n$ matrix.", or something similar, without first stating what m and n are, it should be assumed that $m, n \in \mathbb{Z}^+$.

Notation 3.2.1.7 If m and n are finite and A is an $m \times n$ matrix, then it is customary to write

$$A =: \begin{bmatrix} A^1{}_1 & \cdots & A^i{}_n \\ \vdots & \ddots & \vdots \\ A^m{}_1 & \cdots & A^m{}_n \end{bmatrix}. \tag{3.2.1.8}$$

When we do so, we shall freely use the English language to discuss A without necessarily defining every term first. For example, it should be clear that "the top-right entry" is

referring to $A^i{}_j$, and that "the third row is above the fourth row", etc..

Definition 3.2.1.9 — Rows and columns Let $\mathbb{K}$ be a ring, let m and n be sets, and let A be an $m \times n$ matrix.

(i). For $i \in M$, the i^{th} ***row*** of A, $A^i{}_\cdot$, is the $1 \times n$ matrix $N \ni j \mapsto A^i{}_j$.

(ii). For $j \in N$, the j^{th} ***column*** of A, $A^\cdot{}_j$, is the $m \times 1$ matrix $M \ni i \mapsto A^i{}_j$.

R In particular, you should commit to memory the fact that the superscript indicates the *row* and the subscript indicates the *column*.

Definition 3.2.1.10 — Matrix addition Let $\mathbb{K}$ be a ring, let m and n be sets, and let A and B be $m \times n$ matrices with entries in $\mathbb{K}$. Then, the ***sum***, $A + B$, is defined by

$$[A + B]^i{}_j := A^i{}_j + B^i{}_j. \tag{3.2.1.11}$$

Matrix addition was easy. Matrix multiplication, however, not so much. Before our 'official' definition of matrices, we briefly explained how one associates a matrix to a linear-transformation (given a choice of bases). We would like our definition of matrix multiplication to correspond to *composition* of linear-transformations. That is, if you compose linear-transformations and taken the corresponding matrix, you should get the same result as if you first took the corresponding matrices and multiplied them. So, let's investigate what such a definition might look like.

Recall (3.2.1.4):

$$T(v) = \left(\sum_{i=1}^{d} v^i T^1{}_i\right) \cdot c_1 + \cdots + \left(\sum_{i=1}^{d} T^e{}_i\right) \cdot c_e. \tag{3.2.1.12}$$

Now, if U is another vector space with basis $\mathcal{A} =: \{a_1, \ldots, a_c\}$ and $S\colon U \to V$ is another linear-transformation, the analogous equation for S looks like

$$S(u) = \left(\sum_{h=1}^{c} u^h S^1{}_h\right) \cdot b_1 + \cdots + \left(\sum_{h=1}^{c} u^h S^d{}_h\right) b_d \qquad (3.2.1.13)$$

Taking $v = S(u)$ in (3.2.1.12), so that

$$v^j = \sum_{h=1}^{c} u^h S^j{}_h, \qquad (3.2.1.14)$$

it becomes

$$T(S(u)) = \left(\sum_{h=1}^{c} u^h \left(\sum_{i=1}^{d} S^i{}_h T^1{}_i\right)\right) + \cdots + \left(\sum_{h=1}^{c} u^h \left(\sum_{i=1}^{d} S^i{}_h T^e{}_i\right)\right) \cdot c_e.$$

From this, we can read off that the $\langle j, h\rangle$ entry is

$$\sum_{i=1}^{d} S^i{}_h T^j{}_i\,. \qquad (3.2.1.15)$$

R The notation is perhaps a bit hard to parse, but the idea is quite easy. (3.2.1.12) tells us how to read off the matrix of a linear-transformation. As we are interested in the matrix associated to $T \circ S$, we compute $T \circ S$ in essentially the only way possible using these equations, and read off the relevant coefficients.

This yields the following definition.

Definition 3.2.1.16 — Matrix multiplication Let $\mathbb{K}$ be a ring; let m, n, and o be sets, let A be an $m \times n$ matrix with entries in $\mathbb{K}$, and let B be an $n \times o$ matrix with entries in $\mathbb{K}$. Then, A and B are ***multipliable*** iff for every $\langle i, k\rangle \in m \times o$,

$$\left\{j \in n : A^i{}_j B^j{}_k \neq 0\right\} \qquad (3.2.1.17)$$

is a finite set, in which case the ***product*** of A and B, AB, is defined by

$$[AB]^i{}_k := \sum_{j\in n} B^j{}_k A^i{}_j. \tag{3.2.1.18}$$

R Warning: Note the order of $B^j{}_k$ and $A^i{}_j$. Of course, this won't matter if $\mathbb{K}$ is commutative, but in general it makes a big difference. For example, matrices would not define linear-transformations if we didn't do this! (See Proposition 3.2.1.80 for an elaboration on this. This is relevant again for similar reasons in Theorem 3.2.2.1 and Proposition 3.2.2.12.)

R Warning: Not all authors define it this way and instead use $A^i{}_j B^{jk}$ in the definition instead of $B^j{}_k A^i{}_j$. This admittedly makes the definition more natural, but it breaks things later on. In order to remedy these "broken" things, one has to work with the opposite ring (Definition A.4.27) $\mathbb{K}^{\mathrm{op}}$ in places, which can make the theory quite messy.

R Note that, in order to multiply A and B, the number of columns of A has to be equal to the number of rows of B. Furthermore, AB is an $m \times o$ matrix. Heuristically, you can think of this as

$$(m \times n) \cdot (n \times o) = m \times o. \tag{3.2.1.19}$$

R The definition of multipliable is defined the way it is so that the sum in (3.2.1.18) makes sense.

R Note how awkward this definition is from a naive perspective. Think about this: if you went up to a high school student, showed them how to add matrices, and then asked them how they think matrices should be multiplied, what do you think they would say?

Unless they already knew the answer (or were particularly clever), not this! Most likely, they probably would have guessed something like

$$[AB]^i{}_j \coloneqq A^i{}_j B^i{}_j, \tag{3.2.1.20}$$

that is, simply 'componentwise multiplication', which of course would require that they be of the same dimension. Nevertheless, the definition (3.2.1.18) is the right one. The sense in which it is "right" is made precise in Proposition 3.2.2.12 (this result essentially says that multiplication of matrices corresponds to composition of linear-transformations).

What follows is another way of thinking of matrix multiplication.

Proposition 3.2.1.21 Let $\mathbb{K}$ be a ring; let m, n, and o be sets, and let A and B be multipliable matrices of respective dimensions $m \times n$ and $n \times o$.

(i).

$$[AB]^{\cdot}{}_i = A[B^{\cdot}{}_i] \tag{3.2.1.22}$$

(ii).

$$[AB]^k{}_{\cdot} = [A^k{}_{\cdot}]B. \tag{3.2.1.23}$$

R (i) says that column i of AB can be computed by multiplying column i of B on the left by A.

Dually, (ii) says that column k of AB can be computed by multiplying row k of A on the right by B.

R The first, after writing B in terms of its columns, looks something like

$$\begin{aligned} AB &= A\begin{bmatrix} B^{\cdot}{}_1 & \cdots & B^{\cdot}{}_o \end{bmatrix} \\ &= \begin{bmatrix} AB^{\cdot}{}_1 & \cdots & AB^{\cdot}{}_o \end{bmatrix}. \end{aligned} \tag{3.2.1.24}$$

On the other hand, the second, after writing A in terms of its row, looks something like

$$AB = \begin{bmatrix} A^1{}_\cdot \\ \vdots \\ A^m{}_\cdot \end{bmatrix} B = \begin{bmatrix} A^1{}_\cdot B \\ \vdots \\ A^m{}_\cdot B \end{bmatrix}. \tag{3.2.1.25}$$

I very much remember these by thinking that matrix multiplication 'distributes' over columns on the left and over rows on the right.

For what it's worth, I most often find it easiest to think of matrix multiplication as in (i), that is, as "distributing" over the columns on the left.

Proof. We leave this as an exercise.

Exercise 3.2.1.26 Prove this yourself.

■

In case B happens to be a column vector, there is yet another way to think of matrix multiplication, namely, as a linear-combination of the columns of A.

Proposition 3.2.1.27 Let $\mathbb{K}$ be a ring, let A be an $m \times n$ matrix with entries in $\mathbb{K}$, and let

$$v =: \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \in \mathbb{K}^n. \tag{3.2.1.28}$$

Then,

$$Av = v^1 \cdot A^\cdot{}_1 + \cdots + v^n \cdot A^\cdot{}_n. \tag{3.2.1.29}$$

For what it's worth, in practice, I often compute the product of matrices by combining this with (i) of

Proposition 3.2.1.21: I use Proposition 3.2.1.21 to reduce the problem to computing a matrix times a column vector, and then I use this result to compute that simpler product.

R Of course, there is an exact 'dual' result involving rows, though we refrain from presenting it here, as, though not strictly necessary, it is more appropriately understood using the concept of a *dual space*, which we have not yet discussed (I also personally find it slightly less intuitive.) In brief, however, it says that wB is a linear-combination of the rows of B, where w is a row vector.[a]

[a] Row vectors should almost always be thought of as elements of the dual space of $\mathbb{K}^d$.

Proof. We leave this as an exercise.

Exercise 3.2.1.30 Prove this yourself.

■

We now present some trivial but necessary terminology.

Definition 3.2.1.31 Let $\mathbb{K}$ be a ring, and m and n be sets, and let A be an $m \times n$ matrix with entries in $\mathbb{K}$.

(i). A is ***square*** iff $m = n$.
(ii). A is ***diagonal*** iff A is square and $A^i{}_j = 0$ for $i \neq j$.
(iii). A is ***upper-triangular*** iff A is square, m is preordered, and $A^i{}_j = 0$ for $i > j$.
(iv). A is ***strictly upper-triangular*** iff A is square, m is preordered, and $A^i{}_j = 0$ for $i \geq j$.
(v). A is ***lower-triangular*** iff A is square, m is preordered, and $A^i{}_j = 0$ for $i < j$.
(vi). A is ***strictly lower-triangular*** iff A is square, m is preordered, and $A^i{}_j = 0$ for $i \geq j$.

(vii). For A square, the ***diagonal*** of A is the function $M \ni i \mapsto A^i{}_i \in \mathbb{K}$.

R These terms get their names from the following pictures.

Diagonal: $\begin{bmatrix} * & 0 & \cdots & 0 \\ 0 & * & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{bmatrix}$

Upper-triangular: $\begin{bmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{bmatrix}$

Strictly upper-triangular: $\begin{bmatrix} 0 & * & \cdots & * \\ 0 & 0 & \cdots & * \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$

Lower-triangular: $\begin{bmatrix} * & 0 & \cdots & 0 \\ * & * & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ * & * & \cdots & * \end{bmatrix}$

Strictly lower-triangular: $\begin{bmatrix} 0 & 0 & \cdots & 0 \\ * & 0 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ * & * & \cdots & 0 \end{bmatrix}$

Unfortunately, if the indexing sets of the matrices are infinite, then we won't be able to multiply any two matrices. On the other hand, if m is a finite set, the set of all such square matrices can be made into a ring.

Proposition 3.2.1.33 — Matrix ring Let $\mathbb{K}$ be a ring, let m be a finite set, and define

$$\text{Matrix}_m(\mathbb{K}) := \mathbb{K}^{m\times m}.^a \tag{3.2.1.34}$$

Then, $\text{Matrix}_m(\mathbb{K})$ is a ring with matrix addition and multiplication, additive identity the 0 matrix, and multiplicative identity the diagonal matrix with 1s on the diagonal.

R The multiplicative identity, that is, the diagonal matrix with 1s on the diagonal has a name: surprise surprise, the $m \times m$ ***identity matrix***

$$\text{id}_{m\times m} := \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix}. \tag{3.2.1.35}$$

R Though it will not be a ring (because we can't multiply them), we may also write $\text{Matrix}_{m\times n}(\mathbb{K})$ for the set of all $m \times n$ matrices with entries in $\mathbb{K}$.

[a] Recall (Definition A.3.9) that $\mathbb{K}^{m\times m}$ is the set of all functions from $m \times m$ into $\mathbb{K}$, that is, the set of all $m \times m$ matrices with entries in $\mathbb{K}$.

Proof. We leave this as an exercise.

Exercise 3.2.1.36 Prove this yourself.

■

This allows us to return to a counter-example we mentioned before in Exercise 1.1.35.

▪ **Example 3.2.1.37 — A scaling of a linear map that is not linear** Define $\mathbb{K} := \text{Matrix}_2(\mathbb{C})$ and $V := \mathbb{C}^2$ regarded as a $\mathbb{K}$-module with scaling operation given by matrix multiplication. Of course, $\text{id}_V \in \text{End}_{\mathbb{K}\text{-}\mathbf{Mod}}(V)$ is $\mathbb{K}$-linear, but yet, for

example,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \mathrm{id}_V = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \tag{3.2.1.38}$$

is not $\mathbb{K}$-linear.[a]

Exercise 3.2.1.39 Check that this is in fact not $\mathbb{K}$-linear.

R Note however that it is $\mathbb{C}$-*linear*.

R Indeed, it at first might be a bit confusing to think of matrices as "scalars" (and in fact, this is one reason why that term is not so often used in the context of general R-modules), but, as you can verify, it most certainly satisfies the axioms of a $\mathbb{K}$-module.

[a] Here, we are being sloppy and writing a matrix when in fact we mean the $\mathbb{C}$-linear-transformation defined by the matrix. We will make similar abuses of notation throughout.

We could very well now return to our original objective of studying coordinates of linear-transformations, and if you would like to do so now, feel free to skip to Subsection 3.2.2. However, this is a set of linear algebra notes after all, and as such, it would be a bit perverse to make no mention of systems of equations, matrices, and row reduction at all, and given that I'm going to discuss it at all, it makes sense to do so here, in the subsection on matrices.[3]

Row reduction

My understanding is that, historically, the motivation for the study of what we know understand to be linear algebra was the systematic solution of linear systems of equations. Indeed, even today, this is how the subject is introduced at an elementary level. While for us

[3] Shoe-horning this into, e.g., a section on eigenvalues wouldn't make much sense, no?

the solution of linear systems is not exactly the raison d'être of linear algebra, this does very much serve to illustrate the concepts.

The first step in applying techniques of linear algebra to solve systems of linear equations is to encode the system of linear equations in a matrix. For example, we associate to the linear system of equations

$$\begin{aligned} 3x_1 \qquad\qquad & -5x_3 = 2 && \text{(3.2.1.40a)} \\ -4x_1 \qquad +2x_2 \qquad & +3x_3 = -1 && \text{(3.2.1.40b)} \end{aligned}$$

the matrix

$$\left[\begin{array}{ccc|c} 3 & 0 & -5 & 2 \\ -4 & 2 & 3 & -1 \end{array}\right]. \tag{3.2.1.41}$$

(This is really nothing more than eliminating unnecessary symbols—it is clear how one can determine the original equations from the matrix itself.) Sometimes, we will only be interested in the ***coefficient matrix***.

$$\begin{bmatrix} 3 & 0 & -5 \\ -4 & 2 & 3 \end{bmatrix}. \tag{3.2.1.42}$$

If we every need to distinguish between the two, the matrix in (3.2.1.41) will be referred to as the ***augmented matrix*** associated to the system. (Incidentally, the vertical bar in this matrix only serves to remind us that the far right-hand column corresponds to the constants on the right-hand side of the equations (3.2.1.40) instead of coefficients of a fourth variable as one might have guessed if the bar weren't there.)

If we were working with the original equations, we would perform blah blah blah algebraic operations in an attempt to isolate each of the "variables" x_1, x_2, and x_3. As it turns out, there are three fundamental operations that one can perform on the equations to solve any system (at least when the coefficients come from a field): we can reorder the equations, we can scale any equation by a unit[4], and we can add any scalar multiple of one equation to a different one. These three operations have the property that they do not change the set of solutions, and furthermore, every system can be solved using these

[4]A scalar that has an inverse—see Definition A.4.16.

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

three operations.[5] In terms of the matrix, we can swap any two rows, we can scale any row by a unit, and we can add any multiple of one row to a different one. The method of solution using these three operations is essentially algorithmic, with the goal being to "reduce" the matrix to *reduced echelon form*.

Definition 3.2.1.43 — Row operation Let $\mathbb{K}$ be a ring, and let m and n be sets. A ***row operation*** is a function $\text{Matrix}_{m\times n}(\mathbb{K}) \to \text{Matrix}_{m\times n}(\mathbb{K})$ that is one of the following.

(i). For $i_1, i_2 \in m$,

$$A \mapsto \text{Row}_{i_1\leftrightarrow i_2}(A), \tag{3.2.1.44}$$

where $\text{Row}_{i_1\leftrightarrow i_2}(A)$ is the same as A except its i_1 row is the i_2 row of A and its i_2 row is the i_1 of A.[a]

(ii). For $i_0 \in m$ and $\alpha \in \mathbb{K}^\times$,

$$A \mapsto \text{Row}_{i_0\to\alpha i_0}(A), \tag{3.2.1.45}$$

where $\text{Row}_{i_0\to\alpha i_0}(A)$ is the same as A except its i_0 row is the i_0 row of A scaled by α.

(iii). For $i_1, i_2 \in m$ distinct and $\alpha \in \mathbb{K}$,

$$A \mapsto \text{Row}_{i_1\to i_1+\alpha i_2}(A), \tag{3.2.1.46}$$

where $\text{Row}_{i_1\to i_1+\alpha i_2}(A)$ is the same as A except its i_1 row is the i_1 row of A plus the i_2 row of A scaled by α.

[a] That is, $\text{Row}_{i_1\leftrightarrow i_2}(A)$ is the matrix obtained from A by 'swapping' the i_1 and i_2 rows of A.

Definition 3.2.1.47 — Row-equivalence Let $\mathbb{K}$ be a ring, let m and n be sets, and let A and B be $m \times n$ matrices. Then,

[5] Note how some operations you might try are 'valid' but yet will change the set of solutions. For example, while it is true that if $x = 2$, then $x^2 = 4$, these two equations do not have the same set of solutions—the latter also has the solution $x = -2$.

A and B are ***row-equivalent*** iff there is a finite sequence of matrices $C_1, \ldots, C_l$ such that

(i). $A = C_1$;
(ii). $B = C_l$; and
(iii). C_{k+1} is obtained from C_k by a row operation for $1 \leq k < l$.

R In other words, two matrices are row-equivalent iff one can be obtained from the other by application of a finite number of row operations.

R The whole point of this is that row operations don't change the solution set that the matrix corresponds to. Thus, if two matrices are row-equivalent, then the systems of equations they correspond to have the same set of solutions. In fact, it turns out that the converse is true: two matrices are row-equivalent iff the systems of equations they correspond to have the same set of solutions (over a division ring anyways). Using language we will learn shortly, we can say that two matrices are row-equivalent iff they have the same null-space.

Definition 3.2.1.48 — Reduced echelon form Let $\mathbb{K}$ be a ring and let A be an $m \times n$ matrix with entries in $\mathbb{K}$. Then, A is in ***reduced echelon form*** iff

(i). all nonzero rows are above any rows of all zeros;
(ii). each leading entry is in a column to the right of the leading entry of the row above it;
(iii). all entries in a column below a leading entry are zero;
(iv). the leading entry in each nonzero row is 1; and
(v). each leading 1 is the only nonzero entry in its column.

R An entry is the ***leading entry*** of its row iff it is the first nonzero entry in that row.

R For what its worth, a matrix satisfying (i)–(iii) is said to be in ***echelon form***.

The significance of reduced echelon form is that one can immediately read off the solution set. For example, the following matrix is in reduced echelon form

$$\left[\begin{array}{ccccc|c} 1 & 0 & 5 & 2 & 0 & -7 \\ 0 & 1 & -4 & 3 & 0 & 5 \\ 0 & 0 & 0 & 0 & 1 & 5 \end{array}\right], \tag{3.2.1.49}$$

whence we see that its solution set of the corresponding system of equations is described by[6]

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = x_3 \begin{bmatrix} -5 \\ 4 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -2 \\ -3 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} -7 \\ 5 \\ 0 \\ 0 \\ 5 \end{bmatrix}. \tag{3.2.1.50}$$

Given your original matrix A then, the strategy is try to *row-reduce*, that is, apply row operations to A, to find a row-equivalent matrix in reduced echelon form. We can then read off the solution set from the matrix in reduced echelon form as above, and this is in turn the solution set for our original matrix A. The following result says that this is always possible (and more).

Proposition 3.2.1.51 Let $\mathbb{F}$ be a division ring and let A be an $m \times n$ matrix with entries in $\mathbb{F}$. Then, there is a unique matrix in reduced echelon form that is row equivalent to A.

R This matrix in reduced echelon form is the ***reduced echelon form*** of A.

R Note this obviously fails if $\mathbb{F}$ is not a division ring. For example, consider the 1×1 matrix in $\mathbb{Z}$, $\begin{bmatrix} 2 & 1 \end{bmatrix}$—

[6] See Example 3.2.1.54 below if you don't see how to read this off immediately from the matrix.

there is no way to make this entry into a 1 using only integers.

Proof. We leave this as an exercise.

Exercise 3.2.1.52 Prove the result yourself.

■

The uniqueness of the reduced echelon form allows us to make some definitions.

Definition 3.2.1.53 — Pivots and free-variables Let $\mathbb{F}$ be a division ring, let A be an $m \times n$ matrix with entries in $\mathbb{F}$, and let R be the reduced echelon form of A.

(i). An entry of A is a ***pivot*** iff the corresponding entry of R is a leading 1.

(ii). A column of A is a ***pivot column*** iff that columns contains a pivot.

(iii). A column of A is a ***free-variable column*** iff it is not a pivot column.

R In the context of systems of equations, the columns of A (except perhaps the last one if A is the augmented matrix of a system) often correspond to variables. We then say that a variable is a ***free-variable*** iff the column it corresponds to is a free-variable column.

For example, the free-variables of (3.2.1.49) are x_3 and x_4.

■ **Example 3.2.1.54** Above, we simply read off the set of solutions (3.2.1.50) from the corresponding matrix in reduced echelon form in (3.2.1.49). At the time, we glossed over how to make that jump, essentially because we wanted to stress how easy reduced echelon form makes this. The catch, of course, is that it's only very easy *after* you've learned how to

do it. So, in case this is not so familiar, let's look at this in more detail.

I'm going to explain this in two ways. The first time, I'm going to be more explicit and give more detail. This is so you understand what's going on and why the "jump" we make is legitimate. This is fine for understanding, but in practice you won't want to go through that much work every time, so the second time through I'll explain what you want to do in practice after you understand what's going on (in particular, you're not going to want to waste your time working with any actual equations).

Recall that the we had an augmented matrix corresponding to a system of equations in reduced echelon form,

$$\left[\begin{array}{ccccc|c} 1 & 0 & 5 & 2 & 0 & -7 \\ 0 & 1 & -4 & 3 & 0 & 5 \\ 0 & 0 & 0 & 0 & 1 & 5 \end{array}\right], \tag{3.2.1.55}$$

and the objective was to determine the set of solutions. First of all, note that this matrix corresponds to the following system of equations.

$$x_1 \quad +5x_3 \quad +2x_4 \quad = -7 \tag{3.2.1.56a}$$

$$x_2 \quad -4x_3 \quad +3x_4 \quad = 5 \tag{3.2.1.56b}$$

$$x_5 \quad = 5 \tag{3.2.1.56c}$$

Looking at the above, we see that we can vary x_3 and x_4 "freely", that is, we can choose any values for them we like, and the above equations will dictate the values of the other variables.[a] For convenience, let us move those variables to the other side. Furthermore, for the purpose of having 5 equations and 5 unknowns (instead of 3 equations and 5 unknowns), let us introduce the tautological equations $x_3 = x_3$ and $x_4 = x_4$— it will become more apparent why this is helpful for us now in

a moment.

$$x_1 = -5x_3 - 2x_4 - 7 \quad \text{(3.2.1.57a)}$$
$$x_2 = 4x_3 - 3x_4 + 5 \quad \text{(3.2.1.57b)}$$
$$x_3 = x_3 \quad \text{(3.2.1.57c)}$$
$$x_4 = x_4 \quad \text{(3.2.1.57d)}$$
$$x_5 = 5 \quad \text{(3.2.1.57e)}$$

Alternatively, using column-vectors, we can write this as

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = x_3 \begin{bmatrix} -5 \\ 4 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -2 \\ -3 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} -7 \\ 5 \\ 0 \\ 0 \\ 5 \end{bmatrix}. \quad \text{(3.2.1.58)}$$

So that was the easier-to-understand but less efficient way. The trick to figuring this out fast is as follows. First of all, forget the constant terms—pretend they aren't there—they will come back in the final solution as the far right-hand column vector in (3.2.1.58). Then, for each free variable, set that free variable equal to 1, set the other free variables equal to 0, and solve for the remaining nonfree variables. This will give you a column vector of scalars, and those column-vectors correspond to the column-vectors appearing in (3.2.1.58) with coefficients x_3 and x_4.

For example, first set $x_3 = 1$ and $x_4 = 0$. Solving for the other three,[b] we find $x_1 = -5$, $x_2 = 4$, and $x_5 = 0$ (note with practice you can easily read this off from the matrix without every writing down any equations). This yields the column-vector

$$\begin{bmatrix} -5 \\ 4 \\ 1 \\ 0 \\ 0 \end{bmatrix}. \quad \text{(3.2.1.59)}$$

Similarly, setting $x_4 = 1$ and $x_3 = 0$, we find that $x_1 = -2$, $x_2 = -3$, and $x_5 = 0$, giving us the column-vector

$$\begin{bmatrix} -2 \\ -3 \\ 0 \\ 1 \\ 0 \end{bmatrix}. \tag{3.2.1.60}$$

To determine what the 'constant' column-vector should be, set all the free variables to 0. In this case, we see this gives the solution

$$\begin{bmatrix} -7 \\ 5 \\ 0 \\ 0 \\ 5 \end{bmatrix}. \tag{3.2.1.61}$$

Putting this together gives the same result as in (3.2.1.58).

Thus, in brief: the coefficient column-vector of the free variable x_k is the solution you find when you set that free variable equal to 1 and the other free variables equal to 0, and the constant column-vector is the solution you find when you set all free variables equal to 0.

[a] These aren't necessarily the only two variables with this property, but given the form of the equations, they are the easiest ones to work with in this regard (all the other variables appear in just one equation).

[b] Remember we are pretending the constants aren't there!

There is another important application of row-reduction besides solving equations, namely, computing inverses of matrices. To best understand how this works, I think it is easiest to think in terms of *elementary matrices*.

Theorem 3.2.1.62 — Elementary matrices. Let $\mathbb{K}$ be a ring, let $m, n \in \mathbb{N}$, and let $R\colon \text{Matrix}_{m\times n}(\mathbb{K}) \to \text{Matrix}_{m\times n}(\mathbb{K})$ be a row operation. Then, there is an $m \times m$ matrix E_R, unique if $\mathbb{K}$ is a division-ring, such that

$$E_R A = R(A) \tag{3.2.1.63}$$

for all $A \in \text{Matrix}_{m\times n}(\mathbb{K})$.

Furthermore, explicitly,

$$E_R = R(\text{id}_{m\times m}) \tag{3.2.1.64}$$

R In other words, you could do the row operation directly, or you could just multiply on the left by E_R.

R (3.2.1.64) says that E_R is obtained by applying the given row operation to the identity matrix. So, for example, for $m = 3$,[a]

$$E_{2\to 2-5\cdot 3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{bmatrix}. \tag{3.2.1.65}$$

[a] Note how this doesn't depend on n—the same elementary matrix would work for any number of columns.

Proof. We leave this as an exercise.

Exercise 3.2.1.66 Prove the result yourself.

■

Elementary matrices can be used to prove that an algorithm to compute inverses of matrices actually works. That algorithm is called ***Gauss-Jordan elimination***.[7]

[7] Some people actually use this term to refer more generally to just "row reduction".

Theorem 3.2.1.67 — Gauss-Jordan elimination. Let $\mathbb{F}$ be a division ring, let A be an invertible $m \times m$ matrix with entries in $\mathbb{F}$ so that it's reduced echelon form is $\mathrm{id}_{m\times m}$, and let $R\colon \mathrm{Matrix}_m(\mathbb{F}) \to \mathrm{Matrix}_m(\mathbb{F})$ be any composition of row operations such that $R(A) = \mathrm{id}_{m\times m}$. Then, $A^{-1} = R(\mathrm{id}_{m\times m})$.

R In practice, this is done as follows. Take the matrix A and "augment" it with the identity matrix $\mathrm{id}_{m\times m}$ to form an $m \times 2m$ matrix as follows.

$$\left[A|\,\mathrm{id}_{m\times m}\right]\Big| \tag{3.2.1.68}$$

Now, row-reduce this matrix until you obtain the identity matrix on the left—what pops out on the right is A^{-1}:

$$\left[\mathrm{id}_{m\times m}\,|A^{-1}\right]\Big| \tag{3.2.1.69}$$

Proof. Write $R = R_1 \circ \cdots \circ R_n$, where $R_1, \ldots, R_n$ are the individual row operations appearing in the composition R. For convenience, let us write

$$E_R \coloneqq E_{R_1} \cdots E_{R_n}, \tag{3.2.1.70}$$

where E_{R_k} is the elementary matrix corresponding to the row operation R_k. The defining result of elementary matrices (Theorem 3.2.1.62) implies that

$$R(A) = E_R A. \tag{3.2.1.71}$$

On the other hand, by hypothesis, $R(A) = \mathrm{id}_{m\times m}$, and hence

$$E_R A = \mathrm{id}_{m\times m}\,. \tag{3.2.1.72}$$

Exercise 3.2.1.73 e have just shown that E_R is a left-inverse of A. Show that it is also a right-inverse, so that we can conclude $A^{-1} = E_R$.

R Warning: In general, if A and B are matrices such that $AB = \mathrm{id}_{m\times m}$, one *cannot* conclude that $A^{-1} = B$.

However, Theorem 3.2.1.62 also said that each $E_{R_k} = R_k(\mathrm{id}_{m\times m})$. It follows that $E_R = R(\mathrm{id}_{m\times m})$, and hence

$$A^{-1} = E_R = R(\mathrm{id}_{m\times m}). \tag{3.2.1.74}$$

■

▪ **Example 3.2.1.75** Suppose we would like to find the inverse of the matrix

$$\frac{1}{2}\begin{bmatrix} 1 & 2 & 0 \\ -1 & 1 & -1 \\ -3 & 2 & 0 \end{bmatrix}. \tag{3.2.1.76}$$

Using Gauss-Jordan elimination, we form the 3×6 augmented matrix

$$\left[\begin{array}{ccc|ccc} \frac{1}{2} & 1 & 0 & 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & 0 & 1 & 0 \\ -\frac{3}{2} & 1 & 0 & 0 & 0 & 1 \end{array}\right]. \tag{3.2.1.77}$$

Row reducing this to row-echelon form as if it were any old 3×6 matrix, we find

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & \frac{3}{4} & 0 & \frac{1}{4} \\ 0 & 0 & 1 & \frac{1}{4} & -2 & \frac{3}{4} \end{array}\right]. \tag{3.2.1.78}$$

Thus, we can read off

$$A^{-1} = \frac{1}{4}\begin{bmatrix} 2 & 0 & -2 \\ 3 & 0 & 4 \\ 1 & -8 & 3 \end{bmatrix}. \tag{3.2.1.79}$$

Matrix linear-transformations

One of the most important facts about matrices is that they define linear-transformations. In fact, in a sense we will make precise later (Theorem 3.2.2.1), *every* linear-transformation can be thought of as matrix multiplication.

Proposition 3.2.1.80 — Linear-transformation of a matrix Let $\mathbb{K}$ be a ring, let m and n be finite sets, and let A be an $m \times n$ matrix with entries in $\mathbb{K}$. Then, $T_A \colon \mathbb{K}^n \to \mathbb{K}^m$, the ***linear-transformation defined by*** A, defined by

$$T_A(x) \coloneqq Ax. \tag{3.2.1.81}$$

is a linear-transformation.

R In one of the remarks in the definition of matrix multiplication (Definition 3.2.1.16), we mentioned that the order of ${B^k}_j$ and ${A^i}_j$ is not what one might have expected, and that the motivation for doing things in this odd way is justified in part because this proposition would not be true otherwise. To see why, it is probably best to just examine the proof.

R Here, we are thinking of $x \in \mathbb{K}^n$ as a $n \times 1$ matrix and Ax is matrix multiplication.

Proof. We leave addition as an exercise.

Exercise 3.2.1.82 Verify that T_A preserves addition.

Let $x \in \mathbb{K}^n$, let $\alpha \in \mathbb{K}$, and let $1 \leq i \leq m$. Then,

$$\begin{aligned} T_A(\alpha \cdot x)^i &:= [A(\alpha x)]^i := \sum_{k=1}^{n} [\alpha x]^k A^i{}_k \\ &= \alpha \sum_{k=1}^{d} x^k A^i{}_k =: \alpha [Ax]^i = \alpha T_A(x)^i \\ &= [\alpha \cdot T_A(x)]^i, \end{aligned} \tag{3.2.1.83}$$

and so $T_A(\alpha \cdot x) = \alpha \cdot T_A(x)$, as desired. ■

R It could be instructive to see how this would have gone if we hadn't used the definition of matrix multiplication we did. Using the other possible definition, we would have found

$$\begin{aligned} T_A(\alpha \cdot x)^i := [A(\alpha x)]^i &= \sum_{k=1}^{n} A^i{}_k [\alpha x]^k \\ &= \sum_{k=1}^{n} A^i{}_k \alpha x^k. \end{aligned} \tag{3.2.1.84}$$

But now we have no way of pulling the α out front (if the ring is not commutative) to write this as $\alpha \cdot Ax$!.

Definition 3.2.1.85 — Null space and column space Let A be a matrix and T_A the associative linear-transformation. The ***null space*** of A, $\mathrm{Null}(A)$, is defined by

$$\mathrm{Null}(A) := \mathrm{Ker}(T_A). \tag{3.2.1.86}$$

The ***column space*** of A, $\mathrm{Col}(A)$, is defined by

$$\mathrm{Col}(A) := \mathrm{Im}(T_A). \tag{3.2.1.87}$$

R The term "column space" comes from the fact that $\mathrm{Col}(A)$ is the span of the columns of A—see the following result.

Proposition 3.2.1.88 Let A be a matrix. Then, $\mathrm{Col}(A)$ is the span of the columns of A.

Proof. We leave this as an exercise.

Exercise 3.2.1.89 Prove the result.

■

Matrix linear-transformations play quite an important role in the theory. For one, they are pedagogically useful as they provide an abundance of examples that tend not to scare students. But more fundamentally, in a sense to be described (Theorem 3.2.2.1), every linear-transformation between finite-dimensional vector spaces is given by a matrix linear-transformation. As they do play such an important role, it is important to know (i) when such linear-transformations are injective, surjective, and bijective; and (ii) how to calculate their kernel and image.

We begin with the first.

Proposition 3.2.1.90 — Injectivity and surjectivity of matrix linear-transformations Let $\mathbb{K}$ be a ring, let $d, e \in \mathbb{N}$, let A be an $e \times d$ matrix with entries in $\mathbb{K}$, and let $T_A \colon \mathbb{K}^d \to \mathbb{K}^e$ denote the corresponding linear-transformation. Then,

(i). T_A is injective iff the columns of A are linearly-independent in W;
(ii). T_A is surjective iff the columns of A are span W; and
(iii). T_A is bijective iff the columns of A are a basis of W.

Proof. We leave this as an exercise.

Exercise 3.2.1.91 Prove this yourself.

■

We now turn to the issue of "computing" the kernel and image of a matrix linear-transformation. In this context, "computing" is best

understood as "to find a basis for". As a first step, it will help to know the *dimension* of the space of solutions.

Proposition 3.2.1.92 Let $\mathbb{F}$ be a division ring, let A be an $e \times d$ matrix with entries in $\mathbb{F}$, and let $T_A \colon \mathbb{F}^d \to \mathbb{F}^e$ be the corresponding linear-transformation. Then,

(i). $\dim(\mathrm{Ker}(T_A))$ is the number of free-variables of A; and
(ii). $\dim(\mathrm{Im}(T_A))$ is the number of pivots of A.

R In fact, a basis for $\mathrm{Im}(T_A)$ is given by the pivot columns of A. It's not much harder to find a basis for the kernel, but it is harder to describe that basis in general, so we instead relegate an explanation of this to the following example.

Proof. We leave this as an exercise.

Exercise 3.2.1.93 Prove the result yourself.

■

▪ **Example 3.2.1.94 — Bases for the null space and column space of a matrix** [a] Suppose you are interested in solving the following system of equations.

$$\begin{aligned} 3x_2 - 6x_3 + 6x_4 + 4x_5 &= 0 \quad (3.2.1.95a)\\ 3x_1 - 7x_2 + 8x_3 - 5x_4 + 8x_5 &= 0 \quad (3.2.1.95b)\\ 3x_1 - 9x_2 + 12x_3 - 9x_4 + 6x_5 &= 0 \quad (3.2.1.95c) \end{aligned}$$

The corresponding coefficient matrix is

$$A := \begin{bmatrix} 0 & 3 & -6 & 6 & 4 \\ 3 & -7 & 8 & -5 & 8 \\ 3 & -9 & 12 & -9 & 6 \end{bmatrix}, \qquad (3.2.1.96)$$

whose reduced echelon form is

$$\begin{bmatrix} 1 & 0 & -2 & 3 & 0 \\ 0 & 1 & -2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.2.1.97}$$

From this, we can immediately read off the set of solutions:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = x_3 \begin{bmatrix} 2 \\ 2 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -3 \\ -2 \\ 0 \\ 1 \\ 0 \end{bmatrix}. \tag{3.2.1.98}$$

Thus,

$$\left\{ \begin{bmatrix} 2 \\ 2 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ -2 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\} \tag{3.2.1.99}$$

is a basis of the space of solutions, that is, the kernel of the linear-transformation defined by A. We can also read off a basis for the image of this linear-transformation by looking at the pivot columns of A^b

$$\left\{ \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ -7 \\ -9 \end{bmatrix} \begin{bmatrix} 4 \\ 8 \\ 6 \end{bmatrix} \right\}. \tag{3.2.1.100}$$

We explain how we came up with (3.2.1.98) as this process can be generalized to find a basis for the null-space of any matrix. After putting the matrix in reduced echelon form, list the free-variables (in this case, x_3 and x_4). Then, for each free-variable, set that free-variable equal to 1, the remaining free-variables equal to 0, and solve for the 'nonfree' variables. Thus, for the first vector in (3.2.1.99), we set $x_3 = 1$ and

$x_4 = 0$, and for the second vector in (3.2.1.99) we set $x_4 = 1$ and $x_3 = 0$. As we get one basis element for each free-variable, this procedure makes it 'obvious' that the dimension of the null-space is precisely the number of free-variables.

[a] Taken from [C L12]. Because I'm too lazy to find my own numbers that work out nice.

[b] When you do this, it is important to look back to the *original matrix*, not the row-reduced matrix.

3.2.2 Coordinates of linear-transformations

Having take a (longer than necessary) diversion investigating matrices, let us return to the original objective: *coordinates of linear-transformations*.

Theorem 3.2.2.1 — Coordinates (of a linear-transformation). Let V and W be $\mathbb{K}$-modules, let $\mathcal{B} =: \{b_1, \dots, b_d\}$ and $C =: \{c_1, \dots, c_e\}$ be bases for V and W respectively, and let $T : V \to W$ be a linear-transformation. Then, there is a unique $e \times d$ matrix, $[T]_{C \leftarrow \mathcal{B}}$, the ***coordinates*** of T with respect to the bases $\mathcal{B}$ and C, such that

$$[T(v)]_C = [T]_{C \leftarrow \mathcal{B}} [v]_{\mathcal{B}} \tag{3.2.2.2}$$

for all $v \in V$.

Furthermore, explicitly

$$[T]_{C \leftarrow \mathcal{B}} = \begin{bmatrix} [T(b_1)]_C & \cdots & [T(b_d)]_C \end{bmatrix}. \tag{3.2.2.3}$$

R In words, $[T]_{C \leftarrow \mathcal{B}}$ is computed column-by-column, with the k^{th} column itself being computed by applying T to b_k and taking coordinates of the result with respect to C: $[T(b_k)]_C$.

R The notation is supposed to be suggestive:

$$C = (C \leftarrow \mathcal{B})(\mathcal{B}). \tag{3.2.2.4}$$

I found this particularly helpful for remembering how to compute change of basis matrices (Definition 3.2.2.48) when I was first learning linear algebra—before I realized this, I was always forgetting whether it should be $[b_k]_C$ or $[c_k]_{\mathcal{B}}$.

R In case $\mathcal{B} = C$, we may write

$$[T]_{\mathcal{B}} \coloneqq [T]_{\mathcal{B}\leftarrow\mathcal{B}} \tag{3.2.2.5}$$

R You can't really generalize this to infinite bases because the matrix product in (3.2.2.2) will not make sense in general.

R We may sometimes instead speak of the ***matrix*** of T with respect to a basis instead of the "coordinates" of T, though it means the same thing.

Proof. Step 1: Define $[T]_{C\leftarrow\mathcal{B}}$
Define

$$[T]_{C\leftarrow\mathcal{B}} = \begin{bmatrix}[T(b_1)]_C & \cdots & [T(b_d)]_C\end{bmatrix}. \tag{3.2.2.6}$$

Step 2: Verify $[T]_{C\leftarrow\mathcal{B}}$ satisfies the desired properties
Let $v \in V$ and write

$$v = v^1 \cdot b_1 + \cdots + v^d \cdot b_d \tag{3.2.2.7}$$

for unique $v^k \in \mathbb{K}$, so that

$$[v]_{\mathcal{B}} \coloneqq \begin{bmatrix} v^1 \\ \vdots \\ v^d \end{bmatrix}. \tag{3.2.2.8}$$

Then, for $1 \leq i \leq e$,

$$\begin{aligned}
[[T]_{C\leftarrow\mathcal{B}}[v]_{\mathcal{B}}]^i &:= \sum_{k=1}^{d} [v]_{\mathcal{B}}{}^k [T]_{C\leftarrow\mathcal{B}}{}^i{}_k \\
&:= \sum_{k=1}^{d} v^k [T(b_k)]_C{}^i \\
&= \left[T\left(\sum_{k=1}^{d} v^k \cdot b_k \right) \right]_C^i \\
&= [T(v)]_C{}^i
\end{aligned} \tag{3.2.2.9}$$

Hence,

$$[T]_{C\leftarrow\mathcal{B}}[v]_{\mathcal{B}} = [T(v)]_C, \tag{3.2.2.10}$$

as desired.

Step 3: Prove uniqueness
Let M be another $e \times d$ matrix with entries in $\mathbb{K}$ such that

$$[T(v)]_C = M[v]_{\mathcal{B}} \tag{3.2.2.11}$$

for all $v \in V$. Taking $v = b_k$, the left-hand side becomes $[T(b_k)]_C$ and the right-hand side becomes the k^{th} column of M, so that indeed $M = [T]_{C\leftarrow\mathcal{B}}$. ■

We mentioned before when defining matrix multiplication that its seemingly awkward definition was made precisely so that matrix multiplication corresponds exactly to composition of linear-transformations. It is about time we make this statement precise.

Proposition 3.2.2.12 — Coordinates of a composition is the product of the coordinates Let U, V, and W be $\mathbb{K}$-modules; let $\mathcal{A}$, $\mathcal{B}$, and C be finite bases for U, V, and W respectively; and let $S\colon U \to V$ and $T\colon V \to W$ be linear-

transformations. Then,

$$[T \circ S]_{C \leftarrow \mathcal{A}} = [T]_{C \leftarrow \mathcal{B}} [S]_{\mathcal{B} \leftarrow \mathcal{A}}. \tag{3.2.2.13}$$

R Besides just giving us conceptual clarity into the meaning of matrix multiplication, this can be useful for proving things. For example, this makes proving that matrix multiplication is associative trivial—it's associative because composition is associative. Compare this with the masochistic methods of using the definition Definition 3.2.1.16.

Nothing is special about associativity of course. The same logic can be used to show that essentially all algebraic properties satisfies by composition of linear-transformations is always satisfies by matrix multiplication (e.g. matrix multiplication distributes over addition, etc.).

Proof. By definition, $[T \circ S]_{C \leftarrow \mathcal{A}}$ is the unique matrix such that

$$[T(S(v))]_C = [T \circ S]_{C \leftarrow \mathcal{A}} [v]_{\mathcal{A}} \tag{3.2.2.14}$$

for all $v \in V$. Thus, to demonstrate the equality (3.2.2.13), it suffices to show that the matrix $[T]_{C \leftarrow \mathcal{B}} [S]_{\mathcal{B} \leftarrow \mathcal{A}}$ also satisfies this property.

So, let $v \in V$. We then have

$$\begin{aligned} [T]_{C \leftarrow \mathcal{B}} [S]_{\mathcal{B} \leftarrow \mathcal{A}} [v]_{\mathcal{A}} &= [T]_{C \leftarrow \mathcal{B}} [S(v)]_{\mathcal{B}} \\ &= [T(S(v))]_{\mathcal{A}}, \end{aligned} \tag{3.2.2.15}$$

as desired. ∎

Similarly, as $V \ni v \mapsto [v]_{\mathcal{B}} \in \mathbb{K}^d$ was an isomorphism, so to is $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V,W) \ni T \mapsto [T]_{C\leftarrow\mathcal{B}} \in \mathrm{Matrix}_{m\times n}(\mathbb{K})$. However, in this case, we need $\mathbb{K}$ to be commutative.[8]

Proposition 3.2.2.16 — $[\cdot]_{C\leftarrow\mathcal{B}}$ is an isomorphism Let $\mathbb{K}$ be a cring, let V and W be $\mathbb{K}$-modules, and let $\mathcal{B}$ and C be bases for V and W respectively with respective finite cardinalities d and e. Then,

$$\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V,W) \ni T \mapsto [T]_{C\leftarrow\mathcal{B}} \in \mathrm{Matrix}_{e\times d}(\mathbb{K})$$

is an isomorphism of $\mathbb{K}$-modules.

R In particular, we have that

$$[T_1 + T_2]_{C\leftarrow\mathcal{B}} = [T_1]_{C\leftarrow\mathcal{B}} + [T_2]_{C\leftarrow\mathcal{B}} \quad (3.2.2.17)$$

and

$$[\alpha \cdot T]_{C\leftarrow\mathcal{B}} = \alpha \cdot [T]_{C\leftarrow\mathcal{B}}. \quad (3.2.2.18)$$

R If $\mathbb{K}$ weren't commutative, this instead would only be an isomorphism of groups.

Proof. We first check linearity. To show that $[T_1 + T_2]_{C\leftarrow\mathcal{B}} = [T_1]_{C\leftarrow\mathcal{B}} + [T_2]_{C\leftarrow\mathcal{B}}$, we wish to show that the matrix $[T_1]_{C\leftarrow\mathcal{B}} + [T_2]_{C\leftarrow\mathcal{B}}$ satisfies the property that uniquely defines $[T_1 + T_2]_{C\leftarrow\mathcal{B}}$. That is, we would like to show that

$$[[T_1 + T_2](v)]_C = ([T_1]_{C\leftarrow\mathcal{B}} + [T_2]_{C\leftarrow\mathcal{B}})\,[v]_{\mathcal{B}} \quad (3.2.2.19)$$

for all $v \in V$. However, using the definition of coordinates of a linear-transformation and the fact that we already know that taking coordinates of vectors (Proposition 3.1.7) is linear, we

[8] Otherwise $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V,W)$ won't have the structure of a $\mathbb{K}$-module—see Subsection 1.1.1. That said, they would still be isomorphic as commutative groups (with respect to addition).

see that

$$\begin{aligned}([T_1]_{C\leftarrow\mathcal{B}} + [T_2]_{C\leftarrow\mathcal{B}})\,[v]_{\mathcal{B}} \\ = [T_1(v)]_C + [T_2(v)]_C \\ = [T_1(v) + T_2(v)]_C = [[T_1 + T_2](v)]_C,\end{aligned} \tag{3.2.2.20}$$

as desired.

Exercise 3.2.2.21 Show that $[\cdot]_{C\leftarrow\mathcal{B}}$ preserves scaling.

As for injectivity, suppose that $[T]_{C\leftarrow\mathcal{B}} = 0$. It follows that

$$[T(v)]_C = [T]_{C\leftarrow\mathcal{B}}[v]_{\mathcal{B}} = 0 \tag{3.2.2.22}$$

for all $v \in V$, and so, as $[\cdot]_C$ is injective, $T(v) = 0$ for all $v \in V$, that is, $T = 0$.

As for surjectivity, let $A \in \text{Matrix}_{e\times d}(\mathbb{K})$. By virtue of Theorem 2.2.25, there is a unique linear-transformation $T : V \to W$ such that

$$T(b_i) = \sum_{j=1}^{e} A^j{}_i \cdot c_j \tag{3.2.2.23}$$

for all $1 \leq i \leq d$. We claim that $[T]_{C\leftarrow\mathcal{B}} = A$. Again, to do this, we show that A satisfies the unique defining property of $[T]_{C\leftarrow\mathcal{B}}$. So, let $v \in V$, and write

$$v = v^1 \cdot b_1 + \cdots + v^d \cdot b_d, \tag{3.2.2.24}$$

so that

$$[v]_{\mathcal{B}} = \begin{bmatrix} v^1 \\ \vdots \\ v^d \end{bmatrix}. \tag{3.2.2.25}$$

We then have that

$$[A[v]_{\mathcal{B}}]^j := \sum_{i=1}^{d} v^i A^j{}_i. \tag{3.2.2.26}$$

On the other hand,

$$T(v) = \sum_{i=1}^{d} v^i T(v_i) = \sum_{i=1}^{d} \sum_{j=1}^{e} v^i A^j{}_i \cdot c_j. \tag{3.2.2.27}$$

From (3.2.2.26), we see that the j entry of $A[v]_{\mathcal{B}}$ is

$$\sum_{i=1}^{d} v^i A^j{}_i. \tag{3.2.2.28}$$

From (3.2.2.27), we see that the j coordinate of $T(v)$ is the same thing, and hence

$$[T(v)]_{\mathcal{C}} = A[v]_{\mathcal{B}}, \tag{3.2.2.29}$$

as desired. ■

We saw in Proposition 3.1.17 that the coordinates of a column vector (with respect to the standard basis) is just the original column vector itself. As you likely expected, we have an analogous result for matrices.

Proposition 3.2.2.30 — Coordinates of matrices Let $\mathbb{K}$ be a ring, let A be an $m \times n$ matrix with entries in $\mathbb{K}$, let $T_A : \mathbb{K}^n \to \mathbb{K}^m$ be the associated linear-transformation, and denote by $\mathcal{S}$ and $\mathcal{T}$ respectively the standard bases of $\mathbb{K}^m$ and $\mathbb{K}^n$. Then,

$$[T_A]_{\mathcal{T} \leftarrow \mathcal{S}} = A. \tag{3.2.2.31}$$

Proof. We leave this as an exercise.

Exercise 3.2.2.32 Prove the result yourself.

■

▪ **Example 3.2.2.33 — Rotation** Let $\theta \in (-\pi, \pi]$ and let $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be rotation counter-clockwise about the origin by θ. Let $\mathcal{S} =: \{e_1, e_2\}$ be the standard basis of $\mathbb{R}^2$. Using some trig, we see that

$$T(e_1) = \begin{bmatrix} \cos(\theta) \\ \sin(\theta) \end{bmatrix} \text{ and } T(e_2) = \begin{bmatrix} -\sin(\theta) \\ \cos(\theta) \end{bmatrix}. \quad (3.2.2.34)$$

Thus, we have that

$$\begin{aligned} [T]_{\mathcal{S}\leftarrow\mathcal{S}} &= \begin{bmatrix} [T(e_1)]_{\mathcal{S}} & [T(e_2)]_{\mathcal{S}} \end{bmatrix} \\ &= \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}. \end{aligned} \quad (3.2.2.35)$$

Exercise 3.2.2.36 The zero vector space, 0, has a unique basis, the empty-set. Furthermore, there is a unique linear-transformation $0 \to 0$. What are the coordinates of this unique linear-transformation with respect to the basis that is the empty-set?

R Hint: It's the empty matrix.

R The inclusion of this is in part a joke. Think about why this is true if you like, but I wouldn't waste too much time on it.

▪ **Example 3.2.2.37** Let V be the kernel of the linear transformation $C^\infty(\mathbb{R}) \ni f \mapsto f'' + f \in C^\infty(\mathbb{R})$, so that two bases of V are given by $\mathcal{B} := \{x \mapsto e^{ix}, x \mapsto e^{-ix}$ and $C := \{x \mapsto \cos(x), x \mapsto \sin(x)\}$—see Example 3.1.20, and define $D\colon V \to V$ by $D(f) := f'$.

Exercise 3.2.2.38 Check indeed that if $f \in V$, then $f' \in V$.

We compute $[D]_{C\leftarrow\mathcal{B}}$. We have that

$$D(e^{ix}) = ie^{ix} = i\cos(x) - \sin(x) \tag{3.2.2.39}$$

and

$$D(e^{-ix}) = -ie^{-ix} = -i\cos(x) - \sin(x), \tag{3.2.2.40}$$

so that

$$[D(e^{ix})]]_C = \begin{bmatrix} i \\ -1 \end{bmatrix} \text{ and } [D(e^{-ix})]_C = \begin{bmatrix} -i \\ -1 \end{bmatrix}, \tag{3.2.2.41}$$

and hence

$$\begin{aligned} [D]_{C\leftarrow\mathcal{B}} &= \begin{bmatrix} [D(e^{ix})]_C & [D(e^{-ix})]_C \end{bmatrix} \\ &= \begin{bmatrix} i & -i \\ -1 & -1 \end{bmatrix}. \end{aligned} \tag{3.2.2.42}$$

Exercise 3.2.2.43

(i). Compute $[D]_{\mathcal{B}\leftarrow\mathcal{B}}$.
(ii). Compute $[D]_{\mathcal{B}\leftarrow C}$.
(iii). Compute $[D]_{C\leftarrow C}$.

▪ **Example 3.2.2.44** As in Example 1.1.54, define $\mathbb{F} := \mathbb{Q}$, $V := \mathbb{Q}(\sqrt{2})$, fix $a, b \in \mathbb{Q}$, and define $T\colon V \to V$ by

$$T(x) := (a + b\sqrt{2})x. \tag{3.2.2.45}$$

Define $\mathcal{B} := \{1, \sqrt{2}\}$.

Exercise 3.2.2.46 Check that $\mathcal{B}$ is a basis for V.

Let us compute $[T]_{\mathcal{B}\leftarrow\mathcal{B}}$. First of all, of course $T(1) = a + b\sqrt{2}$. On the other hand, $T(\sqrt{2}) = 2b + a\sqrt{2}$. Hence,

$$[T]_{\mathcal{B}\leftarrow\mathcal{B}} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}. \tag{3.2.2.47}$$

There is an important special case of the coordinates of a linear transformation: *change-of-basis matrices*.

Definition 3.2.2.48 — Change of basis matrix Let V be a $\mathbb{K}$-module, and let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two well-ordered bases of V. Then, the ***change-of-basis matrix*** from $\mathcal{B}_1$ to $\mathcal{B}_2$ is defined to be

$$[\mathrm{id}]_{\mathcal{B}_2\leftarrow\mathcal{B}_1}. \tag{3.2.2.49}$$

R If you look at the defining equation (3.2.2.3), the change-of-basis matrix from $\mathcal{B}_1$ to $\mathcal{B}_2$ is the unique matrix such that

$$[v]_{\mathcal{B}_2} = [\mathrm{id}]_{\mathcal{B}_2\leftarrow\mathcal{B}_1}[v]_{\mathcal{B}_1} \tag{3.2.2.50}$$

for all $v \in V$. Hopefully it is clear from this why this is called a "change-of-basis" matrix.

R In other words, the change-of-basis matrix is just the coordinates of the identity linear-transformation with respect to the two bases.

▪ **Example 3.2.2.51** Using the two well-ordered bases $\mathcal{B} := \{e^{ix}, e^{-ix}\}$ and $C := \{\cos(x), \sin(x)\}$ again of the vector space appearing in Example 3.1.20, we see from (3.1.25) that the change-of-basis matrix from $\mathcal{B}$ to C is given by

$$[\mathrm{id}]_{C\leftarrow\mathcal{B}} = \begin{bmatrix} [e^{ix}]_C & [e^{-ix}]_{\mathcal{B}} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{3.2.2.52}$$

Finally, coordinates of linear-transformations make it easy to compute the dimension of the vector-space of linear-transformations.

Proposition 3.2.2.53 Let V and W be a vector spaces over a field $\mathbb{F}$. Then,

$$\dim(\mathrm{Mor}_{\mathbf{Vect}_{\mathbb{F}}}(V,W)) = \dim(V)\dim(W). \qquad (3.2.2.54)$$

R Recall that (Subsection 1.1.1) morphism sets need not be modules over the ground ring if that ground ring is not commutative. Thus, we need to take the ground division ring to be a field for this result.

Proof. We leave this as an exercise.

Exercise 3.2.2.55 Prove the result.

R Hint: Use coordinates of linear-transformations to observe that the dimension of $\mathrm{Mor}_{\mathbf{Vect}_{\mathbb{F}}}(V,W)$ is the same as the dimension of some vector space of matrices. Then, compute the dimension of the vector space of matrices by exhibiting an explicit basis.

■

3.3 Summary

We met the first big theorem of elementary linear algebra in the last chapter (the Rank-Nullity Theorem (Theorem 2.2.2.2)). In this chapter, we came to what I would consider the second big milestone: the connection between the abstract and the concrete. This connection is given by *coordinates*.

To define coordinates, however, one my first make a choice of *basis*—no basis, no coordinates. So, let V and W be (finite-

dimensional)[9] vector spaces with respective bases $\mathcal{B}$ and C. In what follows, $v \in V$ and $T\colon V \to W$ is a linear-transformation.

(i). Definition 3.1.1 tells us how to associate column vectors to 'abstract' vectors in a vector space—take $v \in V$, write v as a linear-combination of elements of $\mathcal{B}$, and read off the coefficients.

(ii). Theorem 3.2.2.1 tells us how to associate matrices to linear-transformations. It first defines the matrix implicitly by the condition

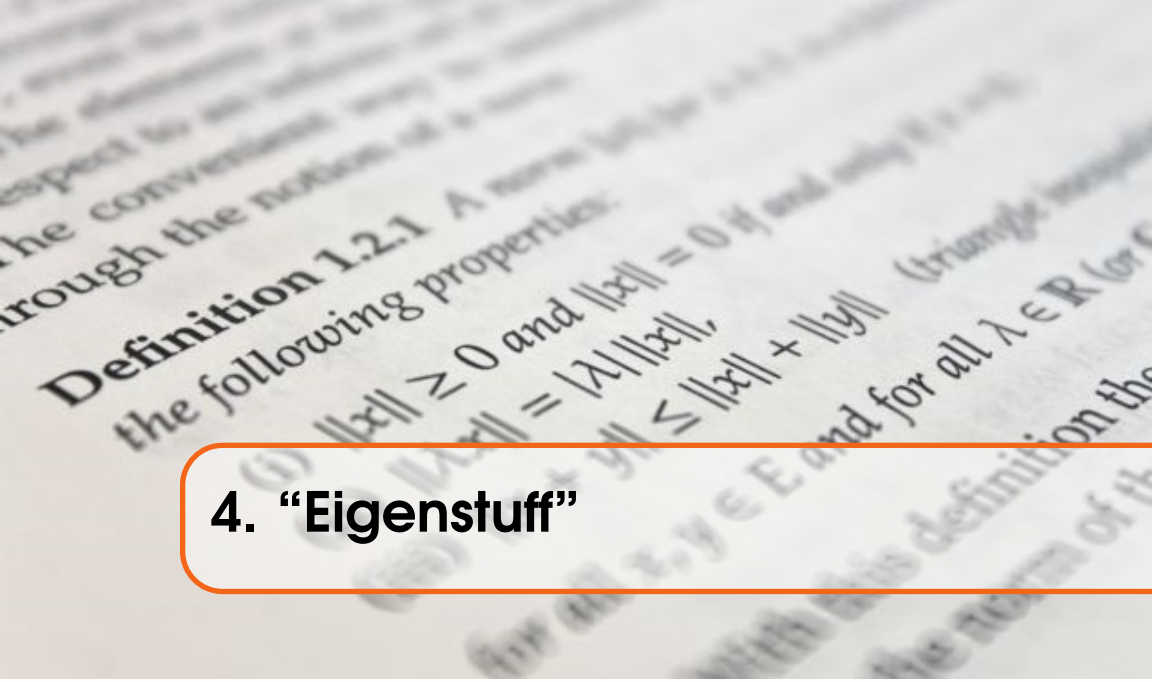
$$[T(v)]_C = [T]_{C \leftarrow \mathcal{B}}[v]_{\mathcal{B}}. \tag{3.3.1}$$

It also tells you how to explicitly compute this matrix: the k^{th} column is given by $[T(b_k)]_C$.

Finally, as this was our first 'official' introduction with matrices, we introduced basic definitions, notation, and terminology regarding them.

[9] Some of this will hold in infinite dimensions, but not all, and in any case, for us, the most important special case is by bar the finite-dimensional case.

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12



4. "Eigenstuff"

4.1 Motivation

As mentioned at the very beginning, linear algebra is the study of vector spaces. More accurately, it is the study of the *category* of vector spaces. Thus, not only are we interested in vector spaces, but we're also interested in studying linear-transformations. In fact, linear-transformations are arguably more important than the vector spaces themselves.

We saw in the last chapter that, given choice of bases, we can associate matrices to linear-transformations. This is incredibly useful as matrices are more concrete and amenable to (scary) things like computation. However, there isn't just one matrix associated to a linear-transformation, but you get one matrix for every choice of bases. Some of these matrices might be quite ugly, and others might be quite nice. The motivating objective for this chapter is to try to find basis in which the associated matrix is *nice*.

Perhaps the simplest matrix one might hope for is a *diagonal* matrix.[1] Let us investigate what it would require for our matrix to be diagonal.

[1] It turns out that one can almost, but not quite, do this. In any case, having this as an objective, even if it can't always be obtained, it sufficient for motivation.

So, let V be a finite-dimensional vector space, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ be a basis for V, and let $T\colon V \to V$ be a linear operator. Looking back to the defining theorem of $[T]_{\mathcal{B}\leftarrow\mathcal{B}}$ (Theorem 3.2.2.1), we see that the k^{th} column of this matrix is given by

$$[T(b_k)]_{\mathcal{B}}, \tag{4.1.1}$$

that is, the coordinates of the vector $T(b_k) \in V$ with respect to the basis $\mathcal{B}$. To compute these coordinates (Definition 3.1.1), we write $T(b_k)$ as a linear combination of the elements of $\mathcal{B}$:

$$T(b_k) = T^1{}_k\, b_1 + \cdots + T^d{}_k\, b_d, \tag{4.1.2}$$

so that

$$[T(b_k)]_{\mathcal{B}} = \begin{bmatrix} T^1{}_k \\ \vdots \\ T^d{}_k \end{bmatrix}. \tag{4.1.3}$$

Now, for a matrix to be diagonal, by definition, everything in the k^{th} column should vanish except for possibly the k^{th} entry in that column. Thus, as $[T(b_k)]_{\mathcal{B}}$ is the k^{th} column of $[T]_{\mathcal{B}\leftarrow\mathcal{B}}$, if this matrix is to be diagonal, we had better have that $T^l{}_k = 0$ for $l \neq k$. Plugging this back into (4.1.2), we find

$$T(b_k) = T^k{}_k\, b_k. \tag{4.1.4}$$

We have found the following.

> If $[T]_{\mathcal{B}\leftarrow\mathcal{B}}$ is to be a diagonal matrix, it had better be the case that $T(b_k)$ is a scalar multiple of b_k for all $b_k \in \mathcal{B}$.

It is thus of interest to find a basis consisting of vectors b such that $T(b)$ is a scalar multiple of b. Such vectors have a name: they are *eigenvectors* of T.[2]

4.2 Basic definitions

[2] By the way, in case it's not obvious, "eigenstuff" is a catch-all term I'm using as short-hand for "eigenvalues, eigenvectors, and eigenspaces".

Definition 4.2.1 — Eigenspaces, eigenvalues, and eigenvectors Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be linear, let $W \subseteq V$ be a nonzero subspace, and let $\lambda \in \mathbb{K}$. Then, W is a ***λ-eigenspace*** iff

(i). $T|_W = \lambda \operatorname{id}_W$; and
(ii). W is maximal with this property.

R Such a λ is referred to as an ***eigenvalue*** of T, and we write

$$\operatorname{Eig}(T) := \{\lambda \in \mathbb{K} : \lambda \text{ is an eigenvalue of } T.\}\ . \tag{4.2.2}$$

R Nonzero elements of W are ***eigenvectors*** of T with eigenvalue λ.

R Warning: The eigenspace is *not* the set of eigenvectors—we must have $0 \in W$ as W is a subspace, but, by definition, $0 \in W$ is forbidden from being an eigenvector.

R Warning: Eigenvalues need not be unique—see Example 4.2.13. On the other hand, they certainly will be for vector spaces—see Proposition 4.2.14.

Eigenvectors on the other hand are essentially never unique: any scalar multiple of an eigenvector is another eigenvector with the same eigenvalue (because eigenspaces are in particular subspaces).

R To clarify, (ii) means the following. If $U \subseteq V$ is a nonzero subspace with $U \supseteq W$ and such that $T|_U = \lambda \operatorname{id}_U$, then $U = W$.

R Recall that (Example 1.1.40) scaling by elements of $\mathbb{K}$ need not actually define a linear-transformation. Thus, it is implicit in this condition that $\lambda \operatorname{id}_W : W \to W$ is actually a linear-transformation. If V is a vector space, this will actually force λ to commute with everything in $\mathbb{K}$ (in which case scaling by λ defines a linear-transformation on all of V)—see Theorem 4.2.16.

R One reason to see we need the maximality condition is to get uniqueness of the eigenspace. For example, consider the linear-transformation $\mathbb{R}^2 \to \mathbb{R}^2$ defined by the matrix

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}. \tag{4.2.3}$$

Without the maximality condition, every nonzero subspace would be considered a 2-eigenspace. But that's silly. We want our definition to be so that, in this example, there is only one 2-eigenspace, namely all of $\mathbb{R}^2$.

R If we allowed $W = 0$, then we might have stupid things happening like every scalar being an eigenvalue of T. Thus, unless you're a fan of stupid things, you're going to want $W = 0$ here.

R The ***eigenspaces***, ***eigenvalues***, and ***eigenvectors*** of a matrix are respectively the eigenspaces, eigenvalues, and eigenvectors of the associated linear-transformation.

Before moving on, there is a common mistake that students make that we should clear up.

Eigen*vectors* cannot be 0. On the other hand, eigen*values* can be.

This is of course true just by definition. The reason we exclude the zero vector from being an eigenvector however is because we would always have $T(0) = \lambda \cdot 0$ for all $\lambda \in \mathbb{K}$, not a particularly interesting condition.

Our first order of business is to establish the uniqueness of eigenspaces, which will allow us in particular to utilize unambiguous notation to denote them.

Proposition 4.2.4 — Eigenspaces are unique Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be linear, let $\lambda \in \mathbb{K}$, and let $U, W \subseteq V$ be λ-eigenspaces of T. Then, $U = W$.

R We denote the unique λ-eigenspace of V by $\mathrm{Eig}_{\lambda,T}$. If T is clear from context, we may simply write $\mathrm{Eig}_\lambda := \mathrm{Eig}_{\lambda,T}$.

R If ever we write "$\mathrm{Eig}_{\lambda,T}$" without having explicitly said so, it should be assumed that λ is an eigenvalue of T.

R Warning: Though eigenvalues themselves may still not be unique—we may still have $\mathrm{Eig}_{\lambda,T} = \mathrm{Eig}_{\mu,T}$ for $\lambda \neq \mu$.

R Of course, λ-eigenspaces need not exist—this only says that, *if* they do exist, they must be unique.

R If $\mathbb{K}$ is a division ring (so that we can talk about dimension, then the ***geometric multiplicity*** of $\lambda \in \mathrm{Eig}(T)$ is $\dim(\mathrm{Eig}_\lambda)$.[a]

[a] Do *not* just say "multiplicity". This means something else—see Proposition 4.4.3.35.

Proof. $U + W$ is a subspace of V. Furthermore, for $u + w \in U + W$, with $u \in U$ and $w \in W$, we have

$$T(u + w) = T(u) + T(w) = \lambda u + \lambda w = \lambda(u + w), \quad (4.2.5)$$

and so $T|_{U+W} = \lambda\,\mathrm{id}_{U+W}$. As $U + W \supseteq U, W$, by maximality of eigenspaces, we have $U = U + W = W$. ∎

According to the definition, in order to show that λ is an eigenvalue, you have to find a nonzero subspace on which T acts by λ, and furthermore, is maximal with respect to this property. Having to check maximality by hand would be obnoxious. Fortunately, we have

the following result that gives a relatively simple sufficient condition for guaranteeing that λ be an eigenvalue.

Proposition 4.2.6 — Sufficient condition to be an eigenvalue Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be linear, and let $\lambda \in \mathbb{K}$. Then, if there is some nonzero subspace $W \subseteq V$ such that $T|_W = \lambda \operatorname{id}_W$, then λ is an eigenvalue.

Proof. Suppose that there is some nonzero subspace $W \subseteq V$ such that $T|_W = \lambda \operatorname{id}_W$. Define

$$\mathscr{W} := \{W \subseteq V : W \text{ a nonzero subspace such that } T|_W = \lambda \operatorname{id}_W .\}. \tag{4.2.7}$$

Exercise 4.2.8 Check that $\mathscr{W}$ is a partially-ordered set with respect to inclusion and satisfies the hypotheses of Zorn's Lemma.

By Zorn's Lemma, $\mathscr{W}$ has a maximal element, and so λ is an eigenvalue. ∎

In fact, eigenspaces aren't just maximal subspaces on which T acts by λ, but in fact they are *maximum* with this property.

Proposition 4.2.9 — Eigenspaces are maximum with their defining property Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be linear, let $W \subseteq V$ be a subspace, and let $\lambda \in \mathbb{K}$ be an eigenvalue of V. Then, if $T|_W = \lambda \operatorname{id}_W$, then $W \subseteq \operatorname{Eig}_\lambda$.

Proof. Suppose that $T|_W = \lambda \operatorname{id}_W$. Define

$$\mathscr{U} := \{U \subseteq V \text{ a subspace} : T|_U = \lambda \operatorname{id}_U\} \tag{4.2.10}$$

and

$$E := \sum_{U \in \mathscr{U}} U. \tag{4.2.11}$$

Every element in E can be written as a finite sum $u_1 + \cdots + u_m$ where $T(u_k) = \lambda u_k$ for each u_k, and so

$$T(u_1 + \cdots + u_m) = \lambda(u_1 + \cdots + u_m). \tag{4.2.12}$$

That is, $T|_E = \lambda \operatorname{id}_E$. E is maximal with this property, and hence $E = \operatorname{Eig}_\lambda$. Finally, note that $W \in \mathscr{U}$, and hence $W \subseteq E = \operatorname{Eig}_\lambda$. ∎

▪ **Example 4.2.13 — An eigenspace with infinitely many distinct eigenvalues** Define $V := \mathbb{Z}/2\mathbb{Z}$, regard it as a $\mathbb{K} := \mathbb{Z}$-module, and define $T := 0$. Then, of course $T|_V = 0 \operatorname{id}_V$, but also $T|_V = 2 \operatorname{id}_V$. (It is obviously maximal as this is the entire space!) Thus, $V \subseteq V$ is an eigenspace of T with eigenvalues $0, 2 \in \mathbb{K}$. Of course, 2 is not special—any even integer would have worked just as well, and so there are in fact infinitely many distinct eigenvalues!

Proposition 4.2.14 — Eigenvalues are unique (in vector spaces) Let V be a vector space and let $T : V \to V$ be linear. Then, if $\operatorname{Eig}_{\lambda,T} = \operatorname{Eig}_{\mu,T}$, it follows that $\lambda = \mu$.

Proof. Suppose that $\operatorname{Eig}_{\lambda,T} = \operatorname{Eig}_{\mu,T}$. There must be some nonzero $v \in \operatorname{Eig}_{\lambda,T} = \operatorname{Eig}_{\mu,T}$. It follows that

$$\lambda v = T(v) = \mu v, \tag{4.2.15}$$

and so $(\lambda - \mu)v = 0$. As $v \neq 0$ and the ground ring is a division ring, we must have that $\lambda - \mu = 0$, that is, $\lambda = \mu$. ∎

If you've seen eigenvalues and eigenvectors before, you'll note that this is similar, but not identical to how they are usually defined. The motivation for this slight deviation has to do with the fact that, even for vector spaces, the ground division ring $\mathbb{F}$ need not be commutative. In this case, we would like eigenvalues to define linear-transformations by scaling (for reasons we'll see in a moment), even if $\mathbb{K}$ itself is not

commutative. The definition as stated above *implies* that eigenvalues have to be central, and hence define linear-transformations by scaling. Thus, we don't have to put this condition into the definition by hand—in a sense, we get it for free.

Another advantage it has is that it places the emphasis on eigen*spaces* instead of eigen*vectors*. Eigenspaces are the more fundamental of the two concepts simply because they are unique—in general, there will be infinitely many eigenvectors with the same eigenvalue, and no one of them is more 'correct' than the other, whereas for eigen*spaces* there is no arbitrary choice to be made—there's only one thing to pick from. In any case, it would be good to know that our presentation is equivalent to the usual one.

Theorem 4.2.16. V be a vector space over a division ring $\mathbb{F}$, let $T\colon V \to V$ be linear, and let $\lambda \in \mathbb{F}$. Then,

(i). $\lambda \in \mathrm{Eig}(T)$ iff λ is central and there is some nonzero $v \in V$ such that $T(v) = \lambda v$, in which case v is an eigenvector of T with eigenvalue λ; and

(ii). if λ is an eigenvalue, then

$$\mathrm{Eig}_{\lambda,T} = \{v \in V : T(v) = \lambda v\} = \mathrm{Ker}(T - \lambda). \quad (4.2.17)$$

R Recall (Definition A.4.12) that for λ to be *central* means that λ commutes with everything. For example, in the quaternions $\mathbb{H}$, $\mathrm{i}, \mathrm{j}, \mathrm{k} \in \mathbb{H}$ are *not* central, though $1 \in \mathbb{H}$ is.

Of course, if $\mathbb{F}$ is commutative (that is, if $\mathbb{F}$ is a field), then everything is central, and may ignore this part of the result. Upon doing so, we obtain exactly the condition you are likely familiar with (assuming you've seen eigenvalues before, that is).

R Perhaps the most relevant fact for us about central elements is that scaling by them defines linear-transformations. That is, if $\alpha \in \mathbb{F}$ is central, then $V \ni v \mapsto \alpha \cdot v \in V$ is a linear-transformation.

R In particular, note that, if 0 is an eigenvalue, then its eigenspace is precisely $\mathrm{Ker}(T)$. Thus, T is injective iff 0 is *not* an eigenvalue.

Proof. (i) ($\Rightarrow$) Suppose that λ is an eigenvalue of T. As λ is an eigenvalue, there is a nonzero subspace $\mathrm{Eig}_\lambda \subseteq V$, such that $T(v) = \lambda v$ for all $v \in \mathrm{Eig}_\lambda$. In particular, there is *some* nonzero $v \in V$ such that $T(v) = \lambda v$. By definition, v is an eigenvector with eigenvalue λ.

We now check that λ is central. Let $\alpha \in \mathbb{F}$. Then,

$$\begin{aligned}(\alpha\lambda) \cdot v = \alpha(\lambda v) = \alpha T(v) = T(\alpha v) = {}^a\lambda(\alpha v) \\ = (\lambda\alpha) \cdot v.\end{aligned} \tag{4.2.18}$$

As $v \neq 0$ and we are working over a division ring, it follows that $\alpha\lambda = \lambda\alpha$, that is, λ is central.

($\Leftarrow$) Suppose that λ is central and that there is some nonzero $v \in V$ such that $T(v) = \lambda v$. Define

$$W \coloneqq \{v \in V : T(v) = \lambda v\}. \tag{4.2.19}$$

As λ is central, this is a subspace. It is furthermore a nonzero subspace by hypothesis. By definition, $T|_W = \lambda \,\mathrm{id}_W$.

To show maximality, let $U \supseteq W$ be a subspace such that $T|_U = \lambda \,\mathrm{id}_U$. We then of course have that $T(u) = \lambda u$ for all $u \in U$, that is, $U \subseteq W$, showing maximality. Hence,

$$W \coloneqq \{v \in V : T(v) = \lambda v\} = \mathrm{Eig}_{\lambda T}\,. \tag{4.2.20}$$

In particular, λ is an eigenvalue of T.

(ii) Note that this has already been proven in (4.2.20). ∎

[a] If $v \in \mathrm{Eig}_\lambda$, $\alpha v \in \mathrm{Eig}_\lambda$ as well because this is a subspace.

There is an equivalent way to state this that is often used in practice.

Proposition 4.2.21 Let V be a vector space over a division ring $\mathbb{F}$, let $T\colon V \to V$ be linear, and let $\lambda \in \mathbb{F}$. Then, $\lambda \in \mathrm{Eig}(T)$ iff $\mathrm{Ker}(T - \lambda) \neq 0$.

R In practice, this is often used as follows. Suppose A is a matrix and you would like to compute its eigenvalues. Row-reduce $A - \lambda$. The eigenvalues are then the values of λ for which the null-space of the result is nonzero, in which case the eigenvectors are the elements of those nonzero null-spaces.

A more common method to compute eigenvalues (Theorem 5.7.2.120) is not able to be stated until after we've done determinants. While that method is admittedly sometimes more practical for computing the eigenvalues themselves, this method has the advantage that it lends itself to computing the eigenvalues and eigenvectors simultaneously.

R Thus, $\lambda \in \mathrm{Eig}(T)$ iff $T - \lambda$ is not injective, which, in finite-dimensions, is equivalent to $T - \lambda$ *not being invertible*.

Proof. We leave this as an exercise.

Exercise 4.2.22 Prove the result.

■

▪ **Example 4.2.23** Define

$$A := \begin{bmatrix} 42 & -30 \\ 60 & -43 \end{bmatrix} \tag{4.2.24}$$

as a matrix over $\mathbb{C}$.

Then,

$$A - \lambda = \begin{bmatrix} 42 - \lambda & -30 \\ 60 & -43 - \lambda \end{bmatrix}. \tag{4.2.25}$$

Swap the rows, and after doing so, add $-(42-\lambda)/60$ times the first row to the second. The result is

$$\begin{bmatrix} 60 & -43-\lambda \\ 0 & -30-\frac{1}{60}(42-\lambda)(-43-\lambda) \end{bmatrix}. \tag{4.2.26}$$

This has a free-variable iff the bottom-right entry vanishes, that is, iff

$$-30-\tfrac{1}{60}(42-\lambda)(-43-\lambda)=0. \tag{4.2.27}$$

Solving this equation for λ, one finds

$$\lambda=-3,2. \tag{4.2.28}$$

These are the eigenvectors.

As for the eigenvectors, plug these values into our row-reduced $A-\lambda$ in (4.2.26). If you solved for λ properly, you know the bottom row is going to vanish, and so you only need to compute the top row which is easy:

$$\begin{bmatrix} 60 & -40 \\ 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 60 & -45 \\ 0 & 0 \end{bmatrix} \tag{4.2.29}$$

respectively for $\lambda=-3$ and $\lambda=2$. From this, we can read off the null-spaces to find

$$\mathrm{Eig}_{-3}=\mathrm{Span}\left(\begin{bmatrix}2\\3\end{bmatrix}\right) \text{ and } \mathrm{Eig}_{2}=\mathrm{Span}\left(\begin{bmatrix}3\\4\end{bmatrix}\right). \tag{4.2.30}$$

■ **Example 4.2.31** Define $D\colon C^\infty(\mathbb{R})\to C^\infty(\mathbb{R})$ by $D(f):=f'$. Then, $\lambda\in\mathbb{C}$ is an eigenvalue of f iff f is nonzero and $f'=:D(f)=\lambda f$. If this is true, it follows that $f(x)=C\exp(\lambda x)$ for some constant $C\in\mathbb{C}$, and hence that the function $x\mapsto\exp(\lambda x)$ is an eigenvector of D with eigenvalue

λ. Thus, every $\lambda \in \mathbb{C}$ is an eigenvalue and

$$\mathrm{Eig}_\lambda = \mathrm{Span}(\exp(\lambda x)). \tag{4.2.32}$$

▪ **Example 4.2.33** Let $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the linear-transformation that is counter-clockwise rotation about the origin by $\pi/2$. If $v \in \mathbb{R}^2$ and $T(v) = \lambda v$ for some $\lambda \in \mathbb{R}$, then the rotate of v would have to be parallel to v. This is impossible unless $v = 0$. Thus, this linear-transformation has no eigenvalues.

▪ **Example 4.2.34** Let A be an upper-triangular matrix with entries in a field. Then, the eigenvalues of A are the scalars appearing on the diagonal of A.

Exercise 4.2.35 Check this.

▪ **Example 4.2.36** Let $\mathbb{F}$ be a division ring and let $L, R\colon \mathbb{F}^{\mathbb{N}} \to \mathbb{F}^{\mathbb{N}}$ be the left and right shift operators respectively (Example 1.1.48). Then, $\mathrm{Eig}(L) = \mathbb{F}$ but $\mathrm{Eig}(R) = \emptyset$. We now check this.

Let $\lambda \in \mathbb{F}$ be an eigenvalue of R. Then, there is some nonzero sequence $\langle a_0, a_1, \ldots\rangle \in \mathbb{F}^{\mathbb{N}}$ such that

$$\begin{aligned}\langle 0, a_0, a_1, \ldots\rangle &=: R(a_0, a_1, a_2, \ldots)\\ &= \lambda(a_0, a_1, a_2, \ldots),\end{aligned} \tag{4.2.37}$$

whence it follows that $\lambda a_0 = 0$ and $a_k = \lambda a_{k+1}$ for $k \geq 0$. If $\lambda = 0$, the latter implies that $a_k = 0$ for all $k \in \mathbb{N}$. On the other hand, if $\lambda \neq 0$, then former implies that $a_0 = 0$, in which case the latter gives $a_1 = \lambda \cdot 0 = 0$, $a_2 = \lambda \cdot a_1$, and so on. In either case, the sequence is 0, in which case λ cannot be an eigenvalue. Thus, the set of eigenvalues of R is the empty-set.

Now suppose that $\lambda \in \mathbb{F}$ is an eigenvalue of L. Then, there is some nonzero sequence $\langle a_0, a_1, \ldots \rangle \in \mathbb{F}^{\mathbb{N}}$ such that

$$\begin{aligned} \langle a_1, a_2, a_3, \ldots \rangle &=: L(a_0, , a_1, a_2, \ldots) \\ &= \lambda \langle a_0, a_1, a_2, \ldots \rangle, \end{aligned} \tag{4.2.38}$$

whence it follows that $a_{k+1} = \lambda a_k$ for all $k \in \mathbb{N}$. Inductively, we find that $a_k = \lambda^k a_0$. Hence, every $\lambda \in \mathbb{F}$ is an eigenvalue with

$$\mathrm{Eig}_\lambda = \mathrm{Span}\left(\langle 1, \lambda, \lambda^2, \ldots \rangle \right). \tag{4.2.39}$$

Proposition 4.2.40 — Eigenspaces with distinct eigenvalues are linearly-independent Let V be a vector space and let $T : V \to V$ be linear. Then,

$$\left\{ \mathrm{Eig}_\lambda : \lambda \in \mathrm{Eig}(T) \right\} \tag{4.2.41}$$

is linearly-independent.

R Explicitly, this means that any collection of eigenvectors with distinct eigenvalues is linearly-independent.

R When we investigate generalized-eigenvectors, we will encounter a strict generalization of this—see Proposition 4.4.3.67.

Proof. Denote the ground division ring by $\mathbb{F}$. We proceed by induction on m. The $m = 0$ case is immediate as eigenvectors are nonzero. So, let $m \in \mathbb{Z}^+$ and suppose the result is true $m-1$. To prove the result for m, we proceed by contradiction: let $v_1 \in \mathrm{Eig}_{\lambda_1}, \ldots, v_m \in \mathrm{Eig}_{\lambda_m}$ for $\lambda_1, \ldots, \lambda_m \in \mathrm{Eig}(T)$ and suppose that $\{v_1, \ldots, v_m\}$ is linearly-dependent. By Proposition 2.1.3.7, there is some v_k such that

$$v_k \in \mathrm{Span}(v_1, \ldots, v_{k-1}). \tag{4.2.42}$$

Without loss of generality, we may assume that k is the smallest such integer. Thus, there are $\alpha_1, \ldots, \alpha_{k-1} \in \mathbb{F}$ such that

$$v_k = \alpha_1 \cdot v_1 + \cdots + \alpha_{k-1} \cdot v_{k-1}. \tag{4.2.43}$$

Applying T to this equation yields

$$\lambda_k v_k = \alpha_1 \lambda_1 v_1 + \cdots + \alpha_{k-1} \lambda_{k-1} v_{k-1}. \tag{4.2.44}$$

Multiplying (4.2.43) by λ_k and subtracting the result from (4.2.44) yields[a]

$$0 = \alpha_1(\lambda_1 - \lambda_k)v_1 + \cdots + \alpha_{k-1}(\lambda_{k-1} - \lambda_k). \tag{4.2.45}$$

Now, by the induction hypothesis, it follows that $\alpha_i(\lambda_i - \lambda_k) = 0$ for all $1 \leq i \leq k-1$. If some $\alpha_i \neq 0$, then it would follows that $\lambda_i = \lambda_k$: a contradiction of the fact that the eigenvalues are distinct. Thus, we must have that $\alpha_i = 0$ for all $1 \leq i \leq k-1$, whence it follows from (4.2.43) that $v_k = 0$, which itself is a contradiction (eigenvectors can't be 0). Thus, it must have been the case that $\{v_1, \ldots, v_m\}$ was linearly-independent, as desired. ■

[a] Note that I am allowed to commute λ_k past the α_is as λ_k is central.

Corollary 4.2.46 Let V be a vector space, let $T : V \to V$ be linear, and let $\mathcal{E}$ denote the set of eigenvalues of T. Then, $|\mathcal{E}| \leq \dim(V)$.

R In words, the number of eigenvalues is at most the dimension.

Proof. For every $\lambda \in \mathcal{E}$, let $v_\lambda \in \mathrm{Eig}_\lambda$ be an eigenvector. By the previous result, $\{v_\lambda : \lambda \in \mathcal{E}\}$ is linearly-independent, and so[a]

$$|\mathcal{E}| = |\{v_\lambda : \lambda \in \mathcal{E}\}| \leq \dim(V). \tag{4.2.47}$$

■

[a] By Corollary 2.2.1.18—this is the result that says linearly-independent sets have cardinality at most the cardinality of any spanning set.

Let V be a vector space over a division ring $\mathbb{F}$ and let $T: V \to V$ be a linear-transformation. In Example 4.4.2.1, we saw that we could make V into an $\mathbb{F}[x]$-module, by having a polynomial p act on V by the $\mathbb{F}$-linear-transformation $p(T)$. In the following result, we examine how such operators act on eigenvectors.

Proposition 4.2.48 Let V be a vector space over a division ring $\mathbb{F}$, let $T: V \to V$ be linear, let $p \in \mathbb{F}[x]$ be a polynomial, and let $\lambda \in \mathbb{F}$ be an eigenvalue of T with eigenvector $v \in V$. Then,

$$[p(T)](v) = p(\lambda)v. \tag{4.2.49}$$

R In fact, over the complex numbers at least, this generalizes to p any Borel function—the trick in making this precise is that first one has to actually *define* what one means by $p(T)$ in this case.

R Indeed, note that you can view the equation $T(v) = \lambda v$ as the special case of this result for the polynomial $p(x) := x$.

Proof. We leave this as an exercise.

Exercise 4.2.50 Prove the result.

■

Corollary 4.2.51 Let V be a vector space over a division ring $\mathbb{F}$, let $T: V \to V$ be linear, and let $p \in \mathbb{F}[x]$ be a polynomial. Then, if $p(T) = 0$, then $p(\lambda) = 0$ for all $\lambda \in \mathrm{Eig}(T)$.

R This can have practical applications for actually *computing* eigenvalues. For example, if for whatever reason you know that $T^2 - 1 = 0$, then you know that $\lambda^2 - 1 = 0$ for any eigenvalue $\lambda \in \mathbb{F}$ of T. Thus, in this case, one could deduce that the only possible eigenvalues for T were ± 1.

Proof. Suppose that $p(T) = 0$. Let $\lambda \in \text{Eig}(T)$ with eigenvector $v \in V$. By the previous result, we have that

$$0 = [p(T)](v) = p(\lambda)v. \tag{4.2.52}$$

As v is nonzero, it follows that $p(\lambda) = 0$. ∎

▪ **Example 4.2.53** For example, suppose that $3 \in \mathbb{C}$ is an eigenvalue of T with eigenvector $v \in V$, so that $T(v) = 3v$. If $p(x) := -5x^2 + 2x + 1$, then we would have

$$\begin{aligned}[-5T^2 + 2T + \text{id}](v) =: [p(T)](v) &= p(3)v \\ &= [-5 \cdot 9 + 2 \cdot 3 + 1]v \\ &= -38v.\end{aligned} \tag{4.2.54}$$

4.3 Diagonalization

We started this chapter with the objective of finding a basis for which the coordinates of a given linear-transformation was a diagonal matrix. We now have the tools to discuss this.

Definition 4.3.1 — Diagonalizable Let V be a finite-dimensional vector space and let $T\colon V \to V$ be linear. Then, T is ***diagonalizable*** iff there is a basis $\mathcal{B}$ of V such that $[T]_{\mathcal{B}\leftarrow\mathcal{B}}$ is a diagonal matrix.

R In this case, $[T]_{\mathcal{B}\leftarrow\mathcal{B}}$ is the ***diagonalization*** of T.

R If A is a matrix, we say that A is ***diagonalizable*** iff the associated linear-transformation is diagonalizable.

R For some odd reason, many students seem to think there is a relationship between being diagonalizable and being invertible. So, let me make this perfectly clear.

THERE IS NO RELATIONSHIP BETWEEN DIAGONALIZABILITY AND INVERTIBILITY!

Sometimes when students get something wrong, even though it's wrong, it makes sense how they might have thought that wrong thing. This is not one of these cases. I have absolutely zero idea what makes students think this, but I think every time I've taught linear algebra, at least one (usually more) student has made this mistake.

So, to that end, see the following example.

▪ **Example 4.3.2** The 1×1 0 matrix is diagonal (so obviously diagonalizable) but not invertible.

The 1×1 identity matrix is both diagonal and invertible.

The 2×2 matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{4.3.3}$$

is not diagonalizable[a] but invertible.

The 2×2 matrix

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \tag{4.3.4}$$

is neither diagonalizable nor invertible.

[a] Though this will not be obvious to use until after having studied Jordan canonical form.

The whole point of discussing the "eigenstuff" was, as we saw in Section 4.1 Motivation, that the existence of eigenvalues was related

to the diagonalizability of the linear-transformation. We now make this precise.

Theorem 4.3.5 — Fundamental Theorem of Diagonalizability. Let V be a finite-dimensional vector space, let $T: V \to V$ be linear, and let $\lambda_1, \ldots, \lambda_m$ denote the eigenvalues of T.[a] Then, the following are equivalent.

(i). T is diagonalizable.

(ii). There is a basis of V consisting of eigenvectors of T.

(iii).

$$\dim(V) = \dim(\mathrm{Eig}_{\lambda_1}) + \cdots + \dim(\mathrm{Eig}_{\lambda_m}). \quad (4.3.6)$$

(iv).

$$V = \mathrm{Eig}_{\lambda_1} \oplus \cdots \oplus \mathrm{Eig}_{\lambda_m}. \quad (4.3.7)$$

(v). The geometric multiplicity of λ_k is the same as the algebraic multiplicity of λ_k for all $1 \leq k \leq m$.

In this case, if $\mathcal{B}$ is a basis of eigenvectors of V consisting of eigenvectors of T, then $[T]_{\mathcal{B} \leftarrow \mathcal{B}}$ is a diagonal matrix.

R We actually haven't yet met all the material required to understand (iv) and (v) yet.

The "$\oplus$" in (iv) is called the *direct-sum* and is defined in Definition 4.4.1.1.[b]

The *algebraic multiplicity* is defined to be the dimension of the corresponding generalized eigenspaces—see Theorem 4.3.5. Thus, one always knows that the geometric multiplicity is at most the algebraic multiplicity. In practice, one uses this condition by computing the characteristic polynomial (Theorem 5.7.2.110) together with the fact that the power of $(x - \lambda)$ in the characteristic polynomial is the algebraic multiplicity (Theorem 5.7.2.120). This then tells you how many linearly-independent eigenvectors you need to find for each eigenvalue in order for the linear-transformation to be diagonalizable.

R In particular, as eigenspaces are of course at least one-dimensional, if T has $\dim(V)$ distinct eigenvalues, then T must be diagonalizable. That said, the converse is not true—see Example 4.3.15.

R Warning: This name is nonstandard—there is no standard name for this result.

[a] Note that there are finitely many eigenvalues by Corollary 4.2.46.
[b] Also see the remark in Proposition 4.4.1.30.

Proof. We leave this as an exercise.

Exercise 4.3.8 Prove the result.

■

▪ **Example 4.3.9** Define

$$A := \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{bmatrix}. \tag{4.3.10}$$

As A is upper-triangular, the eigenvalues are the elements on the diagonal 1, 4, and 6. Thus, as A has 3 distinct eigenvalues, it must be diagonalizable.

Diagonalizability is yet another context where the ground division ring matters.

▪ **Example 4.3.11 — A matrix diagonalizable over $\mathbb{C}$ but not over $\mathbb{R}$** Define

$$A := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{4.3.12}$$

This matrix defines a linear-transformation $\mathbb{R}^2 \to \mathbb{R}^2$ and also $\mathbb{C}^2 \to \mathbb{C}^2$. In either case, if λ is an eigenvalue, then it must be

the case that

$$\lambda^2 + 1 = 0. \tag{4.3.13}$$

Exercise 4.3.14 Check this, that is, show that in both case $F = \mathbb{R}, \mathbb{C}$, $\lambda \in \mathbb{F}$ is an eigenvalue iff $\lambda^2 + 1 = 0$.

Thus, if the ground field is $\mathbb{R}$, there are no eigenvalues. On the other hand, if the ground field in $\mathbb{C}$, then there are two distinct eigenvalues, ± 1. Thus, according to Fundamental Theorem of Diagonalizability (Theorem 4.3.5), this linear-transformation is diagonalizable over $\mathbb{C}$ but not over $\mathbb{R}$.

The phenomenon we observed in the previous example is quite general, so it's worth it to take the time to point out its significance.

As we will see later, it turns out that to every linear operator, there is an associated polynomial, the *characteristic polynomial*, that has the property that a scalar is an eigenvalue iff it is a root of that polynomial.

In the previous example, the characteristic polynomial was $\lambda^2 + 1$. Thus, if the characteristic polynomial doesn't have any roots, the linear operator doesn't have any eigenvalues. Thus, we observe the following.

If order to guarantee that all linear operators have an eigenvalue, we're going to want to require all polynomials to have at least one root.

The property that all polynomials have a root is an important one called *algebraically closed*, and we will return to it later. For now, however, we resume discussion of examples regarding diagonalizability.

▪ **Example 4.3.15 — A diagonalizable linear-transformation with fewer eigenvalues than the dimension** The identity $\mathbb{R}^2 \to \mathbb{R}^2$ has a single eigenvalue (1), but yet it is diagonalizable (with respect to the standard basis).

▪ **Example 4.3.16 — A matrix over $\mathbb{C}$ that is not diagonalizable** Define

$$A := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \tag{4.3.17}$$

There is only one eigenvalue, 0. The eigenspace is the nullspace of $A - 0 = A$, which is just

$$\text{Span}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right). \tag{4.3.18}$$

As the sum of the dimensions of the eigenspaces is only 1, A cannot be diagonalizable.

Exercise 4.3.19 Define $V := \{f \in C^\infty(\mathbb{R}) : f'' + f = 0\}$ and define $D : V \to V$ by $D(f) := f'$. Show that D is diagonalizable by exhibiting a basis of V with respect to which the coordinates of D is a diagonal matrix.

4.3.1 Diagonalization of matrix linear-transformations

While the concept of diagonalization makes sense for any linear-transformation, there is an extra question one might ask if the linear-transformation happens to be defined by a matrix: what is the relationship between the original matrix and its diagonalization? The answer to this question is given by the following result.

Proposition 4.3.1.1 Let A be an $m \times m$ diagonalizable matrix with entries in a division ring $\mathbb{F}$ and let $\mathcal{B}$ be a basis of

eigenvectors of A. Then,

$$[A]_{\mathcal{B}\leftarrow\mathcal{B}} = [\mathrm{id}]_{\mathcal{B}\leftarrow\mathcal{S}}[A]_{\mathcal{S}\leftarrow\mathcal{S}}[\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}, \tag{4.3.1.2}$$

where $\mathcal{S}$ is the standard basis of $\mathbb{F}^m$.

R Note that $[A]_{\mathcal{S}\leftarrow\mathcal{S}} = A$ by Proposition 3.2.2.30.[a]
Furthermore, $[A]_{\mathcal{B}\leftarrow\mathcal{B}}$ is the diagonalization of A (by definition) and $[\mathrm{id}]_{\mathcal{B}\leftarrow\mathcal{S}} = [\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}^{-1}$. Thus, writing $D := [A]_{\mathcal{B}\leftarrow\mathcal{B}}$ and $P := [\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}$, this equation is sometimes written more concisely (but perhaps less transparently) as

$$D = P^{-1}AP. \tag{4.3.1.3}$$

R Note that, by Theorem 3.2.2.1, the columns of $[\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}$ are given by $[b_k]_{\mathcal{S}}$ for $b_k \in \mathcal{B}$. However, by Proposition 3.1.17,[b] this is just b_k itself. Thus,

> *$P := [\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}$ is the matrix whose columns are the eigenvectors of A.*

[a] I wrote (4.3.1.2) using $[A]_{\mathcal{S}\leftarrow\mathcal{S}}$ instead of A because I feel as if writing it this way makes it more 'obviously' true.

[b] This is the result that says the coordinates of a column vector with respect to the standard basis is just that original column vector.

Proof. We leave this as an exercise.

Exercise 4.3.1.4 Prove the result yourself.

■

The practical important of this result is as follows. Let A, P, and D be as in the statement of the previous result. Then,

$$A^2 = (PDP^{-1})(PDP^{-1}) = PD^2P^{-1}, \tag{4.3.1.5}$$

where the 'inner' P^{-1} and P have canceled. Similarly,

$$A^3 = (PD^2P^{-1})(PDP^{-1}) = PD^3P^{-1}. \tag{4.3.1.6}$$

And so on. It follows from this that

$$p(A) = Pp(D)P^{-1} \tag{4.3.1.7}$$

for any polynomial $p \in \mathbb{C}[x]$. In fact, essentially the same is true for 'any' function f:

$$f(A) = Pf(D)P^{-1}, \tag{4.3.1.8}$$

the catch being that we haven't actually defined $f(A)$ for nonpolynomial f.

This, coupled with the fact that that $f(D)$ is easily found,

$$f\left(\begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_d \end{bmatrix}\right) = \begin{bmatrix} f(\lambda_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & f(\lambda_d) \end{bmatrix}, \tag{4.3.1.9}$$

make this particularly useful for explicit computation.

For example, suppose I decided I don't like you, and so I to torture you by asking you to compute A^{1000}, where

$$A := \begin{bmatrix} 42 & -30 \\ 60 & -43 \end{bmatrix}. \tag{4.3.1.10}$$

You could just multiply this 2×2 matrix by itself one thousand times. Alternatively, you could diagonalize.

▪ **Example 4.3.1.11** Define

$$A := \begin{bmatrix} 42 & -30 \\ 60 & -43 \end{bmatrix} \tag{4.3.1.12}$$

as a matrix over $\mathbb{C}$.

Fortunately for you, the astute student that you are, you already know what the eigenvalues and eigenvectors are because

you've read Example 4.2.23:

$$\text{Eig}(A) = \{-3, 2\}, \tag{4.3.1.13}$$

and

$$\text{Eig}_{-3} = \text{Span}\left(\begin{bmatrix}2\\3\end{bmatrix}\right) \text{ and } \text{Eig}_2 = \text{Span}\left(\begin{bmatrix}3\\4\end{bmatrix}\right). \tag{4.3.1.14}$$

Writing

$$P := \begin{bmatrix}2 & 3\\3 & 4\end{bmatrix}, ^a, \tag{4.3.1.15}$$

according to the above result, we should have

$$A = PDP^{-1}, \tag{4.3.1.16}$$

where

$$D = \begin{bmatrix}-3 & 0\\0 & 2\end{bmatrix}. \tag{4.3.1.17}$$

Hence,

$$A^{1000} = P\begin{bmatrix}(-3)^{1000} & 0\\0 & 2^{1000}\end{bmatrix}P^{-1}, \tag{4.3.1.18}$$

whatever that simplifies to.

[a] Though you can't tell from this example, this matrix is formed by taking the vectors $\langle 2, 3\rangle$ and $\langle 3, 4\rangle$ as its *columns*, not as its rows.

4.4 Jordan Canonical Form

Diagonalizable linear-transformations are great. There's just one little itsy-bitsy problem: not all linear-transformations are diagonalizable! Not even in the context of finite-dimensional vector space over algebraically closed (Definition C.3.3.1) fields. Fortunately, there is something that is almost as good, but *always* exist (at least if the

ground ring is sufficiently nice): the *Jordan canonical form* of a linear-transformation.

Before doing Jordan canonical form itself, let us quickly investigate a more obvious method one might use in an attempt to 'fix' this defect, a method that winds up not being particularly useful. The original objective was to find a basis $\mathcal{B}$ such that $[T]_{\mathcal{B}} := [T]_{\mathcal{B}\leftarrow\mathcal{B}}$ is diagonal. If we can't do this, it is natural to ask "Okay, so why don't I drop the requirement that the domain and codomain bases be the same, and instead just try to find a basis $\mathcal{B}$ for the domain and a C for the codomain such that $[T]_{C\leftarrow\mathcal{B}}$ is diagonal?". Sure enough, you can do this, but the answer is almost stupidly easy to the point of being useless.

For simplicity, consider for the moment the case T is invertible. Then, for *any* basis $\mathcal{B} =: \{b_1, \ldots, b_d\}$,

$$C := T(\mathcal{B}) := \{T(b_1), \ldots, T(b_d)\} \tag{4.4.1}$$

is another basis (this uses the fact that T is invertible. But then, using (3.2.2.3),

$$[T]_{C\leftarrow\mathcal{B}} = \mathrm{id}_{d\times d}\,. \tag{4.4.2}$$

That is, you can always find bases $\mathcal{B}$ and C such that $[T]_{C\leftarrow\mathcal{B}}$ is the identity matrix! In fact, any basis $\mathcal{B}$ will work (which itself determines C). Now in the general case T is not necessarily invertible, you find almost the same thing: instead of just the identity matrix, you obtain a matrix that is identically 0 except for some 1s on the diagonal.

It should be intuitively clear that because this works all the time and doesn't even really even depend on T (in the sense that any basis $\mathcal{B}$ will work), this isn't going to be very useful. More practically speaking, the result that would be analogous to Proposition 4.3.1.1 wouldn't lend itself to computation. You'll recall there that the computational usefulness of $A = PDP^{-1}$ came down to the fact that the P and P^{-1} canceled when multiplying A by itself. Here, however, there would be no such cancellation if we tried to develop this alternative to diagonalization. Thus, aside from it just being intuitively clear that this isn't going to be very useful, we see more explicitly that this

can't be useful because the trick that made $A = PDP^{-1}$ useful for computation just isn't going to work.

Anyways, let's get back to the "fix" that *will* actually work: Jordan canonical form.

Before we get to Jordan canonical form itself, we must first take a detour to discuss *direct-sums* and *invariant-subspaces*. Very roughly speaking, the idea is to decompose a vector space into smaller pieces that are easier to study. For example, if $b \in V$ is an eigenvector of T, then Span(b) the behavior of T on this subspace is particularly easy to understand. While we can't quite have the subspaces be that simple in general, we will find that we can still decompose our space into pieces which are not that much more complicated.

4.4.1 Direct-sums

The precise sense in which we are going to decompose vector spaces is called the *direct-sum* and is defined as follows.

Definition 4.4.1.1 — Direct-sum Let V be a $\mathbb{K}$-module, and let $\mathscr{W}$ be a collection of subspaces of V. Then, V is the ***direct-sum*** of the elements of $\mathscr{W}$ iff for every $v \in V$ there are unique $v^W \in W$ such that

$$v = \sum_{W \in \mathscr{W}} v^W. \tag{4.4.1.2}$$

R In this case, we write

$$V = \bigoplus_{W \in \mathscr{W}} W. \tag{4.4.1.3}$$

R We say that

$$V = \bigoplus_{W \in \mathscr{W}} W \tag{4.4.1.4}$$

or just $\mathscr{W}$ is a ***direct-sum decomposition*** or ***decomposition*** of V.

R As per usual, the arbitrary (nonfinite) case obfuscates the simplicity of this concept. If $\mathscr{W} = \{W_1, \dots, W_m\}$, then this definition reads: V is the ***direct-sum*** of $W_1, \dots, W_m$ iff for every $v \in V$ there are unique $v^1 \in W, \dots, v^m \in W_m$ such that

$$v = v^1 + \cdots + v^m, \tag{4.4.1.5}$$

in which case we write

$$V = W_1 \oplus \cdots \oplus W_m. \tag{4.4.1.6}$$

R Note how this definition is similar in ways to that of a basis—see Definition 4.4.1.62 and Proposition 4.4.1.14.

We will see that a given direct-sum decomposition is in many ways similar to the specification of a basis. Indeed, there is a sense in which it is a generalization—see Proposition 4.4.1.14. The notions of *linear-independence* and *spanning* generalized to the context of subspaces as well, and, as with bases, these concepts will help us understand direct-sum decompositions.

Theorem 4.4.1.7 — Span (of subspaces). Let V be a $\mathbb{K}$-module and let $\mathscr{W}$ be a collection of subspaces of V. Then, there is a unique subspace of V, the ***span*** of $\mathscr{W}$, $\text{Span}(\mathscr{W})$, such that

(i). $W \subseteq \text{Span}(\mathscr{W})$ for all $S \in \mathscr{W}$; and
(ii). if $U \subseteq V$ is other subspace containing each $W \in \mathscr{W}$, it follows that $\text{Span}(\mathscr{W}) \subseteq U$.

Furthermore, explicitly,

$$\text{Span}(\mathscr{W}) = \sum_{W \in \mathscr{W}} W. \tag{4.4.1.8}$$

R Thus, if $\mathscr{W} = \{W_1, \ldots, W_m\}$, we have that

$$\begin{aligned} \text{Span}(W_1, \ldots, W_m) &:= \text{Span}(\mathscr{W}) \\ &= W_1 + \cdots + W_m. \end{aligned} \tag{4.4.1.9}$$

R It is incredibly uncommon to see people to write $\text{Span}(W_1, \ldots, W_m)$, and instead, people simply write the more explicit $W_1 + \cdots + W_m$.

Proof. We leave this as an exercise.

Exercise 4.4.1.10 Prove the result.

■

Definition 4.4.1.11 — Spanning (subspace) Let V be a $\mathbb{K}$-module and let $\mathscr{W}$ be a collection of subspaces of V. Then, $\mathscr{W}$ is ***spanning*** iff $\text{Span}(\mathscr{W}) = V$.

R Synonymously, we also say that $\mathscr{W}$ ***spans*** V.

Definition 4.4.1.12 — Linear-independence (of subspaces) Let V be a $\mathbb{K}$-module and let $\mathscr{W}$ be a collection of subspaces of V. Then, $\mathscr{W}$ is ***linearly-independent*** iff for all $m \in \mathbb{Z}^+$, $W_1, \ldots, W_m \in \mathscr{W}$, $w_k \in W_k$,

$$w_1 + \cdots + w_m = 0 \text{ implies } w_1 = 0, \ldots, w_m = 0. \tag{4.4.1.13}$$

$\mathscr{W}$ is ***linearly-dependent*** iff it is not linearly-independent.

Now let us see in what sense these concepts are generalizations of the ones we met before.

Proposition 4.4.1.14 Let V be a $\mathbb{K}$-module and let $\mathcal{B} \subseteq V$.

(i). $\mathcal{B}$ is spanning iff $\{\text{Span}(b) : b \in \mathcal{B}\}$ is spanning.

(ii). $\mathcal{B}$ is linearly-independent iff $\{\text{Span}(b) : b \in \mathcal{B}\}$ is linearly-independent.

(iii). $\mathcal{B}$ is a basis iff

$$V = \bigoplus_{b\in\mathcal{B}} \text{Span}(b). \tag{4.4.1.15}$$

R In finite dimensions, with $\mathcal{B} =: \{b_1, \ldots, b_d\}$, (4.4.1.15) reads

$$V = \text{Span}(b_1) \oplus \cdots \oplus \text{Span}(b_d). \tag{4.4.1.16}$$

Proof. We leave this as an exercise.

Exercise 4.4.1.17 Prove the result.

■

This suggests the following criterion for checking whether a vector space can be written as a direct-sum.

Proposition 4.4.1.18 — Criterion for direct-sums of an arbitrary collection of subspaces Let V be a $\mathbb{K}$-module, let $\mathscr{W}$ be a collection of subspaces of V. Then,

$$V = \bigoplus_{W\in\mathscr{W}} W \tag{4.4.1.19}$$

iff $\mathscr{W}$ is linearly-independent and spans V.

R Again, the case where $\mathscr{W} := \{W_1, \ldots, W_M\}$ is clearer. It says:

$$V = W_1 \oplus \cdots \oplus W_m \tag{4.4.1.20}$$

iff (i) $V = W_1 + \cdots + W_m$ and (ii) the equation $0 = w_1 + \cdots + w_m$ with $w_k \in W_k$ implies every $w_k = 0$.

Proof. ($\Rightarrow$) Suppose that

$$V = \bigoplus_{W \in \mathscr{W}} W. \tag{4.4.1.21}$$

By definition, this means that for every $v \in V$ there are unique $v^W \in W$ such that

$$v = \sum_{W \in \mathscr{W}} v^W. \tag{4.4.1.22}$$

In particular, there are *some* sum v^Ws, and so $V = \sum_{W \in \mathscr{W}} W$. Thus, $\mathscr{W}$ spans V. For linear-independence, suppose that

$$0 = \sum_{W \in \mathscr{W}} v^W. \tag{4.4.1.23}$$

As we also have

$$0 = \sum_{v \in \mathscr{W}} 0, \tag{4.4.1.24}$$

uniqueness implies that v^W, and so $\mathscr{W}$ is linearly-independent, as desired.

($\Leftarrow$) Suppose that $\mathscr{W}$ is linearly-independent and spans V. Let $v \in V$. As $\mathscr{W}$ spans V, there are $v^W \in W$ such that

$$v = \sum_{W \in \mathscr{W}} v^W. \tag{4.4.1.25}$$

To show uniqueness, suppose that there are other $u^W \in W$ such that

$$v = \sum_{W \in \mathscr{W}} u^W. \tag{4.4.1.26}$$

Subtracting these two expressions for v, we find

$$0 = \sum_{W \in \mathscr{W}} [v^W - u^W], \tag{4.4.1.27}$$

whence $v^W = u^W$ by linear-independence, giving us uniqueness, as desired. ∎

The case of two subspaces is particularly important, and in this case the criterion simplifies, and so we state it separately.

Corollary 4.4.1.28 — Criterion for direct-sums of two spaces Let V be a $\mathbb{K}$-module, and let $U, W \subseteq V$ be subspaces. Then,

$$V = U \oplus W \tag{4.4.1.29}$$

iff (i) $V = U + W$ and (ii) $U \cap W = 0$.

R Warning: The naive generalization of this criterion to more than two subspaces is not true. That is, if $W_1, \ldots, W_m \subseteq V$ are subspaces such that $V = W_1 + \cdots + W_m$ and $W_k \cap W_l = 0$ for $k \neq l$, it is *not* necessarily the case that $V = W_1 \oplus \cdots \oplus W_m$—see Example 4.4.1.34.

Proof. From the previous result, it suffices to show that $U \cap W = 0$ is true iff it is true that the equation $0 = u + w$ with $u \in U$ and $w \in W$ implies $u = 0 = w$.

($\Rightarrow$) Suppose that $U \cap W = 0$. Let $u \in U$, $w \in W$, and suppose that $0 = u + w$. Then, $w = -u \in U$, and so $w \in U \cap W$, and so $w = 0$. We then have $u = -w = 0$.

($\Leftarrow$) Suppose that the equation $0 = u + w$ with $u \in U$ and $w \in W$ implies $u = 0 = w$. Let $v \in U \cap W$. We have that $0 = v + (-v)$, and as $v \in U$ and $-v \in W$, it follows in particular that $v = 0$, and hence $U \cap W = 0$. ∎

There are also more practical criterion specific to the finite-dimensional case.

Proposition 4.4.1.30 Let V be a finite-dimensional vector space and let $W_1, \ldots, W_m \subseteq V$ be subspaces such that

$$\dim(V) = \dim(W_1) + \cdots + \dim(W_m). \tag{4.4.1.31}$$

(i). If $\{W_1, \ldots, W_m\}$ is spanning, then $V = W_1 \oplus \cdots \oplus W_m$.

(ii). If $\{W_1, \ldots, W_m\}$ are linearly-independent, then $V = W_1 \oplus \cdots \oplus W_m$.

R Thus, if the sum of the dimensions of the W_ks add up to that of V, then you only need to check one of the two usual conditions, instead of both.

R Note that a corollary of this (together with Theorem 4.3.5) is that a linear operator $V \to V$ is diagonalizable iff V is the direct-sum of its eigenspaces:

$$V = \mathrm{Eig}_{\lambda_1} \oplus \cdots \oplus \mathrm{Eig}_{\lambda_m} . \tag{4.4.1.32}$$

Proof. We leave this as an exercise.

Exercise 4.4.1.33 Prove the result.

■

▪ **Example 4.4.1.34 — $W_1, W_2, W_3 \subseteq V$ subspaces with trivial pairwise intersections and $V = W_1 + W_2 + W_3$ but $V \neq W_1 \oplus W_2 \oplus W_3$** Define $V := \mathbb{R}^2$, $W_1 := \mathrm{Span}(\langle 1, 0\rangle)$, $W_2 := \mathrm{Span}(\langle 0, 1\rangle)$, and $W_3 := \mathrm{Span}(\langle 1, 1\rangle)$. Then, $W_1 \cap W_2 = 0$, $W_1 \cap W_3 = 0$, $W_2 \cap W_3 = 0$, $W_1 + W_2 + W_3 = V$, but the sum is not direct: we can write both

$$\langle 1, 1\rangle = 0 + 0 + \langle 1, 1\rangle \tag{4.4.1.35}$$

and

$$\langle 1, 1\rangle = \langle 1, 0\rangle + \langle 0, 1\rangle + 0. \tag{4.4.1.36}$$

▪ **Example 4.4.1.37** Define

$$U = \text{Span}\left(\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}\right) \text{ and } W = \text{Span}\left(\begin{bmatrix}1\\2\\3\end{bmatrix}\right). \quad (4.4.1.38)$$

Then, $\mathbb{R}^3 = U \oplus V$.

Exercise 4.4.1.39 Check this.

▪ **Example 4.4.1.40** Define

$$V := \left\{ f \in \text{Mor}_{\mathbf{Set}}(\mathbb{R}^2, \mathbb{R}) : \lim_{|x|\to\infty} f(x) \text{ exists.} \right\}. \quad (4.4.1.41)$$

Then,

$$V = \{f \in V : f \text{ is constant.}\} \oplus \left\{ f \in V : \lim_{|x|\to\infty} f(x) = 0 \right\}.$$

To see this, note that we may write

$$f = \lim_{|x|\to\infty} f(x) + (f - \lim_{|x|\to\infty} f(x)) \quad (4.4.1.42)$$

for any $f \in V$.

Exercise 4.4.1.43 Check this in more detail.

One important fact about direct-sums that will be of use to us is, to find a basis for the entire space, it suffices to find a basis for each of the direct-summands.

Proposition 4.4.1.44 Let V be a $\mathbb{K}$-module, let $\mathscr{W}$ be a collection of subspaces of V such that $V = \bigoplus_{W\in\mathscr{W}} W$, and

for each $W \in \mathscr{W}$ let $\mathcal{B}_W$ be a basis of W. Then,

$$\bigcup_{W \in \mathscr{W}} \mathcal{B}_W \tag{4.4.1.45}$$

is a basis of V.

Proof. We leave this as an exercise.

Exercise 4.4.1.46 Prove the result.

■

In a way roughly analogous to how we can extend linearly-independent subsets to bases, we can 'extend' subspaces into direct-sum decompositions, at least for vector spaces

Proposition 4.4.1.47 — Subspaces of vector spaces have complements Let V be a vector space and let $U \subseteq V$ be a subspace. Then, there is a subspace $W \subseteq V$ such that $V = U \oplus W$.

R If V is a $\mathbb{K}$-module and $U \subseteq V$ is a subspace, then a subspace $W \subseteq V$ such that $V = U \oplus W$ is a ***complement*** of U.

R Warning: Complements are not unique, even for vector spaces—see Example 4.4.1.51.

R Warning: This will fail in general for $\mathbb{K}$-modules—see Example 4.4.2.19.

Proof. Let $\mathcal{A}$ be a basis of U and extend it to a basis $\mathcal{B}$ of V. Define $C := \mathcal{B} \setminus \mathcal{A}$ and $W := \mathrm{Span}(C)$. We certainly have

$$\begin{aligned} V &= \mathrm{Span}(\mathcal{B}) = \mathrm{Span}(\mathcal{A} \cup C) \\ &= \mathrm{Span}(\mathcal{A}) + \mathrm{Span}(C) = U + W. \end{aligned} \tag{4.4.1.48}$$

On the other hand, an element in the intersection $V \cap W$ must be able to be written as a linear-combination of both elements of $\mathcal{A}$ and elements of C. This would then yield a nontrivial linear-dependence relation among elements of $\mathcal{A} \cup C = \mathcal{B}$ unless the element in the intersection were 0. Thus, we must have $U \cap W = 0$, and hence $V = U \oplus W$ by Corollary 4.4.1.28. ■

Direct-sums allow us to define *projections*.

Proposition 4.4.1.49 — Projection Let V be a $\mathbb{K}$-module, and let $\mathscr{W}$ be a collection of subspaces of V such that $V = \bigoplus_{W \in \mathscr{W}} W$. Then, for every $W_0 \in \mathscr{W}$, there is a unique linear-transformation $\text{proj}_{W_0} : V \to W_0$, the ***projection*** onto W with respect to the decomposition $V = \bigoplus_{W \in \mathscr{W}} W$, such that $\text{proj}_{W_0}(v) = v^{W_0}$, where $v = \sum_{W \in \mathscr{W}} v^W$ for unique $v^W \in W$.

R For example, if $V = U \oplus W$, for $v \in V$, we can write $v = u + w$ for unique $u \in U$ and $w \in U$. In this case, $\text{proj}_U(v) = u$. (Similarly, $\text{proj}_W(v) = w$.)

R Warning: proj_{W_0} is *not* uniquely determined by W_0 itself—it depends on the other Ws, on the entire decomposition—see Example 4.4.1.51 for a concrete example of this.

Proof. We leave this as an exercise.

Exercise 4.4.1.50 Prove the result yourself.

■

▪ **Example 4.4.1.51 — $V = U \oplus W_1 = U \oplus W_2$ for $W_1 \neq W_2$** Define $V := \mathbb{R}^2$, $U := \text{Span}(\langle 1, 0\rangle)$, $W_1 := \text{Span}(\langle 0, 1\rangle)$, and $W_2 := \text{Span}(\langle 1, 1\rangle)$.

Exercise 4.4.1.52 Check that $V = U \oplus W_1$ and $V = U \oplus W_2$.

Define $v := \langle a, b \rangle \in \mathbb{R}^2$. The decomposition of v with respect to the decomposition $V = U \oplus W_1$ is given by

$$v := \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ b \end{bmatrix}. \tag{4.4.1.53}$$

On the other hand, the decomposition of v with respect to the decomposition $V = U \oplus W_2$ is given by

$$v := \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a - b \\ 0 \end{bmatrix} + \begin{bmatrix} b \\ b \end{bmatrix} \tag{4.4.1.54}$$

Hence,

$$\mathrm{proj}_U(w) = \begin{bmatrix} a \\ 0 \end{bmatrix} \tag{4.4.1.55}$$

with respect to the first decomposition, but

$$\mathrm{proj}_U(w) = \begin{bmatrix} a - b \\ 0 \end{bmatrix} \tag{4.4.1.56}$$

with respect to the second decomposition.

Coordinates with respect to direct-sum decompositions

We saw in Definition 3.1.1 that, given a basis of a $\mathbb{K}$-module V, we can define the *coordinates* of elements of v with respect to that basis. In a similar way, we can also talk about the coordinates of elements of V with respect to a direct-sum decomposition. In fact, the definition of coordinates we learned before is a special case of this—see Proposition 4.4.1.14.

We saw before that the coordinates of an 'abstract' vector was an element of $\mathbb{K}^d$, $\mathbb{K}$ the ground ring. Given a direct-sum decomposition $V = W_1 \oplus \cdots \oplus W_m$, the first question we must address is "What

plays the role of $\mathbb{K}^d$ in this context?". To see what the answer should be, recall (Proposition 4.4.1.14) that, given a basis $\mathcal{B}$ of V, V can be written as the direct-sum of the subspaces $\{\text{Span}(b) : b \in \mathcal{B}\}$.

Over a division ring $\mathbb{F}$, $\text{Span}(b) \cong_{\mathbf{Vect}_\mathbb{F}} \mathbb{F}$ via the map $\mathbb{F} \ni \alpha \mapsto \alpha \cdot b \in \text{Span}(b)$. Thus, if $\mathcal{B} =: \{b_1, \ldots, b_d\}$ is a basis for the vector space V, after identifying each $\text{Span}(b_k)$ with $\mathbb{F}$, (4.4.1.16) reads

$$V \cong \underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{d}. \tag{4.4.1.57}$$

On the other hand, we know from Proposition 3.1.7 that the map that sends an "abstract" vector to its coordinates yields an isomorphism

$$V \cong \mathbb{F}^d := \underbrace{\mathbb{F} \times \cdots \times \mathbb{F}}_{d}. \tag{4.4.1.58}$$

These two facts together suggest that in the general case $V = W_1 \oplus \cdots \oplus W_d$, $W_1 \times \cdots \times W_d$ should play the role that $\mathbb{F}^d$ did with coordinates before. That is, the map that sends an "abstract" vector to its coordinates should be a map $V \to W_1 \times \cdots \times W_d$ (and with any luck, it will be an isomorphism). This is exactly how we're doing to define things. But first, we want to give $W_1 \times \cdots \times W_d$ the structure of a vector space.

Proposition 4.4.1.59 — Product of modules Let $\mathscr{V}$ be an indexed collection of $\mathbb{K}$-modules, and define $\prod_{V\in\mathscr{V}} V \times \prod_{V\in\mathscr{V}} V \to \prod_{V\in\mathscr{V}} V$ and $\mathbb{K} \times \prod_{V\in\mathscr{V}} V \to \prod_{V\in\mathscr{V}} V$ respectively by

$$[v_1 + v_2]^V := v_1^V + v_2^V \tag{4.4.1.60a}$$
$$[\alpha \cdot v]^V := \alpha \cdot v^V. \tag{4.4.1.60b}$$

Then, $\prod_{V\in\mathscr{V}} V$ is a $\mathbb{K}$-module, the ***product***, with this addition and scaling.

R $v \in \prod_{V\in\mathscr{V}} V$, that is, it is a function $\mathscr{V} \to \bigsqcup_{V\in\mathscr{V}} V$ whose value at $V \in \mathscr{V}$ is an element of V—see Definition A.3.1.6. $\alpha \cdot v$ is a new function, one we are defining, and $[\alpha \cdot v]^V$ is its value at $v \in \mathscr{V}$. Similarly for the definition of addition.

R In words, addition and scaling are defined *componentwise*.

R In the finite case $\mathscr{V} =: \{V_1, \dots, V_m\}$, these definitions (in more suggestive notation) look like

$$\langle v^1, \dots, v^d \rangle + \langle w^1, \dots, w^d \rangle := \langle v^1 + w^1, \dots, v^d + w^d \rangle$$
$$\alpha \cdot \langle v^1, \dots, v^d \rangle := \langle \alpha v^1, \dots, \alpha v^d \rangle,$$

just as in $\mathbb{K}^m$ (Example 1.1.15).

Proof. We leave this as an exercise.

Exercise 4.4.1.61 Prove the result.

R Hint: The proof is as easy as verifying the axioms of a $\mathbb{K}$-module—see Definition 1.1.1.

■

We are now ready define coordinates with respect to a direct-sum decomposition.

Definition 4.4.1.62 — Coordinates (of a vector with respect to a decomposition) Let V be a $\mathbb{K}$-module, let $V = \bigoplus_{W \in \mathscr{W}} W$ be a direct-sum decomposition of V, let $v \in V$, and write

$$v = \sum_{W \in \mathscr{W}} v^W \tag{4.4.1.63}$$

for unique $v^W \in \mathscr{W}$. Then, the ***coordinates*** of v with respect to the decomposition $\mathscr{W}$, $[v]_{\mathscr{W}}$, is defined by

$$[v]_{\mathscr{W}} := \langle v^W : W \in \mathscr{W} \rangle \in \prod_{W \in \mathscr{W}} W. \tag{4.4.1.64}$$

R If $\mathscr{W} =: \{W_1, \dots, W_m\}$ is finite, where are unique $v^1 \in W^1, \dots, v^m \in W^m$ such that

$$v = v^1 + \cdots + v^m. \tag{4.4.1.65}$$

Then, the coordinates of v are given by the column vector

$$[v]_{\mathscr{W}} := \begin{bmatrix} v^1 \\ \vdots \\ v^m \end{bmatrix} \in \prod_{k=1}^{m} W_k. \tag{4.4.1.66}$$

R Note that this generalizes coordinates with respect to a basis (Definition 3.1.1), at least for vector spaces. Indeed, if $\mathcal{B}$ is a basis for V, then we obtain a corresponding direct-sum decomposition

$$V = \bigoplus_{b \in \mathcal{B}} \mathrm{Span}(b) \tag{4.4.1.67}$$

by the previous result. If the ground ring $\mathbb{F}$ is a division ring, then $\mathrm{Span}(b)$ is isomorphic to the one-dimensional vector space $\mathbb{F}$, and after this identification, we can view the component $v^b \in \mathrm{Span}(B)$ in the sense of this definition as a scalar, which gives us $[v]_{\mathcal{B}}$.

As before, this is an isomorphism if the direct-sum decomposition is finite.

Proposition 4.4.1.68 — $[\cdot]_{\mathscr{W}}$ is linear and injective (and surjective in finite dimensions) Let V be a $\mathbb{K}$-module, and let $V = \bigoplus_{W \in \mathscr{W}} W$ be a direct-sum decomposition of V. Then,

$$V \ni v \mapsto [v]_{\mathscr{W}} \in \prod_{W \in \mathscr{W}} W \tag{4.4.1.69}$$

is linear and injective with image

$$\left\{ \langle v^W : W \in \mathscr{W} \rangle : v^W = 0 \text{ for cofinitely many } W \in \mathscr{W}. \right\}.$$

R In particular, if $\mathscr{W} =: \{W^1, \dots, W^m\}$ is finite this gives an isomorphism $V \to W^1 \times \cdots \times W^m$. In particular,

$$W^1 \oplus \cdots \oplus W^m \cong W^1 \times \cdots \times W^m. \quad (4.4.1.70)$$

For this reason, people are not always careful to distinguish between the two, and quite often people will write $V \oplus W$ when technically they mean $V \times W$. Indeed, I have even heard $V \times W$ called the "external direct sum" (in which case they referred to what we have been calling "direct sum" as "internal direct sum").

Proof. We leave this as an exercise.

Exercise 4.4.1.71 Prove this yourself.

■

As you might now expect, we obtain an analogous notion of coordinates of linear-transformations with respect to (finite) direct-sum decompositions. As with coordinates of vectors, our first order of business is to determine what the analogue of matrices is in this context (just as we had to determine what the analogue of $\mathbb{K}^d$ should be). We will see that the answer is still essentially "matrices", but now matrices whose entries themselves are linear-transformations (similar to how one might think of an element of $W_1 \times \cdots \times W_m$ as a "column vector" whose entries are themselves vectors).

Definition 4.4.1.72 — Matrix (of linear-transformations) Let m and n be collections of $\mathbb{K}$-modules. Then, an $m \times n$ ***matrix*** is a function

$$m \times n \ni \langle i, j \rangle \mapsto A^i{}_j \in \bigsqcup_{\substack{W \in m \\ V \in n}} \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W) \quad (4.4.1.73)$$

such that $A^i{}_j \in \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(i, j)$.

R We make use of all of the suggestive notation and language as we did with matrices (of scalars) before. One thing to note, however, is that in the equation defining matrix multiplication ((3.2.1.18)), upon generalizing to this context, the multiplication denoted by juxtaposition should be interpreted there as composition in *postfix notation*, that is, $B^k{}_j A^i{}_k := A^i{}_k \circ B^k{}_j$ (otherwise the composition wouldn't make sense in general).

R We write $\text{Matrix}_{m\times n}$ for the set of all $m \times n$ matrices. Note that we need not specify the ground ring as we did before (e.g. as $\text{Matrix}_{m\times n}(\mathbb{K})$) because this is implicitly contained in the data given in m and n—they are collections of $\mathbb{K}$-modules. In case $m = n$, we may write $\text{Matrix}_m := \text{Matrix}_{m\times m}$. As before, $\text{Matrix}_{m\times n}$ has the structure of a (commutative) group always, it will additionally have the structure of a $\mathbb{K}$-module if $\mathbb{K}$ is commutative, and Matrix_m has the structure of a ring.

R If the two collection of $\mathbb{K}$-modules are finite, say $\{W^1, \dots, W^m\}$ and $\{V^1, \dots, V^n\}$, then a $\{W^1, \dots, W^m\} \times \{V^1, \dots, V^n\}$ matrix should be thought of as a double-indexed array $A^i{}_j$, $1 \le i \le m$ and $1 \le j \le n$, where $A^i{}_j : V^j \to W^i$ is a linear-transformation from V^j to W^i. As before, this will be written

$$A = \begin{bmatrix} A^1{}_1 & \cdots & A^1{}_n \\ \vdots & \ddots & \vdots \\ A^m{}_1 & \dots & A^m{}_n \end{bmatrix}. \tag{4.4.1.74}$$

We will see later that this will define a linear-transformation $V^1 \times \cdots \times V^n \to W^1 \times \cdots \times W^m$. Indeed, that is somehow the point of matrices of linear-transformations—they make it easier to think about linear-transformations between products.

R If $A^i{}_j = 0$ for $i \neq j$, we write

$$A^1{}_1 \oplus \cdots \oplus A^m{}_m := \begin{bmatrix} A^1{}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A^m{}_n \end{bmatrix}. \quad (4.4.1.75)$$

This matrix of linear-transformations is the ***direct-sum***. Matrices of this form are referred to as ***Block-diagonal***.[a]

[a] It is of course just a diagonal matrix in our old terminology, but in this context it is far more common to say "block-diagonal" to emphasize that the entries on the diagonal are not scalars but linear-transformations.

Before moving on, we introduce a convention that will prove quite convenient.

Identifying matrices with the linear-transformations they define

Consider a linear-transformation $T : V \to W$. In case $V = \mathbb{K}^n$ and $W = \mathbb{K}^m$, V and W have canonical bases (the standard bases), and so, in a sense, vectors and linear-transformations really are 'the same as' column-vectors and matrices respectively. Ordinarily this identification is arbitrary because it depends on a choice of basis, but not so in this case. Thus, one can be sloppy and fail to make a distinction between a matrix and the linear-transformation it defines. Previously, we didn't do this because (i) pedagogy and (ii) it wasn't really necessary. Of course, it's still not *strictly* necessary, but now it will prove to rather useful.

For example, it is quite cumbersome to say "Consider the linear-transformation $\mathbb{C}^3 \to \mathbb{C}^3$ defined by the follow matrix of linear-transformations

$$\begin{bmatrix} T_A & 0 \\ 0 & T_B \end{bmatrix}, \quad (4.4.1.76)$$

where $T_A : \mathbb{C} \to \mathbb{C}$ is the linear-transformation defined by the matrix $A := \begin{bmatrix} 5 \end{bmatrix}$ and $T_B : \mathbb{C}^2 \to \mathbb{C}^2$ is the linear-transformation defined by

the matrix

$$B := \begin{bmatrix} -3 & 1 \\ 0 & -3 \end{bmatrix}.", \tag{4.4.1.77}$$

especially when you consider that I could be sloppy and alternatively say "Consider the following linear-transformation $\mathbb{C}^3 \to \mathbb{C}^3$

$$\begin{bmatrix} 5 & 0 & 0 \\ 0 & -3 & 1 \\ 0 & 0 & -3 \end{bmatrix}.". \tag{4.4.1.78}$$

Thus, hereafter, we do not guarantee to be careful about making distinctions between matrices and the linear-transformations they define—we trust that by this point in the notes the conceptual difference between the two is firmly cemented in your mind—though we will still make the distinction if it's convenient. Related to this is that you should now consider definitions made for linear-transformations as also being 'officially' made for matrices. For example, we defined above the term "block-diagonal matrix of linear-transformations". A ***block-diagonal matrix*** (of scalars) is one such that the matrix of linear-transformations with respect to the given direct-sum decomposition of the linear-transformation defined by the matrix is block-diagonal. For example,

$$\begin{bmatrix} 1 & 2 & 3 & 0 & 0 \\ 4 & 5 & 7 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \tag{4.4.1.79}$$

is a block-diagonal matrix of scalars, whereas

$$\begin{bmatrix} 1 & 2 & 3 & 0 & -13 \\ 4 & 5 & 7 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \tag{4.4.1.80}$$

is not. Similarly, we may speak of direct-sums of matrices and so on.

▪ **Example 4.4.1.81 — Direct-sum of matrices** For example,

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \oplus \begin{bmatrix} -1 & 1 & -2 & 2 \\ -3 & 3 & -4 & 4 \\ 1 & 2 & -5 & -6 \end{bmatrix} := \begin{bmatrix} 1 & 2 & 3 & 0 & 0 & 0 & 0 \\ 4 & 5 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & -2 & 2 \\ 0 & 0 & 0 & -3 & 3 & -4 & 4 \\ 0 & 0 & 0 & 1 & 2 & -5 & -6 \end{bmatrix} \tag{4.4.1.82}$$

We now turn to defining the coordinates of a linear-transformation with respect to direct-sum decompositions. Our ability to do this will follow from what are in their own right important properties of direct-sum decompositions. The first of these properties is that direct-sum decompositions of a vector space allow one to define a linear-transformation by defining what it does on all the "summands". The second of these properties is the dual property involving mapping *into* summands. We state both results here.

Theorem 4.4.1.83 — Finite direct-sums are biproducts. Let U and V be $\mathbb{K}$-modules, and let $V_1, \ldots, V_m \subseteq V$ be subspaces such that $V = V_1 \oplus \cdots \oplus V_m$.

(i). Let $S_k : U \to V_k$ be linear. Then, there is a unique linear-transformation $S : U \to V$ such that $S_k = \text{proj}_{V_k} \circ S$ for $1 \leq k \leq m$.

(ii). Let $T_k : V_k \to U$ be linear. Then, there is a unique linear-transformation $T : V \to U$ such that $T|_{V_k} = T_k$ for $1 \leq k \leq m$.

R More explicitly, the first implies that

$$S(u) = S_1(u) + \cdots + S_m(u) \tag{4.4.1.84}$$

for all $u \in U$. Likewise, the second implies that

$$T(v_1 + \cdots + v_m) = T_1(v_1) + \cdots + T_m(v_m) \quad (4.4.1.85)$$

for $v_k \in V_k$.

R You should draw an analogy between the property stated in (i) and the corresponding property for *Cartesian products* of sets, namely, that you can define a function $Z \to X \times Y$ by specifying its "components" $Z \to X$ and $Z \to Y$. You will learn when you study category theory in more depth that these both serve examples of *limits*, in fact a special type of limit called a *product* (one in the category of $\mathbb{K}$-modules and the other in the category of sets).

R Dually, you should draw an analogy between the property stated in (ii) and the corresponding property for *disjoint-unions* of sets, namely, that you can define a function $X \coprod Y \to Z$ by specifying its "restrictions" $X \to Z$ and $Y \to Z$. You will learn when you study category theory in more depth that these both serve examples of *colimits*, in fact a special type of colimit called a *coproduct* (one in the category of $\mathbb{K}$-modules and the other in the category of sets).

R The term *biproduct* comes from the fact that $W_1 \oplus \cdots \oplus W_m$ is both a product and a coproduct (though the definition is not quite that simple).

R Warning: While (ii) generalizes to arbitrary direct-sums, (i) *fails* in this case—this is why we stuck to the case of finitely-many subspaces in this result.

Proof. We leave this as an exercise.

Exercise 4.4.1.86 We leave this as an exercise.

■

Combining these two properties, with both the domain and the codomain as a direct-sum, we obtain the following.

Theorem 4.4.1.87 — Coordinates of a linear-transformation (with respect to a decomposition). Let V and W be $\mathbb{K}$-modules, let $\mathscr{V} =: \{V_1, \dots, V_n\}$ and $\mathscr{W} =: \{W_1, \dots, W_m\}$ be collections of subspaces of V and W respectively such that $V = V_1 \oplus \cdots \oplus V_n$ and $W = W_1 \oplus \cdots \oplus W_m$, and let $T : V \to W$ be a linear-transformation. Then, there is a unique $m \times n$ matrix, $[T]_{\mathscr{W} \leftarrow \mathscr{V}}$, the ***coordinates*** with respect to the decompositions $\mathscr{V}$ and $\mathscr{W}$, such that

$$[T(v)]_{\mathscr{W}} = [T]_{\mathscr{W} \leftarrow \mathscr{V}} [v]_{\mathscr{V}} \tag{4.4.1.88}$$

for all $v \in V$.

Furthermore, explicitly

$$[T]_{\mathscr{W} \leftarrow \mathscr{V}} = \begin{bmatrix} T^1{}_1 & \cdots & T^1{}_n \\ \vdots & \ddots & \vdots \\ T^m{}_1 & \dots & T^m{}_n \end{bmatrix}, \tag{4.4.1.89}$$

where we have defined

$$\mathrm{proj}_{W_i} \circ T|_{V_j} =: T^i{}_j := \mathrm{proj}_{W_i} \circ T\big|_{V_j}. \tag{4.4.1.90}$$

R Perhaps the most important thing for you to remember about this is an expression for T in terms of the $T^i{}_j$ s:

For $v \in V$, write $v = v^1 + \cdots + v^n$ for unique $v^k \in V^k$. Then,

$$T(v) = \left(\sum_{j=1}^{n} T^1{}_j (v^j) \right) + \cdots + \left(\sum_{j=1}^{n} T^m{}_j (v^j) \right).$$

That is, the i^{th} coordinate of $T(v)$ with respect to the decomposition $W = W^1 \oplus \cdots \oplus W^m$ is given by

$$T(v)^i = \sum_{j=1}^{n} T^i{}_j (v^j). \tag{4.4.1.91}$$

R To be clear, $[v]_{\mathscr{V}} \in V^1 \times \cdots \times V^n$, $[T(v)]_{\mathscr{W}} \in W^1 \times \cdots \times W^m$, and $[T]_{\mathscr{W} \leftarrow \mathscr{V}} : V^1 \times \cdots \times V^n \to W^1 \times \cdots \times W^m$.

Proof. We leave this as an exercise.

Exercise 4.4.1.92 Prove the result.

■

As before, this yields an isomorphism from the space of linear-transformations to the space of matrices (of linear-transformations).

Proposition 4.4.1.93 — $[\cdot]_{\mathscr{W} \leftarrow \mathscr{V}}$ is an isomorphism Let $\mathbb{K}$ be a cring, let V and W be $\mathbb{K}$-modules, and let $V = V^1 \oplus \cdots \oplus V^n$ and $W = W^m \oplus \cdots \oplus W^m$ be direct-sum decompositions of V and W respectively. Then,

$$\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W) \ni T \mapsto [T]_{\mathscr{W} \leftarrow \mathscr{V}} \in \mathrm{Matrix}_{\mathscr{W} \times \mathscr{V}} \quad (4.4.1.94)$$

is an isomorphism of $\mathbb{K}$-modules, where $\mathscr{V} := \{V^1, \ldots, V^n\}$ and $\mathscr{W} := \{W^1, \ldots, W^m\}$.

R In particular, we have that

$$[T_1 + T_2]_{\mathscr{W} \leftarrow \mathscr{V}} = [T_1]_{\mathscr{W} \leftarrow \mathscr{V}} + [T_2]_{\mathscr{W} \leftarrow \mathscr{V}} \quad (4.4.1.95)$$

and

$$[\alpha \cdot T]_{\mathscr{W} \leftarrow \mathscr{V}} = \alpha \cdot [T]_{\mathscr{W} \leftarrow \mathscr{V}}. \quad (4.4.1.96)$$

R If $\mathbb{K}$ weren't commutative, this instead would only be an isomorphism of groups.

Proof. We leave this as an exercise.

Exercise 4.4.1.97 Prove the result.

■

The (external) direct-sum

Looking back at Theorem 4.4.1.83, we see that if a module $V = V_1 \oplus \cdots \oplus V_m$ is a finite direct-sum, then to define maps *into*, it suffices to define the components of the map into each V_k. Dually, to define a map *out of* V, it suffices to define the map on each V_k. What happens if the direct-sum is infinite?

The answer is that there are spaces which have these properties, but they may no longer coincide. For example, we have the following result about *products* of modules.

Proposition 4.4.1.98 Let V be a $\mathbb{K}$-module, let $\mathscr{W}$ be an indexed collection of $\mathbb{K}$-modules, and for each $W \in \mathscr{W}$ let $T_W : V \to W$ be a linear-transformation. Then, there is a unique linear-transformation $T : V \to \prod_{W \in \mathscr{W}} W$ such that $T_W = \text{proj}_W \circ T$ for all $W \in \mathscr{W}$.

R You should compare this with Theorem 4.4.1.83(i). You should find that it says almost the same exact thing, except with the change of some letters and we now allow $\mathscr{W}$ to be arbitrary (instead of just finite).

Proof. We leave this as an exercise.

Exercise 4.4.1.99 Prove the result.

■

This leaves us to address the question of the "out of" case. The answer is that it is essentially the direct-sum that has this property, but so far we only know "Give a module, is this module a direct-sum of blah blah blah subspaces?". We don't yet know how to create *new* spaces out of old ones by taking direct-sums. The following definition does just that.

Definition 4.4.1.100 — External direct-sum of modules Let $\mathscr{V}$ be an indexed collection of $\mathbb{K}$-modules. Then, the ***external direct-sum*** of $\mathscr{V}$, $\bigoplus_{V\in\mathscr{V}} V$ is defined by

$$\bigoplus_{V\in\mathscr{V}} V := \left\{\langle v^V : V \in \mathscr{V}\rangle : \text{cofinitely many } v^V = 0.\right\}.$$

R That is, it is the subspace of the Cartesian product consisting of those elements with only finitely many nonzero coordinates. For example, this is exactly analogous to the difference between $\mathbb{C}^\infty$ and $\mathbb{C}^{\mathbb{N}}$. Indeed, these are respectively the external direct-sum and Cartesian product of countably-infinitely many copies of $\mathbb{C}$.

We had first better check that it makes sense to refer to this as the "external *direct-sum*".

Proposition 4.4.1.101 Let $\mathscr{V}$ be an indexed collection of $\mathbb{K}$-modules. Then, the external direct-sum $\bigoplus_{V\in\mathscr{V}} V$ is the direct-sum of the elements of $\mathscr{V}$.

R To be clear, we regard each $V_0 \in \mathscr{V}$ as a subspace of $\bigoplus_{V\in\mathscr{V}}$. For example, if $\mathscr{V} = \{V_1, V_2, V_3\}$, then we identity V_2 with

$$\{\langle 0, v_2, 0\rangle \in V_1 \oplus V_2 \oplus V_3 : v_2 \in V_2\}. \quad (4.4.1.102)$$

After making this identification, we can then ask the question "Is this $\mathbb{K}$-module the direct-sum (in the old sense) of the subspaces $\mathscr{V}$.". This result says the answer is "Yes.", which justifies using essentially the same term to refer to both concepts (the old definition in Definition 4.4.1.1 and the definition of the external direct-sum).

Proof. We leave this as an exercise.

Exercise 4.4.1.103 Prove the result.

■

Finally, we check that the external direct-sum has the desired "out of" property described at the beginning of this subsubsection.

Proposition 4.4.1.104 Let $\mathscr{V}$ be an indexed collection of $\mathbb{K}$-modules, let W be a $\mathbb{K}$-module, and for each $V \in \mathscr{V}$ let $T_V : V \to W$ be a linear-transformation. Then, there is a unique linear-transformation $T : \bigoplus_{V \in \mathscr{V}} \to W$ such that $T|_V = T_V$ for all $V \in \mathscr{V}$.

R You should compare this with Theorem 4.4.1.83(ii). You should find that it says almost the same exact thing, except with the change of some letters and we now allow $\mathscr{V}$ to be arbitrary (instead of just finite).

Proof. We leave this as an exercise.

Exercise 4.4.1.105 Prove the result.

■

Thus, the *Cartesian product* of modules satisfies the "into" property described above and the *(external) direct-sum* satisfies the "out of" property described above. However, according to Proposition 4.4.1.68, the direct-sum and Cartesian product are canonically isomorphic if there are only finitely many modules, which is why in Theorem 4.4.1.83 we say that a finite direct-sum satisfies both of these properties.[3]

4.4.2 Invariant subspaces

At the beginning of the previous subsection, we explained that we sought to decompose V into simpler pieces, with the hopes that

[3]For what it's worth, this property means that the Cartesian product is the *product* in the category of $\mathbb{K}$-modules and the other property means that the direct-sum is the *coproduct* in the category of $\mathbb{K}$-modules. For finitely-many modules, the product and coproduct agree, but in general they do not.

this would enable us to associate a relatively simple matrix to a linear-transformation. In this subsection, we investigate the *types* of subspaces we would like to decompose V into in order to achieve this: *invariant subspaces*.[4] If we can decompose V as a direct-sum of smaller T-invariant subspaces, then the form that the matrix of T takes will simplify into a *block-diagonal* matrix—see Theorem 4.4.2.11.

Before turning to the the definition of invariant subspace itself, we first investigate a new example of an R-module that will prove moderately useful in the things to come.

▪ **Example 4.4.2.1 — The $\mathbb{K}[x]$-module defined by a linear-transformation** Let $\mathbb{K}$ be a ring. Before we get to the module itself, note that, while we have previously only thought of $\mathbb{K}[x]$ as a $\mathbb{K}$-module, it also has the canonical structure of a ring: the addition is the same and the multiplication now is just 'ordinary' multiplication of polynomials.[a] This is exactly analogous to how we can consider $\mathbb{R}$ to be both a vector space and a ring.

Having noted that $\mathbb{K}[x]$ has the structure of a ring (so that "$\mathbb{K}[x]$-module" actually makes sense), let us turn to examining the $\mathbb{K}[x]$-module itself. To define this $\mathbb{K}[x]$-module, we must first start with a $\mathbb{K}$-module V and a $\mathbb{K}$-linear operator $T\colon V \to V$.

We now define the $\mathbb{K}[x]$-module as follows: The underlying set of vectors is the same as before, V; the addition is the same as it was before; but now scaling $\mathbb{K}[x] \times V \to V$ is defined by

$$(\alpha_0+\alpha_1 x+\cdots+\alpha_m x^m)\cdot v \coloneqq \alpha_0\cdot v+\alpha_1\cdot T(v)+\cdots+\alpha_m\cdot T^m(v).$$

Intuitively, we require that $x \cdot v \coloneqq T(v)$, and then the "action" of every other polynomial is determined in the obvious way (e.g. $x^2 \cdot v \coloneqq T^2(v)$).

[4] In an ideal world, we could choose these smaller pieces to not just be T-invariant but in fact be eigenspaces, but of course, if we could do that, everything would be diagonalizable, and we wouldn't be discussing this in the first place.

Exercise 4.4.2.2 Check that this actually satisfies the axioms of a $\mathbb{K}[x]$-module.

R If ever V is a $\mathbb{K}$-module and T is a $\mathbb{K}$-linear operator on V, if we say "V is a $\mathbb{K}[x]$-module", it should be understood that the $\mathbb{K}[x]$-module structure we are referring to is the one defined in this example. While I don't want to make the notation 'official',[b] if I want to regard V as a $\mathbb{K}[x]$-module instead of a $\mathbb{K}$-module, I will instead write V_T. Of course, the set of "vectors" itself hasn't change, but this notation indicates to you that I am thinking of the same set of vectors *with different "scalars"*.

[a] This works just like you think it would, with the caveat that the coefficients are assumed to *commute* with x, even if $\mathbb{K}$ is noncommutative. For example, $(\alpha x)\cdot(\beta + x^2) = \alpha\beta x + \alpha x^2$. This assumption is a reasonable one because, as you will see shortly, x is going to act as if it were a linear-transformation, and linear-transformations commute with all scalars, no matter how noncommutative $\mathbb{K}$ might be.

[b] Because the notation is not unique enough to make it effectively unambiguous.

Regarding V as a $\mathbb{K}[x]$-module in this way is just a fancy way of saying that we have defined what $p(T)$ means, $T\colon V \to V$ a $\mathbb{K}$-linear operator and p a polynomial. For example, if $p(x) := 3x^3 - 5x^2 + 2$, then $p(T)\colon V \to V$ is the $\mathbb{K}$-linear transformation

$$\begin{aligned} v \mapsto [p(T)](v) &:= [3T^3 - 5T^2 + 2](v) \\ &:= 3T(T(T(v))) - 5T(T(v)) + 2v. \end{aligned} \tag{4.4.2.3}$$

After having discussed eigenvalues, we can say a little more about these operators—see Proposition 4.2.48.

This example allows us to make the following definition.

Definition 4.4.2.4 — Invariant subspace Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be a $\mathbb{K}$-linear operator, and let $W \subseteq V$ be a subspace. Then, W is ***T*-invariant** iff W is a $\mathbb{K}[x]$-submodule of V.

R If T is clear from context, we may simply say ***invariant***.

R This is succinct but obtuse—see the following proposition for a more down-to-earth characterization of what this means.

R Recall that (Definition 1.2.1.1) "submodule" is synonymous with "subspace". We use the term "submodule" here to emphasize the distinction between thinking of V as a $\mathbb{K}$-module versus a $\mathbb{K}[x]$-module.

R Note that subspaces which satisfy Definition 4.2.1(i) are automatically T-invariant. In particular, eigenspaces are invariant subspaces.

R Strictly speaking, we didn't really *need* the $\mathbb{K}[x]$-module defined in Example 4.4.2.1 to state this definition, and it is admittedly easier to understand characterization in the following proposition. Nonetheless, I decided to present it this way (i) to give you practice thinking about nonartificial examples of R-modules that are not vector spaces, (ii) I personally find it more elegant, and (iii) it is more systematic in the sense that the term "invariant subspace" is used in more general contexts where it can analogously be defined as a particular submodule.

Proposition 4.4.2.5 Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be a $\mathbb{K}$-linear operator, and let $W \subseteq V$ be a subspace. Then, W is T-invariant iff $T(w) \in W$ for all $w \in W$.

R This makes it clear one reason why invariant subspaces might be useful: if W is invariant, then $T|_W\colon W \to W$, that is, T can be considered as a linear operator on W.

R Of course, said another way, this is the same as the statement $T(W) \subseteq W$.

Proof. We leave this as an exercise.

Exercise 4.4.2.6 Prove this yourself.

■

■ **Example 4.4.2.7** Define $D\colon \mathbb{R}[x] \to \mathbb{R}[x]$ by $D(p) \coloneqq p'$. Then, $\mathbb{R}[x]_m \subseteq \mathbb{R}[x]$ is a D-invariant subspace for all $m \in \mathbb{N}$.[a]

[a] Recall (Example 1.1.27) that $\mathbb{R}[x]_m$ is the subspace of all polynomials of degree at most m.

One fact we will find useful is that projections onto invariant subspaces are "compatible" with the linear operator.

Proposition 4.4.2.8 Let V be a $\mathbb{K}$-module, let $V = U \oplus W$ be a direct-sum decomposition, and let $T\colon V \to V$ be a linear operator. Then, if U and W are T-invariant, then

$$\mathrm{proj}_U \circ T = T \circ \mathrm{proj}_U \quad \text{and} \quad \mathrm{proj}_W \circ T = T \circ \mathrm{proj}_W\,. \tag{4.4.2.9}$$

Proof. Suppose that U and W are T-invariant. Let $v \in V$ and write $v = u + w$ for unique $u \in U$ and $w \in W$. Then, $T(v) = T(u) + T(w)$. By invariance, $T(u) \in U$ and $T(w) \in W$, so by definition of projections, $\mathrm{proj}_U(T(v)) = T(u) \coloneqq T(\mathrm{proj}_U(v))$. Hence, $\mathrm{proj}_U \circ T = T \circ \mathrm{proj}_U$. Similarly for W. ■

We know now that we can't always find a basis in which the matrix of a linear operator is diagonal. Our knowledge of direct-sums from the previous subsection suggests that perhaps we can get what is in a sense the 'next best thing': a *block-diagonal* matrix. Before, we saw that the matrix our our linear-transformation will be diagonal iff the basis consisted of eigenvectors. Our goal now then is to determine when the matrix of our linear-transformation with respect to a *direct-sum decomposition* is block-diagonal. As eigenspaces were special types of invariant subspaces, we might guess that the more general invariant subspaces will work. Indeed, this is the case.

Definition 4.4.2.10 — Block-diagonalizable Let V be a finite-dimensional vector space and let $T: V \to V$ be linear. Then, T is ***block-diagonalizable*** iff there is a direct-sum decomposition $V = V^1 \oplus \cdots \oplus V^m$ such that $[T]_{\mathscr{V} \leftarrow \mathscr{V}}$ is a block-diagonal matrix, where $\mathscr{V} := \{V^1, \ldots, V^m\}$.

R In this case, $[T]_{\mathscr{V} \leftarrow \mathscr{V}}$ is the ***block-diagonalization*** of T.

Theorem 4.4.2.11 — Fundamental Theorem of Block-diagonalizability. Let V be a finite-dimensional vector space and let $T: V \to V$ be linear. Then, the following are equivalent.

(i). T is block-diagonalizable.
(ii). There is a direct-sum decomposition of V consisting of T-invariant subspaces.
(iii). There are T-invariant subspaces $V^1, \ldots, V^m$ such that

$$\dim(V) = \dim(V^1) + \cdots + \dim(V^m). \quad (4.4.2.12)$$

In this case, $[T]_{\mathscr{V} \leftarrow \mathscr{V}}$ is a block-diagonal matrix, where $\mathscr{V} := \{V^1, \ldots, V^m\}$.

R Let $V = V^1 \oplus \cdots \oplus V^m$ be a direct-sum decomposition of V consisting of T-invariant subspaces. As each V^k is invariant, T restricts to a linear-transformation $T^k := T|_{V^k}: V^k \to V^k$. Using this notation, we have

$$[T]_{\mathscr{V} \leftarrow \mathscr{V}} = \begin{bmatrix} T^1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & T^m \end{bmatrix} =: T^1 \oplus \cdots \oplus T^m. \quad (4.4.2.13)$$

R Warning: This name is nonstandard—there is no standard name for this result.

Proof. We leave this as an exercise.

Exercise 4.4.2.14 Prove the result.

■

Indecomposability

Of course, $V = V$ is itself a direct-sum decomposition, and one that generally won't be very useful. In order to simplify the block-diagonal form as much as possible, we wish to break up V into the 'smallest' invariant subspaces we can. The precise sense in which we want these subspaces to the the "smallest" possible is called *indecomposable*.

Definition 4.4.2.15 — Indecomposable Let V be a R-module. Then, V is ***indecomposable*** iff whenever $V = U \oplus W$, it follows that either $U = 0$ or $W = 0$.

R If V is a $\mathbb{K}$-module and $T\colon V \to V$ is a linear operator, we say that V is ***T-indecomposable*** iff V is indecomposable when regarded as a $\mathbb{K}[x]$-module (Example 4.4.2.1).

R If we say that a subspace $W \subseteq V$ is T-indecomposable, it is implicit that it is also T-invariant (otherwise it wouldn't actually possess the structure of a $\mathbb{K}[x]$-module, and so the definition given in the previous remark wouldn't make sense).

R You can view the requirement that V be nonzero as roughly analogous to how we disallow $1 \in \mathbb{Z}$ from being considered prime.

R Warning: The term "irreducible" (Definition C.5.1) is *not* the same as "indecomposable" (Example C.5.3), though they are certainly related—irreducible implies indecomposable (Proposition C.5.2).

R Warning: Some authors do not consider the 0 module to be indecomposable. (Presumably their reason for doing so is similar to the reason why $1 \in \mathbb{Z}^+$ is not considered prime.)

We now consider whether we can, and if so, how can we, decompose V into indecomposable submodules. The basic idea is as follows. If V is indecomposable, we're done; otherwise, there are proper nonzero submodules $U, W \subseteq V$ such that $V = U \oplus W$. If U and W are indecomposable, again, we're done; otherwise, we can break up U and/or W as a direct-sum of proper nonzero submodules, and so on. In general, there is no need for this process to terminate. However, the next result says that it does in the primary case of interest.

Proposition 4.4.2.16 Let V be a finite-dimensional vector space and let $T\colon V \to V$ be linear. Then, there are finitely-many T-indecomposable subspaces $V^1, \ldots, V^m \subseteq V$ such that

$$V = V^1 \oplus \cdots \oplus V^m. \tag{4.4.2.17}$$

R For what it's worth, modules that can be written as direct-sums of indecomposable modules are known as ***completely-decomposable*** modules. Here, we would be regarding V as a $\mathbb{F}[x]$-module, $\mathbb{F}$ the ground field,[a] in which case we would say that V is ***T-completely-decomposable*** as short-hand for the statement "V is a completely-decomposable $\mathbb{F}[x]$-module.".

R Warning: This will not be true in general—see Exercise 4.4.2.18.

[a] All vector spaces are 'trivially' completely-decomposable—every basis gives a direct-sum decomposition into $\mathbb{F}$-invariant subspaces.

Proof. If V is indecomposable, we are done. Otherwise, there are proper nonzero invariant subspaces $U_1, U_2 \subseteq V$ such that $V = U_1 \oplus U_2$. Note that as V is finite-dimensional and these are proper subspaces, we have that $\dim(U_1), \dim(U_2) < \dim(V)$.

Again, if each U_1 and U_2 are indecomposable, we are done; otherwise, we can write these as the direct-sum of invariant subspaces whose dimensions are strictly less than $\dim(U_1)$ and $\dim(U_2)$ respectively.

Repeating this process inductively, the process either stops because everything is indecomposable, or we have reached that point where there are no proper nonzero subspaces, in which case the subspace has to have dimension 1, and so must be indecomposable. Thus, we eventually find that $V = V_1 \oplus \cdots \oplus V_M$ for $V_k \subseteq V$ indecomposable subspaces, as desired. ■

Exercise 4.4.2.18 What is an example of a $\mathbb{K}$-module that is not completely-decomposable? Can you find one that is an $\mathbb{F}[x]$-module?

Now seems an appropriate time to return to a counter-example we mentioned previously, namely, a subspace of a $\mathbb{K}$-module with no complement.

▪ **Example 4.4.2.19 — A subspace of a $\mathbb{K}$-module with no complement** Define $\mathbb{K} := \mathbb{C}$, $V := \mathbb{C}^2$, $U := \text{Span}(\langle 1, 0\rangle)$, and let $T_A : V \to V$ be the $\mathbb{C}$-linear-transformation defined by the matrix

$$A := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \tag{4.4.2.20}$$

Note that $U \subseteq V$ is a $\mathbb{C}[x]$-submodule, that is, it is T_A-invariant. We claim that it has no complement.

We proceed by contradiction: let $W \subseteq V$ be a $\mathbb{K}[x]$-submodule such that $V = U \oplus W$ (as $\mathbb{C}[x]$-modules). W is then in particular a $\mathbb{C}$-subspace, and so, by a dimension count, we must have $W = \text{Span}(\langle a, b\rangle)$ for $a, b \in \mathbb{C}$, $b \neq 0$. However, $N(\langle a, b\rangle) = \langle b, 0\rangle \notin W$, and so W is not N-invariant, no matter what a and b are.

R Essentially this same argument shows that V is an indecomposable $\mathbb{C}[x]$-module. In particular, this serves as an example of an indecomposable module with proper nonzero submodules.[a]

[a] One might naively think that if $U \subseteq V$ is proper and nonzero, we can write $V = U \oplus W$ for $W \subseteq V$ also proper nonzero, as we can with vector spaces, and so the existence of such a U implies decomposability. This example shows that this naive thinking is wrong.

4.4.3 Generalized "Eigenstuff"

After realizing that we won't always be able to find a basis in which the matrix of a given linear-transformation was diagonal, we set out to find the 'next best thing'. In the previous sections, we decided that instead we should only try to find a *block*-diagonal matrix, and in order to do that, we should decompose V into invariant subspaces. Furthermore, in order to simplify the description as much as possible, we would like these subspaces not to just be invariant but to be *indecomposable*.

A glimpse of generalized-eigenspaces

Our first hint at how we might do all this is given by the following result Proposition 4.4.3.2.

Proposition 4.4.3.1 Let V be a finite-dimensional vector space and let $T\colon V \to V$ be linear. Then,

$$0 \subseteq \operatorname{Ker}(T) \subseteq \cdots \subseteq \operatorname{Ker}(T^{\dim(V)}) = \operatorname{Ker}(T^{\dim(V)+1}) = \cdots .$$

Proof. Let $v \in \operatorname{Ker}(T^k)$. Then, $T^k(v) = 0$, and so $T^{k+1}(v) := T(T^k(v)) = 0$, and so $v \in \operatorname{Ker}(T^{k+1})$. Hence, $\operatorname{Ker}(T^k) \subseteq \operatorname{Ker}(T^{k+1})$.

If $\operatorname{Ker}(T^m) = \operatorname{Ker}(T^{m+1})$, then in fact $\operatorname{Ker}(T^m) = \operatorname{Ker}(T^n)$ for all $n \geq m$. To see this, write $n = m + k$ for $k \in \mathbb{N}$ and let $v \in \operatorname{Ker}(T^{m+k})$, so that $T^{m+1}(T^{k-1}(v)) = T^{m+k}(v) = 0$. Then, $T^{k-1}(v) \in \operatorname{Ker}(T^{m+1}) = \operatorname{Ker}(T^m)$, and so in fact

$T^m(T^{k-1}(v)) = T^{m+k-1}(v) = 0$. Proceeding inductively, we eventually find that $T^m(v) = 0$.

Thus, if there is some $m \leq \dim(V)$ such that $\text{Ker}(T^m) = \text{Ker}(T^{m+1})$, we are done. Otherwise, 0 is properly contained in $\text{Ker}(T)$, which is properly contained in $\text{Ker}(T^2)$, etc.. This means that $\dim(\text{Ker}(T^k)) \geq \dim(\text{Ker}(T^{k-1})) + 1$ for $1 \leq k \leq \dim(V)$, and hence $\dim(\text{Ker}(T^{\dim(V)})) \geq \dim(V)$,[a] in which case we must have $\text{Ker}(T^{\dim(V)}) = \text{Ker}(T^m)$ for all $m \geq \text{Ker}(T)$, as desired. ■

[a] As you go from 0, to $\text{Ker}(T)$, to $\text{Ker}(T^2)$, etc., you must increase the dimension by 1 at each step, and so by the time you get to $\text{Ker}(T^{\dim(V)})$, the dimension must be at least $\dim(V)$.

Proposition 4.4.3.2 Let V be a vector space over a division ring $\mathbb{F}$, let $T: V \to V$ be linear, let $\lambda \in \mathbb{F}$ be central, and let $m \in \mathbb{N}$. Then, if $\text{Ker}([T-\lambda]^m) = \text{Ker}([T-\lambda]^{m+1})$, then,

$$V = \text{Ker}([T-\lambda]^m) \oplus \text{Im}([T-\lambda]^m) \tag{4.4.3.3}$$

is a direct-sum decomposition of V into T-invariant subspaces.

R Note by the previous result that, if V is finite-dimensional, we always have

$$V = \text{Ker}([T-\lambda]^{\dim(V)}) \oplus \text{Im}([T-\lambda]^{\dim(V)}). \tag{4.4.3.4}$$

R In fact, they are invariant subspaces for all $m \in \mathbb{N}$—we needn't assume anything about m for this part of the result to hold.

R Note that $\text{Eig}_\lambda = \text{Ker}(T-\lambda) \subseteq \text{Ker}([T-\lambda]^{\dim(V)})$, that is, the first invariant subspace here contains the λ-eigenspace of T.[a]

R We will see later that, if $\lambda \in \mathbb{F}$ is an eigenvalue of T, then $\text{Ker}([T-\lambda]^{\dim(V)})$ is the *λ-generalized-eigenspace* of T.

[a] Strictly speaking, we shouldn't be using this notation or language if λ is not an eigenvalue. In any case, the inclusion of the kernels stated remains valid.

Proof. We first check that these are invariant subspaces. Let $v \in \mathrm{Ker}([T-\lambda]^m)$. As T computes with $T-\lambda$, we have that

$$[T-\lambda]^m(T(v)) = T\left([T-\lambda]^m(v)\right) = T(0) = 0, \quad (4.4.3.5)$$

and so $T(v) \in \mathrm{Ker}([T-\lambda]^m)$.

Let $v = [T-\lambda]^m(w) \in \mathrm{Im}([T-\lambda]^m)$. Then,

$$T(v) = T\left([T-\lambda]^m(w)\right) = [T-\lambda]^m\left(T(w)\right), \quad (4.4.3.6)$$

and so $T(v) \in \mathrm{Im}([T-\lambda]^m)$.

It suffices to prove the rest of the result for $\lambda = 0$ (this is the same as proving the result for arbitrary T linear). By Corollary 4.4.1.28, it suffices to show that (i) $V = \mathrm{Ker}(T^m) + \mathrm{Im}(T^m)$ and that (ii) $\mathrm{Ker}(T^m) \cap \mathrm{Im}(T^m) = 0$.

We first check that $\mathrm{Ker}(T^m) \cap \mathrm{Im}(T^m) = 0$. So, let $v = T^m(w) \in \mathrm{Ker}(T^m) \cap \mathrm{Im}(T^m)$. We thus have that

$$0 = T^m(v) = T^{2m}(w), \quad (4.4.3.7)$$

and hence $w \in \mathrm{Ker}(T^{2m})$. By Proposition 4.4.3.1, $\mathrm{Ker}(T^m) = \mathrm{Ker}(T^{2m})$, and so in fact $w \in \mathrm{Ker}(T^m)$, and hence $v = T^m(w) = 0$.

It now follows that

$$\begin{aligned} &\dim(\mathrm{Ker}(T^m) + \mathrm{Im}(T^m)) \\ &\quad = \dim(\mathrm{Ker}(T^m)) + \dim(\mathrm{Im}(T^m)) \\ &\quad = {}^a m, \end{aligned} \quad (4.4.3.8)$$

and hence $V = \mathrm{Ker}(T^m) + \mathrm{Im}(T^m)$. ∎

[a] By the Rank-Nullity Theorem (Theorem 2.2.2.2).

The next idea is to apply this decomposition inductively: List the distinct eigenvalues of T, $\lambda_1, \ldots, \lambda_m$, write $V = \mathrm{Ker}([T-\lambda_1]^{\dim(V)}) \oplus W_1$, where we have defined $W_1 := \mathrm{Im}([T-\lambda_1]^{\dim(V)})$, write $W_1 = \mathrm{Ker}([T-\lambda_2|_{W_1}]^{\dim(W_1)}) \oplus W_2$, where we have defined $W_2 := \mathrm{Im}([T-\lambda_2]|_{W_1}{}^{\dim(V)}$, and so on. With any luck, we will find

$W_m = 0$, so that V can be written as a finite direct-sum of subspaces of the form $\mathrm{Ker}([T - \lambda]^{\dim(V)})$.

That said, the issue or not of whether we can make such a decomposition is going to be irrelevant if we don't understand the behavior of T on subspaces of the form $\mathrm{Ker}([T - \lambda])^{\dim(V)})$. In brief, $T - \lambda$ is *nilpotent* on this subspace, which brings us to the next subsubsection.

Nilpotent linear operators

Before we begin a study if nilpotency proper, let us briefly consider an alternative perspective one can take on finding the "next best thing" to diagonalization.

Let $T : V \to V$ be a linear operator and let $\mathcal{B}$ be a basis for V. As we can't always find a $\mathcal{B}$ such that $[T]_{\mathcal{B}}$ is diagonal, we instead try to see if we can find a $\mathcal{B}$ such that

$$[T]_{\mathcal{B}} = D + N, \tag{4.4.3.9}$$

where D is diagonal and N is 'small' (i.e. 'close' to 0) in some sense.

To see what notion of "small" we might want, recall that we are going to try to decompose V into subspaces of the form $\mathrm{Ker}([T - \lambda]^{\dim(V)})$, and so are also interested in understanding the behavior of the restriction of T to these subspaces. If this were simply $\mathrm{Ker}(T - \lambda)$, that is, an eigenspace,[5] we would have $T - \lambda = 0$ on this subspace—in the notation above, we have $D = \lambda$ and $N = 0$. However, we don't quite have that for the subspace $\mathrm{Ker}([T - \lambda]^{\dim(V)})$. Rather, we only have that the restriction of $T - \lambda$ to this subspace is *nilpotent*. It is in this sense that N will be "small".

Definition 4.4.3.10 — Nilpotent Let X be a rg and let $x \in X$. Then, x is ***nilpotent*** iff there is some $m \in \mathbb{N}$ such that $x^m = 0$.

R The smallest natural number $\mathrm{Rank}(x) \in \mathbb{N}$ such that $x^{\mathrm{Rank}(x)} = 0$ is the ***rank*** of x.

R For us, the rg we're going to be interested in is in fact a ring, $\mathrm{End}_{\mathbb{K}\text{-}\mathbf{Mod}}(V)$, V a $\mathbb{K}$-module, and which

[5] At least for λ an eigenvalue.

case for $T: V \to V$ to be nilpotent means that there is some $m \in \mathbb{N}$ such that $T^m = 0$, where

$$T^m := \underbrace{T \circ \cdots \circ T}_{m}, \tag{4.4.3.11}$$

that is, T composed with itself m times.

R For $N: V \to V$ nilpotent and $v \in V$, we say that v is ***N*-maximal** iff it is *not* the case that $v = N(w)$ for some $w \in V$.[a] Of course, the definition of nilpotent always guarantees that there is some N-maximal element (except for the stupid case $N = 0$).

Note that this is the notion of maximal that corresponds to the preorder $\preceq$ defined by $v \preceq w$ iff $v = N^k(m)$ for some $k \in \mathbb{N}$.

[a] This is just the statement that $v \notin \mathrm{Im}(N)$, though saying "v is N-maximal" is more suggestive in this context for reasons that will hopefully become more apparent later on.

■ **Example 4.4.3.12** Let N be a strictly upper-triangular matrix. Then, N is nilpotent.

Exercise 4.4.3.13 Check this.

One of the first things we note about nilpotent operators is that they have but one possible eigenvalue: zero.

Proposition 4.4.3.14 Let V be a vector space, let $N: V \to V$ be linear, and let $\lambda \in \mathbb{F}$ be an eigenvalue. Then, if N is nilpotent, $\lambda = 0$.

R In fact, except for the silly case $V = 0$ (in which case no operator can have any eigenvalue), 0 will be an eigenvalue of N.

Proof. Suppose that N is nilpotent. By definition, there is then some $m \in \mathbb{N}$ such that $N^m = 0$. By Corollary 4.2.51, it follows that $\lambda^m = 0$, whence $\lambda = 0$ because the ground ring is a division ring. ■

This has an important, albeit unfortunate, consequence.

Corollary 4.4.3.15 Let V be a finite-dimensional vector space and let $N \colon V \to V$ be nilpotent linear. Then, N is diagonalizable iff $N = 0$.

R Moreover, we will see later that, in a sense, having a nonzero 'nilpotent part' is the only way in which a linear operator can fail to be diagonalizable.

Proof. ($\Rightarrow$) Suppose that N is diagonalizable. Then, there is a basis of V consisting of eigenvectors of N. By the previous result, the corresponding eigenvalues are all 0, and so N vanishes on each of these basis vectors. Hence, $N = 0$.

($\Leftarrow$) Suppose that $N = 0$. Then, $[N]_{\mathcal{B}}$ will be a diagonal[a] matrix for any basis $\mathcal{B}$ of V. ■

[a] To accommodate the silly case in which $V = 0$, note that the empty matrix is vacuously diagonal.

We thus know that nilpotent linear-transformations are essentially never diagonalizable, so if we are to come up with a 'next best thing' to diagonalization, we had at the very least know how to do so for nilpotent linear-transformations. The following result is our solution to this problem.

Theorem 4.4.3.16 — Jordan Canonical Form of Nilpotent Operators. Let V be a nonzero finite-dimensional vector space, let $N \colon V \to V$ be nilpotent linear, let $v_0 \in V$ be nonzero, and

let $r \in \mathbb{N}$ be the smallest natural number such that $N^r(v_0) = 0$. Then,

(i). $$N^\infty(v_0) := \{N^{r-1}(v_0), \ldots, N(v_0), v_0\} \quad (4.4.3.17)$$

is linearly-independent;

(ii). $$\mathrm{Span}(N^\infty(v_0)) \quad (4.4.3.18)$$

is N-indecomposable;

(iii). $$\mathrm{Span}(N^\infty(v_0)) \quad (4.4.3.19)$$

is maximal N-indecomposable if $v_0 \in V$ is N-maximal; and

(iv). if V is N-indecomposable and $v_0 \in V$ is N-maximal, then $N^\infty(v_0)$ is a basis of V that has the property that

$$[N]_{N^\infty(v_0) \leftarrow N^\infty(v_0)} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}. \quad (4.4.3.20)$$

R Intuitively, one can think of this as follows. Starting with v_0, if you want something that is N-invariant, that something had better contain $N(v_0)$, $N^2(v_0)$, and so on. This gives you $N^\infty(v_0)$. If you then want that something to be a subspace, you had better taken the span to obtain $\mathrm{Span}(N^\infty(v_0))$. In turns out that this is N-indecomposable, is maximal if v_0 is N-maximal, and furthermore, the matrix of N with respect to this basis is particularly simple—see (4.4.3.20).

R Note that (Proposition 4.4.2.16) we can always write V as a direct-sum of finitely many N-indecomposable submodules, and so in the general case (when V is not necessarily indecomposable), we can use this result to obtain a basis $\mathcal{B}$ of V that has the property that $[N]_{\mathcal{B}\leftarrow\mathcal{B}}$ will be a direct-sum of matrices of the above form.

Proof. (i) Suppose that

$$0 = \alpha_0 \cdot v_0 + \cdots + \alpha_{r-1} \cdot N^{r-1}(v_0). \tag{4.4.3.21}$$

Applying N^{r-1} to this equation, we obtain $0 = \alpha_0 \cdot N^{r-1}(v_0) = 0$, and hence α_0. Applying N^{r-2} in the same way, we find α_1. Proceeding inductively, we eventually find that every $\alpha_k = 0$, establishing linear-independence.

(ii) Let $U, W \subseteq \mathrm{Span}(N^\infty(v_0))$ be N-invariant subspaces such that $\mathrm{Span}(N^\infty(v_0)) = U \oplus W$. Either U or W must contain some vector v for which $N^{r-1}(v) \neq 0$. Without loss of generality, suppose U contains such a vector $v \in U$. Writing

$$v = \alpha_0 \cdot v_0 + \cdots + \alpha_{r-1} \cdot N^{r-1}(v_0), \tag{4.4.3.22}$$

we see that $\alpha_0 \neq 0$ (otherwise $N^{r-1}(v) = 0$). By N-invariance, we must have that

$$\alpha_0 \cdot N^{r-1}(v_0) = N^{r-1}(v) \in U, \tag{4.4.3.23}$$

and so as $\alpha_0 \neq 0$, $N^{r-1}(v_0) \in U$. It follows that

$$v - \alpha_{r-1} \cdot N^{r-1}(v_0) = \alpha_0 \cdot v_0 + \cdots + \alpha_{r-2} \cdot N^{r-2}(v_0) \in U.$$

Continuing this process inductively, eventually we obtain that all terms in (4.4.3.22) with nonzero coefficients are elements of U, and so in particular $v_0 \in U$. But then $U = \mathrm{Span}(N^\infty(v_0))$, and so $\mathrm{Span}(N^\infty(v_0))$ is indecomposable.

(iii) Suppose that $v_0 \in V$ is N-maximal. Let $W \supseteq \text{Span}(N^\infty(v_0))$ be N-indecomposable. We wish to show that $W = \text{Span}(N^\infty(v_0))$. To do this, we proceed by induction.

STEP 1: START THE PROOF OF SPANNING WITH INDUCTION

The statement we prove by induction (on $\text{Rank}(N)$) is as follows.

> If N is a nilpotent linear operator on a finite-dimensional vector space V and $v_0 \in V$ is N-maximal, then $\{N^{\text{Rank}(N)-1}(v_0), \ldots, v_0\}$ spans V.

First take $\text{Rank}(N) =: r = 1$, so that $N = 0$. In this case, every subspace is N-invariant, and so indecomposability forces $\dim(V) = 1$, so that indeed $V = \text{Span}(v_0)$.

Now suppose the result is true for $r-1$. If r is the smallest positive integer such that $N^m = 0$ on V, then $r-1$ is the smallest positive integer such that $N^{r-1} = 0$ on $\text{Im}(N)$. Furthermore, $N(v_0) \in \text{Im}(N)$ is such that $N^{(r-1)-1}(N(v_0)) = N^{r-1}(v_0) \neq 0$. Thus, if we can show that $\text{Im}(N)$ is indecomposable still, then the induction hypothesis will gives us that $\text{Im}(N) = \text{Span}(N^{r-1}(v_0), \ldots, N(v_0))$.

STEP 2: SHOW THAT $\text{Im}(N)$ IS INDECOMPOSABLE

So, let $U, W \subseteq \text{Im}(N)$ be subspaces and suppose that $\text{Im}(N) = U \oplus W$ with U and W N-invariant. Then write $V = U \oplus W \oplus V'$ for some subspace $V' \subseteq V$ (by Proposition 4.4.1.47). For every $v \in V'$, we may write

$$\begin{aligned} N(v) &= \text{proj}_U(N(v)) + \text{proj}_W(N(v)) \\ &= {}^a N(\text{proj}_U(v)) + N(\text{proj}_W(v)) \\ &=: N(v_U) + N(v_W), \end{aligned} \tag{4.4.3.24}$$

where we have written $v_U := \mathrm{proj}_U(v)$ and $v_W := \mathrm{proj}_W(v)$. Let $\mathcal{B}'$ be a basis for V', and define

$$\check{\mathcal{B}} := \{b - b_U : b \in \mathcal{B}'\} \tag{4.4.3.25}$$

and $\check{V} := \mathrm{Span}(\check{\mathcal{B}})$. From (4.4.3.24), we see that $N(b - b_U) = N(b_W) \in W$, and so $W + \check{V}$ is an invariant subspace. Thus, if we can show $V = U \oplus W \oplus \check{V}$, indecomposability will imply that either $U = 0$ or $W \oplus \check{V} = 0$, so that either $U = 0$ or $W = 0$, as desired.

So, suppose that $0 = u + w + \check{v}$ for $u \in U$, $w \in W$, and $\check{v} \in \check{V}$. Write $\check{v} = \alpha_1(b_1 - [b_1]_U) + \cdots + \alpha_m(b_m - [b_m]_U)$, so that

$$0 = \left(u - \sum_{k=1}^{m} \alpha_k [b_k]_U\right) + w + \sum_{k=1}^{r} \alpha_k b_k. \tag{4.4.3.26}$$

As $V = U \oplus W \oplus W'$, it follows that $\sum_{k=1}^{r} \alpha_k b_k = 0$, whence each $\alpha_k = 0$ by linear-independence, that $w = 0$, and that $u = \sum_{k=1}^{r} \alpha_k [b_k]_U = 0$. By Proposition 4.4.1.18, it just remains to check that $V = U + W + \check{V}$.

So, let $v \in V$. We may then write $v = u + w + v'$ for $u \in U$, $w \in W$, and $v' \in V'$. Write $v' = \alpha_1 b_1 + \cdots + \alpha_r b_r$. Then,

$$v' = \left(u + \sum_{k=1}^{r} \alpha_k [b_k]_U\right) + w + \sum_{k=1}^{r} \alpha_k (b_k - [b_k]_U) \in U + W + \check{V},$$

as desired. Thus, $\mathrm{Im}(T)$ is indecomposable, and hence $\mathrm{Im}(N) = \mathrm{Span}(N^{r-1}(v_0), \ldots, N(v_0))$.

Step 3: Finish the proof of spanning

Extend the linear-independent set $\mathcal{B} := \{N^{r-1}(v_0), \ldots, v_0\}$ to a basis C of V such that $C \supseteq \mathcal{B}$. We wish to show that $C = \mathcal{B}$. So, let $c \in C \setminus \mathcal{B}$. As $N(c) \in \mathrm{Im}(N)$, we can write

$$\begin{aligned} N(c) &= \alpha_1 N(v_0) + \cdots + \alpha_{r-1} N^{r-1}(v_0) \\ &= N\left(\alpha_1 v_0 + \cdots + \alpha_{r-1} N^{r-2}(v_0)\right). \end{aligned} \tag{4.4.3.27}$$

Now define

$$\check{c} := c - \sum_{k=1}^{r-1} \alpha_k N^{k-1}(v_0) \tag{4.4.3.28}$$

as well as $\check{\mathcal{A}} := \{\check{c} : c \in C \setminus \mathcal{B}\}$. (4.4.3.27) implies that $N(\check{c}) = 0$. In particular, $\check{V} := \mathrm{Span}(\check{C})$ is invariant. Thus, if we can show that $V = \mathrm{Span}(\mathcal{B}) \oplus \mathrm{Span}(\check{\mathcal{A}})$, indecomposability will force $\mathrm{Span}(\check{\mathcal{A}}) = 0$, hence $\check{\mathcal{A}} = \emptyset$, hence $C \setminus \mathcal{B} = \emptyset$, hence $C = \mathcal{B}$, completing the proof.

Thus, it remains only to check that $V = \mathrm{Span}(\mathcal{B}) \oplus \mathrm{Span}(\check{\mathcal{A}})$. So, let $v \in \mathrm{Span}(\mathcal{B}) \cap \mathrm{Span}(\check{\mathcal{A}})$. We could then write this vector as a linear-combination of both elements of $\mathcal{B}$ and elements of $\check{\mathcal{A}}$. Using the definition of the $\check{c}$s in (4.4.3.28), we see that this would yield a nontrivial linear-dependence relation about elements of $\mathcal{B}$ and elements of $C \setminus \mathcal{B}$ unless $v = 0$. By linear-dependence of C then, we have that $\mathrm{Span}(\mathcal{B}) \cap \mathrm{Span}(\check{\mathcal{A}}) = 0$.

Exercise 4.4.3.29 Finish the proof by showing that $V = \mathrm{Span}(\mathcal{B}) + \mathrm{Span}(C)$.

R Hint: You might try an argument similar to the one we used to show that $V = U + W + \check{V}$ in Step 2.

(iv) Suppose that V is N-indecomposable and $v_0 \in V$ is N-maximal. By the previous part, $\mathrm{Span}(N^\infty(v_0))$ is maximal indecomposable, and so by maximality we have $V = \mathrm{Span}(N^\infty(v_0))$. As we already knew it was linearly-independent (by (i)), it follows that $\mathrm{Span}(N^\infty(v_0))$ is a basis of V. Finally, (4.4.3.20) follows from the fact that $N(N^{r-1}(v_0)) = 0$ and $N(N^k(v_0)) = N^{k+1}(v_0)$ for $0 \leq k < r - 1$. ■

[a] N commutes with the projections because the subspaces are invariant—see Proposition 4.4.2.8.

The use of nilpotent operators is far more common, and in our primary case of interest, it will work just fine. However, for the purposes of dealing with generalized-eigenspaces in general, a related concept is more natural, that of *local-nilpotency*.

Definition 4.4.3.30 — Locally-nilpotent Let V be an R-module and let $T \in R$. Then, T is ***locally-nilpotent*** iff for every $v \in V$ there is some $m_v \in \mathbb{N}$ such that $T^{m_v} \cdot v = 0$.

R Of course, we're interested in the case V is a $\mathbb{K}[x]$-module with module structure defined as usual by a given linear-transformation $T : V \to V$, in which case we say that T is ***locally-nilpotent*** iff $x \in \mathbb{K}[x]$ is. Explicitly, T is locally-nilpotent iff for every $v \in V$ there is some $m_v \in \mathbb{N}$ such that $T^{m_v}(v) = 0$.

R Intuitively, the difference between nilpotency and local-nilpotency if the depends of m_v on V. For local-nilpotency, you are allowed pick a different m_v for each $v \in V$; for nilpotency on the other hand, you must be able to pick a single $m \in \mathbb{N}$ that 'works' "uniformly" for all $v \in V$.

Thus, it is clear from the definitions that a nilpotent linear-transformation is locally-nilpotent.

▪ **Example 4.4.3.31 — A locally-nilpotent operator that is not nilpotent** Consider the left-shift operator $L : \mathbb{C}^\infty \to \mathbb{C}^\infty$ (Example 1.1.48). Let $a \in \mathbb{C}^\infty$. By definition of $\mathbb{C}^\infty$, $m \mapsto a_m$ is eventually 0, so that there is some M such that whenever $m \geq M$ it follows that $a_m = 0$. Then $L^M(a_m) = 0$, and hence L is locally-nilpotent.

To see that L is not nilpotent, note that for every $m \in \mathbb{N}$, the sequence $a \in C^\infty$ that is identically 0 except for a 1 at index m is not 'killed' by L^m: $L^m(a) \neq 0$. Hence, $L^m \neq 0$ for any $m \in \mathbb{N}$, and hence L is not nilpotent.

For $m \in \mathbb{N}$, let $E_m \subseteq \mathbb{C}^\infty$ be the subspace of sequences which vanish for indices larger than m. Note that T is nilpotent on E_m, but not nilpotent on all of $\mathbb{C}^\infty$. Thus, there is no maximal subspace on which T is nilpotent.

R This fact is mentioned later when we discuss generalized-eigenspaces, and in particular, why locally-nilpotent, and not nilpotent, is the notion that should be used in the general definition.

On the other hand, in finite-dimensions, they are equivalent.

Proposition 4.4.3.32 Let V be a finite-dimensional vector space and let $T\colon V \to V$ be linear. Then, T is nilpotent iff it is locally-nilpotent.

Proof. ($\Rightarrow$) This is always true.

($\Leftarrow$) Suppose that T is locally-nilpotent. Let $\mathcal{B} =: \{b_1, \dots, b_d\}$ be a basis for V. Let $m_k \in \mathbb{N}$ be such that $T^{m_k}(b_k) = 0$. Define $m := \max\{m_1, \dots, m_d\}$. Then, $T^m(b_k) = 0$ for all $1 \leq k \leq m$. Let $v \in V$ and write $v = v^1 \cdot b_1 + \cdots + v^d \cdot b_d$. Then,

$$T^m(v) = v^1 \cdot T^m(b_1) + \cdots + v^d \cdot T^m(b_d) = 0. \quad (4.4.3.33)$$

Hence, $T^m = 0$, and so T is nilpotent. ∎

More than a glimpse of generalized-eigenspaces

Having understood the behavior of T on subspaces of the form $\mathrm{Ker}([T - \lambda]^{\dim(V)})$, it is time we actually decompose V into such subspaces. Before we do so, we give such subspaces a name.

Definition 4.4.3.34 — Generalized-eigenspaces Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be linear, let $W \subseteq V$ be a nonzero subspace, and let $\lambda \in \mathbb{K}$. Then, W is a ***λ-generalized-eigenspace*** iff

(i). $T|_W = \lambda \operatorname{id}_W + N$ with $N\colon W \to W$ locally-nilpotent linear; and
(ii). W is maximal with this property.

R Such a λ is referred to a ***generalized-eigenvalue*** of T.[a]

R Warning: There is another meaning of the term "generalized-eigenvalue" which we will not study. As we will see in Proposition 4.4.3.41, generalized-eigenvalues in this sense are just the same as eigenvalues, after which point we will stop using of the term "generalized-eigenvalue".

R Nonzero elements of W are ***generalized-eigenvectors*** of T with eigenvalue λ.

R Note that it follows immediately from this that scaling by λ on W is linear. Furthermore, we shall see shortly (Proposition 4.4.3.41) that generalized-eigenvalues are just eigenvalues,[b] and so will in particular be central, at least for vector spaces (Theorem 4.2.16).

R See the definition of eigenspaces (Definition 4.2.1) for some other potentially useful remarks that apply equally well here.

[a] We will see (Proposition 4.4.3.41) that in fact generalized-eigenvalues are the same as the eigenvalues. So in particular, we don't introduce a separate notation for the set of generalized-eigenvalues.

[b] Which is why you probably won't see the term "generalized-eigenvalue" in most places—it turns out they're just the same as eigenvalues, and so people just stick with using the single term "eigenvalue" for everything.

As before, we start by establishing uniqueness of generalized-eigenspaces.

Proposition 4.4.3.35 — Generalized-eigenspaces are unique Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be linear, let $\lambda \in \mathbb{K}$, and let $U, W \subseteq V$ be λ-generalized-eigenspaces of T. Then, $U = W$.

R We denote the unique λ-generalized-eigenspace of V by $\mathrm{Eig}^{\infty}_{\lambda,T}$ (for reasons that we will understand shortly).[a] If T is clear from context, we may simply write $\mathrm{Eig}^{\infty}_{\lambda} := \mathrm{Eig}^{\infty}_{\lambda,T}$.

R If ever we write "$\mathrm{Eig}^{\infty}_{\lambda,T}$" without having explicitly said so, it should be assumed that λ is an eigenvalue of T.

R If $\mathbb{K}$ is a division ring (so that we can talk about dimension, then the ***multiplicity*** of $\lambda \in \mathrm{Eig}(T)$ is $\dim(\mathrm{Eig}^{\infty}_{\lambda})$. This may also be referred to as ***algebraic multiplicity*** if we wish to distinguish it from the geometric multiplicity.[b]

[a] See Definition 4.4.3.51 to see why the use of "∞" is appropriate here.

[b] The justification for the term "algebraic" here is that this coincides with the power of the factor $(x - \lambda)$ is the characteristic polynomial of T—see Theorem 5.7.2.120.

Proof. We leave this as an exercise.

Exercise 4.4.3.36 Prove the result.

R See the proof of Proposition 4.2.4.

■

Proposition 4.4.3.37 — Generalized-eigenspaces are maximum with their defining property Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be linear, let $W \subseteq V$ be a subspace, and let $\lambda \in \mathbb{K}$ be a generalized-eigenvalue of V. Then,

if $T|_W = \lambda \operatorname{id}_W + N$ with $N\colon W \to W$ locally-nilpotent linear, then $W \subseteq \operatorname{Eig}^\infty_\lambda$.

R A corollary of this is that, to show that λ is a generalized-eigenvalue, it suffices to exhibit a single nonzero subspace W on which $T - \lambda$ is locally-nilpotent linear. For this result implies that $\operatorname{Eig}^\infty_\lambda \supseteq W$, so that if W is nonzero, so is $\operatorname{Eig}^\infty_\lambda$, in which case λ would be a generalized-eigenvalue.

R Note that this is one reason why we prefer locally-nilpotent over nilpotent in the definition of generalized-eigenspaces. Were we to use "nilpotent" in place of "locally-nilpotent" in the definition, this result would fail. A counter-example is given by the left-shift operator on $\mathbb{C}^\infty$—see Example 4.4.3.31.

Proof. Suppose that $T|_W = \lambda \operatorname{id}_W + N$ with $N\colon W \to N$ locally-nilpotent linear. Define

$$\mathscr{U} := \left\{U \subseteq V \text{ a subspace} : T|_U - \lambda \operatorname{id}_U \text{ is locally-nilpotent linear.}\right\} \tag{4.4.3.38}$$

and

$$E := \sum_{U \in \mathscr{U}} U. \tag{4.4.3.39}$$

Let $e \in E$ and and write $e = u_1 + \cdots + u_m$ for some $u_1 \in U_1, \ldots, u_m \in U_m$ with $U_1, \ldots, U_m \in \mathscr{U}$. As $T - \lambda$ is locally-nilpotent on U_k, there is some $n_k \in \mathbb{N}$ such that $[T - \lambda]^{m_k}(u_k) = 0$. Define $n := \max\{n_1, \ldots, n_m\}$. Then,

$$[T-\lambda]^n(e) = [T-\lambda]^n(u_1)+\cdots+[T-\lambda]^n(u_m) = 0. \tag{4.4.3.40}$$

That is, $T|_E = \lambda \operatorname{id}_E + N$ with $N\colon E \to E$ locally-nilpotent linear. E is maximal with this property, and hence $E = \operatorname{Eig}^\infty_\lambda$. Finally, note that $W \in \mathscr{U}$, and hence $W \subseteq E = \operatorname{Eig}^\infty_\lambda$. ∎

Proposition 4.4.3.41 Let V be a $\mathbb{K}$-module, let $T: V \to V$ be linear, and let $\lambda \in \mathbb{K}$. Then, λ is a generalized-eigenvalue of T iff it is an eigenvalue of T.

R Thus, hereafter, we will likely stick with just "eigenvalue" and stop using the term "generalized-eigenvalue".

Proof. ($\Rightarrow$) Suppose that λ is a generalized-eigenvalue of T. Then, $\mathrm{Eig}^{\infty}_{\lambda} \subseteq V$ is a subspace of V on which $T - \lambda$ is locally-nilpotent and is maximal with this property.

For succinctness of notation, let us temporarily write $N \coloneqq T - \lambda|_{\mathrm{Eig}^{\infty}_{\lambda}}$, so that $N: \mathrm{Eig}^{\infty}_{\lambda} \to \mathrm{Eig}^{\infty}_{\lambda}$ is locally-nilpotent linear. If $\mathrm{Ker}(N) = 0$, then N would be injective, and so N^m would be injective for all $m \in \mathbb{N}$, and hence N couldn't possibly be locally-nilpotent. Thus, $\mathrm{Ker}(N) \subseteq V$ is a nonzero subspace such that $T|_{\mathrm{Ker}(N)} = \lambda\,\mathrm{id}_{\mathrm{Ker}(N)}$, and therefore λ is an eigenvalue of T.

($\Leftarrow$) Suppose that λ is an eigenvalue of T. Then, Eig_{λ} is a nonzero subspace on which $T - \lambda$ is locally-nilpotent, and so λ is a generalized-eigenvalue of T. ∎

Proposition 4.4.3.42 — Generalized-eigenvalues are unique (in vector spaces) Let V be a vector space and let $T: V \to V$ be linear. Then, if $\mathrm{Eig}^{\infty}_{\lambda,T} = \mathrm{Eig}^{\infty}_{\mu,T}$, it follows that $\lambda = \mu$.

Proof. Suppose that $\mathrm{Eig}^{\infty}_{\lambda,T} = \mathrm{Eig}^{\infty}_{\mu,T}$. For convenience, let us write $\mathrm{Eig}^{\infty}_{\lambda,T} =: E \coloneqq \mathrm{Eig}^{\infty}_{\mu,T}$. There is then a locally-nilpotent operator $N: E \to E$ such that

$$\lambda\,\mathrm{id}_E + N = T|_E = \mu\,\mathrm{id}_E + N \tag{4.4.3.43}$$

Let $v \in E$ be nonzero. Then,

$$\lambda v + N(v) = \mu v + N(v), \tag{4.4.3.44}$$

and hence $(\lambda - \mu)v = 0$. As $v \neq 0$ and the ground ring is a division ring, we must have that $\lambda - \mu = 0$, that is, $\lambda = \mu$. ■

We also have a result analogous to Theorem 4.2.16 that is useful for actually 'calculating' generalized-eigenspaces.

Theorem 4.4.3.45. Let V be a vector space over a division ring $\mathbb{F}$, let $T : V \to V$ be linear, and let $\lambda \in \mathbb{F}$. Then, if λ is an eigenvalue of T, then

$$\begin{aligned} \mathrm{Eig}^{\infty}_{\lambda,T} &= \{v \in V : [T - \lambda]^m(v) = 0 \text{ for some } m \in \mathbb{N}.\} \\ &= \bigcup_{m \in \mathbb{N}} \mathrm{Ker}([T - \lambda]^m). \end{aligned}$$

In fact, if V is finite-dimensional, then

$$\mathrm{Eig}^{\infty}_{\lambda,T} = \mathrm{Ker}([T - \lambda]^{\dim(V)}). \tag{4.4.3.46}$$

R The analogous result for eigenvalues Theorem 4.2.16 had two parts whereas this result only has one. This is because the first part of Theorem 4.2.16 gives an explicit characterization of eigenvalues, but as eigenvalue and generalized-eigenvalues are the same, there is no additional characterization here.

Proof. Suppose that λ is an eigenvalue of T. Define

$$\begin{aligned} W &:= \{v \in V : [T - \lambda]^m(v) = 0 \text{ for some } m \in \mathbb{N}.\} \\ &= \bigcup_{m \in \mathbb{N}} \mathrm{Ker}([T - \lambda]^m). \end{aligned} \tag{4.4.3.47}$$

Exercise 4.4.3.48 Check that W is a subspace.

W contains $\mathrm{Ker}(T - \lambda)$, and so is nonzero as λ is an eigenvalue. By definition, $T - \lambda$ is locally-nilpotent on W.

To show maximality, let $U \supseteq W$ be a subspace such that $T|_U = \lambda \operatorname{id}_U + N$ for $N\colon U \to U$ locally-nilpotent. Then, for every $u \in U$, there is some $m \in \mathbb{N}$ such that $N^m(u) = 0$, in which case $[T-\lambda]^m(u) = N^m(u) = 0$. Thus, $u \in W$, so that $U \subseteq W$, showing maximality. Hence,

$$\begin{aligned} W &:= \{v \in V : [T-\lambda]^m(v) = 0 \text{for some } m \in \mathbb{N}.\} \\ &= \operatorname{Eig}^\infty_{\lambda,T}\,. \end{aligned} \tag{4.4.3.49}$$

Now suppose that V is finite-dimensional. It follows from Proposition 4.4.3.1 that

$$\operatorname{Eig}^\infty_{T,\lambda} = \bigcup_{m\in\mathbb{N}} \operatorname{Ker}([T-\lambda]^m) = \operatorname{Ker}([T-\lambda]^{\dim(V)}). \tag{4.4.3.50}$$

■

Related to the fact that we can write the generalized-eigenspace as a union in this way is that we now have a notion of *rank*.[6]

Definition 4.4.3.51 — Rank (of generalized-eigenvectors) Let V be a $\mathbb{K}$-module, let $T\colon V \to V$ be linear, let $\lambda \in \mathbb{K}$ be an eigenvalue of T, and let $v \in \operatorname{Eig}^\infty_\lambda$. Then, the ***rank*** of v is the smallest natural number $\operatorname{Rank}(v)$ such that $[T-\lambda]^{\operatorname{Rank}(v)}(v) = 0$.

R For $m \in \mathbb{N}$, the ***rank*** m ***λ-eigenspace***, $\operatorname{Eig}^m_{T,\lambda}$, is defined by

$$\operatorname{Eig}^m_{T,\lambda} := \left\{v \in \operatorname{Eig}^\infty_{T,\lambda} : \operatorname{Rank}(v) \le m\right\}. \tag{4.4.3.52}$$

As before, we will often write $\operatorname{Eig}^m_\lambda := \operatorname{Eig}^m_{\lambda,T}$.

R We may say "rank m eigenvector" instead of the more verbose "rank m generalized-eigenvector"—the fact that we are mentioning the rank at all implies that we do not mean eigenvectors is the 'usual' sense (unless of course m happens to be 1).

[6] Well, I suppose we had a notion of rank before with just eigenvalues, but it's a bit silly because all eigenvalues have rank 1, as you'll see in the following definition.

R Warning: Note that $\mathrm{Eig}^m_{\lambda,T}$ is *not* the space of rank m eigenvectors, but rather, the space of generalized-eigenvectors with rank *at most* m. The set of generalized-eigenvectors with rank exactly equal to m is not a subspace in general.

R As $T - \lambda|_{\mathrm{Eig}^\infty_\lambda}$ is locally-nilpotent, there is by definition some such natural number.

R Note that the rank 1 generalized-eigenvectors are precisely the ('ordinary') eigenvectors. Also note that $0 \in \mathrm{Eig}^\infty_{\lambda,T}$ has rank 0, though it is technically not a generalized-eigenvector.

R Hence,

$$\mathrm{Eig}^1_{\lambda,T} = \mathrm{Eig}_{\lambda,T} \tag{4.4.3.53}$$

and

$$\mathrm{Eig}^0_{\lambda,T} = 0. \tag{4.4.3.54}$$

R Note that $\mathrm{Rank}(v) \leq \dim(V)$ if V is finite-dimensional by the previous result Theorem 4.4.3.45.

■ **Example 4.4.3.55** Define

$$A := \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}. \tag{4.4.3.56}$$

A has a single eigenvalue, 0. $e_1 := \langle 1, 0, 0\rangle$ is a generalized-eigenvector of rank 1 (so just an eigenvector), $e_2 := \langle 0, 1, 0\rangle$ is a generalized-eigenvector of rank 2, and $e_3 := \langle 0, 0, 1\rangle$ is a generalize-eigenvector of rank 3. e_1 should be clear. As for e_2, we can see that it has rank 2 because

$$Ae_2 \neq 0 \text{ but } A^2 e_2 = 0. \tag{4.4.3.57}$$

Similarly, we see that e_3 has rank 3 because

$$A^2 e_3 \neq 0 \text{ but } A^3 e_3 = 0. \tag{4.4.3.58}$$

Thus, $\{e_1, e_2, e_3\}$ is a basis of $\mathbb{R}^3$ consisting of generalized-eigenvectors of A, whose elements have rank 1, 2, and 3 respectively.

Note that this matrix is *not* diagonalizable, so there is *not* a basis of (regular) eigenvectors. Thus, generalizing to, well, generalized-eigenvectors has solved this problem.

Additionally, note that A is nilpotent and e_3 is A-maximal. According to Theorem 4.4.3.16, $\{e_3, Ae_3, A^2 e_3\}$ will be linearly-independent and indecomposable. Indeed, $Ae_3 = e_2$, and $A^2 e_3 = e_1$, so this is certainly linearly-independent.

When it comes to actually computing the Jordan canonical form of linear-transformations, you can't just use any basis of generalized-eigenvectors, but rather you have to pick your generalized-eigenvectors in a certain way. In general, you want to find the "maximal" generalized-eigenvectors and 'generate' a basis by applying the nilpotent operators as we have done here. We'll explain this in more detail later, so don't worry if this doesn't all make sense now.

▪ **Example 4.4.3.59** Define $D\colon C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$. From Example 4.2.31, we know that every $\lambda \in \mathbb{C}$ is an eigenvalue with eigenspace given by $\text{Eig}_\lambda = \text{Span}(e^{\lambda x})$. Let us now investigate the generalized-eigenspaces.

Let $m \in \mathbb{N}$, $\lambda \in \mathbb{C}$, and $f \in C^\infty(\mathbb{R})$. Then, $f \in \text{Eig}_\lambda^m$ iff

$$[D - \lambda]^m(f) = 0. \tag{4.4.3.60}$$

A basis for the set of solutions to this differential equation is given by

$$\left\{e^{\lambda x}, xe^{\lambda x}, \ldots, x^{m-2}e^{\lambda x}, x^{m-1}e^{\lambda x}\right\},^a \tag{4.4.3.61}$$

and hence

$$\mathrm{Eig}_\lambda^m = \mathrm{Span}\left(e^{\lambda x}, xe^{\lambda x}, \ldots, x^{m-2}e^{\lambda x}, x^{m-1}e^{\lambda x}\right). \quad (4.4.3.62)$$

[a] The existence and uniqueness theorem from ordinary differential equations implies that the set of solutions is an m-dimensional vector space. To find a basis, it thus suffices to exhibit m linearly-independent solutions. After staring at it for awhile, you realize that functions of the form $x^k e^{\lambda x}$ do the job. (Seriously, while you might have forgotten after it's become so familiar, ultimately even the solution $e^{\lambda x}$ is originally found by making an educated guess.)

Proposition 4.4.3.63 — Properties of higher rank eigenspaces Let V be a $\mathbb{K}$-module, let $T: V \to V$ be linear, and let $\lambda \in \mathbb{K}$ be an eigenvalue of T. Then,

(i).

$$\mathrm{Eig}_\lambda^m = \mathrm{Ker}([T-\lambda]^m); \quad (4.4.3.64)$$

(ii). $\mathrm{Eig}_\lambda^m \subseteq V$ is a T-invariant subspace; and
(iii).

$$\mathrm{Eig}_\lambda^0 \subseteq \mathrm{Eig}_\lambda^1 \subseteq \mathrm{Eig}_\lambda^2 \subseteq \cdots; \quad (4.4.3.65)$$

and
(iv). if $v \in \mathrm{Eig}_\lambda$ has rank $m \in Z^+$, then $[T-\lambda](v)$ has rank $m-1$.

R In particular, $\mathrm{Eig}_\lambda^0 = 0$ and $\mathrm{Eig}_\lambda^1 = \mathrm{Eig}_\lambda$.

Proof. We leave this as an exercise.

Exercise 4.4.3.66 Prove the result.

■

Recall (Proposition 4.2.40) that eigenvectors with distinct eigenvalues are linearly-independent. The same is true for generalized-

eigenvectors (and in fact this is a strict generalization of the previous result).

Proposition 4.4.3.67 — Generalized-eigenspaces with distinct eigenvalues are linearly-independent Let V be a vector space and let $T\colon V \to V$ be linear. Then,

$$\left\{\mathrm{Eig}_\lambda^\infty : \lambda \in \mathrm{Eig}(T)\right\} \tag{4.4.3.68}$$

is linearly-independent.

R Explicitly, this means that any collection of generalized-eigenvectors with distinct eigenvalues is linearly-independent.

Proof. Denote the ground division ring by $\mathbb{F}$. Let $\lambda_1, \ldots, \lambda_m \in \mathrm{Eig}(T)$ and $v_1 \in \mathrm{Eig}_{\lambda_1}^\infty, \ldots, v_m \in \mathrm{Eig}_{\lambda_m}^\infty$. Suppose that

$$0 = \alpha_1 \cdot v_1 + \cdots + \alpha_m \cdot v_m. \tag{4.4.3.69}$$

Let $n \in \mathbb{Z}$ be the smallest positive integer such that $w_1 \coloneqq [T - \lambda_1]^n(v_1) \neq 0$, so that $[T - \lambda_1](w_1) = 0$, that is, $T(w_1) = \lambda_1 w_1$. It follows that $[T - \lambda](w_1) = (\lambda_1 - \lambda)w$ for any $\lambda \in \mathbb{F}$. Apply $[T - \lambda_1]^n$ to this equation to obtain

$$0 = \alpha_1 \cdot w_1 + \cdots + \alpha_m \cdot w_m, \tag{4.4.3.70}$$

where we have defined $w_k \coloneqq [T - \lambda_1]^n(v_k)$.[a] Note that, as generalized-eigenspaces are T-invariant subspaces and $\lambda_1 \in \mathbb{F}$ is central, $w_k \coloneqq [T - \lambda_1]^n(v_k) \in \mathrm{Eig}_{\lambda_k}^\infty$ is still in the λ_k-generalized-eigenspace. Hence, for each $2 \leq k \leq m$, there is some $n_k \in \mathbb{Z}^+$ such that $[T - \lambda_k]^{n_k}(w_k) = 0$. Applying $[T - \lambda_2]^{n_2} \cdots [T - \lambda_m]^{n_m}$ to this equation, we thus find

$$0 = \alpha_1(\lambda_1 - \lambda_2)^{n_2} \cdots (\lambda_1 - \lambda_m)^{n_m}. \tag{4.4.3.71}$$

As the eigenvalues are distinct and we're working over a division ring, this implies that $\alpha_1 = 0$.

Proceeding inductively and doing the same thing for α_2, α_3, and so on, we eventually obtain $0 = \alpha_1 = \cdots = \alpha_m$, and so $\{v_1, \ldots, v_m\}$ is linearly-independent. ■

[a] The basic strategy for doing this is to hopefully reduce the argument to a similar one we used for the analogous result for eigenvectors (note of course that $w_1 := [T - \lambda_1]^n(v)_1$ is an eigenvectors of T with eigenvalue λ_1 by construction).

We are now essentially ready to put all the pieces together.

4.4.4 The Jordan Canonical Form Theorem

Okay, so that was a lie. There is still one minor detail we need to address: how do we know we have any eigenvalues at all!? Indeed, we don't know that. Because it's just not true. We saw in Example 4.3.11 an example of a linear-transformation that didn't have any eigenvalues. Fortunately, there is a natural hypothesis would can impose on the ground division ring in order to guarantee we have eigenvalues, in which case (Theorem 4.4.4.11), not only do we have a single eigenvalue, but we have 'enough' generalized-eigenvectors to generate the entire space. The hypothesis we speak of is that of being *algebraically closed*, a discussion of which, to a void yet another large interruption before we reach our goal (among other reasons), has been placed in the appendix (Definition C.3.3.1).

The theorem. Finally.

We're finally ready to state the Jordan Canonical Form Theorem, which, among other things, details the near-diagonal form our matrices will take in a suitable basis. To state it, however, it will be convenient to have a name for a special type of matrix appearing in the description.

Definition 4.4.4.1 — Jordan block Let $\mathbb{K}$ be a ring, let $\lambda \in \mathbb{K}$, and let $m \in \mathbb{Z}^+$. Then, the ***Jordan block***, $\mathrm{Jord}_{\lambda,m}$, of size

m with eigenvalue λ is the $m \times m$ matrix

$$\mathrm{Jord}_{\lambda,m} := \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}. \tag{4.4.4.2}$$

R Note that this can be written as

$$\mathrm{Jord}_{\lambda,m} = \lambda\,\mathrm{id} + N_m, \tag{4.4.4.3}$$

where we have used the notation

$$N_m := \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}. \tag{4.4.4.4}$$

■ **Example 4.4.4.5**

$$\mathrm{Jord}_{-2,3} := \begin{bmatrix} -2 & 1 & 0 \\ 0 & -2 & 1 \\ 0 & 0 & -1 \end{bmatrix} \tag{4.4.4.6}$$

and

$$\mathrm{Jord}_{1,1} := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \tag{4.4.4.7}$$

▪ **Example 4.4.4.8 — Jordan blocks and ranks of generalized-eigenvectors** Consider for the sake of example the Jordan block

$$\mathrm{Jord}_{5,4} := \begin{bmatrix} 5 & 1 & 0 & 0 \\ 0 & 5 & 1 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 5 \end{bmatrix}. \tag{4.4.4.9}$$

Note that the standard basis for $\mathbb{C}^4$ $\mathcal{S} =: \{e_1, e_2, e_3, e_4\}$ is a basis consisting of generalized-eigenvectors of $\mathrm{Jord}_{5,4}$. Furthermore, e_1 has rank 1, e_2 has rank 2, e_3 has rank 3, and e_4 has rank 4.

Exercise 4.4.4.10 Check all this.

Of course, none of this is specific to $\mathrm{Jord}_{5,4}$, and in general we have the following.

> For a Jordan block of size m, the standard basis is a basis of generalized-eigenvectors. The first has rank 1, the second has rank 2, and so on.
>
> In particular, *Jordan blocks have a single eigenvector* (up scaling).

And now, what is arguably the most important theorem in the entirety of the notes.[7]

Theorem 4.4.4.11 — Jordan Canonical Form Theorem. Let V be a finite-dimensional vector space over an algebraically closed field $\mathbb{F}$, let $T\colon V \to V$ be linear, and denote the eigenvalues of T by $\lambda_1, \ldots, \lambda_m$. Then,

[7] After reading the statement, if things are still unclear, you might consider jumping to the end of the proof, after which comes some more explanation.

(i).

$$V = \mathrm{Eig}^{\infty}_{\lambda_1} \oplus \cdots \oplus \mathrm{Eig}^{\infty}_{\lambda_m}; \tag{4.4.4.12}$$

(ii). the coordinates of T with respect to this direct-sum decomposition is

$$\begin{bmatrix} \lambda_1 \mathrm{id}_{\mathrm{Eig}^{\infty}_{\lambda_1}} + N_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_m \mathrm{id}_{\mathrm{Eig}^{\infty}_{\lambda_m}} + N_m \end{bmatrix}, \tag{4.4.4.13}$$

where $N_k : \mathrm{Eig}^{\infty}_{\lambda_k} \to \mathrm{Eig}^{\infty}_{\lambda_k}$ is nilpotent linear;

(iii). for every $1 \leq k \leq m$, there is a basis $\mathcal{B}_k$ for $\mathrm{Eig}^{\infty}_{\lambda_k}$ such that the coordinates

$$[\lambda_k \mathrm{id}_{\mathrm{Eig}^{\infty}_{\lambda_k}} + N_k]_{\mathcal{B}_k \leftarrow \mathcal{B}_k} \tag{4.4.4.14}$$

is a direct-sum of Jordan blocks with eigenvalue λ_k, in fact, $\mathcal{B}_k$ is the union of $N^{\infty}_k(v_0) := \{v_0, N(v_0), \ldots, N^{\mathrm{Rank}(N_k)-1}(v_0)\}$ as v_0 ranges over a chosen N_k-maximal from each N-indecomposable summand of $\mathrm{Eig}^{\infty}_{\lambda_k}$;

(iv). $\mathcal{B} := \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m$ is a basis for V such that the coordinates

$$[T]_{\mathcal{B} \leftarrow \mathcal{B}} \tag{4.4.4.15}$$

is the direct-sum of the matrices in (4.4.4.14); and

(v). if C is another basis of V that has the property that $[T]_{C \leftarrow C}$ is a direct-sum of Jordan blocks, then the set of Jordan blocks appearing in this decomposition is the same as the set of Jordan blocks appearing in the decomposition of $[T]_{\mathcal{B} \leftarrow \mathcal{B}}$.

R (4.4.4.12) is the ***generalized-eigenspace decomposition*** of V.

R The matrix in (4.4.4.15) is the[a] ***Jordan canonical form*** of T. It is also called the ***Jordan normal form*** of T, but I prefer "Jordan canonical form" for the simple reason that the word "normal" tends to be overused in mathematics. A basis in which the matrix of T is in Jordan canonical form is called a ***Jordan basis***.

R In short:

(i) says that V is a direct-sum of the generalized-eigenspaces.

(ii) says that the matrix of T with respect to this decomposition is block-diagonal with $\lambda_k \, \mathrm{id}_{\mathrm{Eig}^{\infty}_{\lambda_k}} + N_k$ on the diagonal.

(iii) says that we can choose bases for each of the generalized-eigenspaces in which the matrix associated to the linear operators $\lambda_k \, \mathrm{id}_{\mathrm{Eig}^{\infty}_{\lambda_k}} + N_k$ is a direct-sum of Jordan blocks.

(iv) says that these bases assemble together to form a basis for all of V for which the matrix of T is a direct-sum of the matrices of the previous part, and so in particular a direct-sum of Jordan blocks.

(v) says that the Jordan canonical form of T is essentially unique in the sense that, if you write T as a direct-sum of Jordan blocks, the Jordan blocks appearing in that decomposition must be exactly the same as the ones you found before.

R Note that it follows from this (and the comment made at the end of Example 4.4.4.8) that *the dimension of the λ eigenspace is equal to the number of Jordan blocks with eigenvalue λ appearing in the Jordan canonical form.*

R Note that a direct-sum of Jordan blocks of size 1 is a diagonal matrix, and so, by uniqueness, a matrix is diagonalizable iff all the the Jordan blocks appearing it its Jordan canonical form are of size 1, in which case the diagonalization is the same as its Jordan canonical form. Thus, Jordan canonical form is indeed a strict generalization of diagonalization.

R Warning: For diagonalizable linear operators, any basis of eigenvectors will serve as a diagonalizing basis, the analogous result is *not* true for Jordan canonical form. That is, it is *not* the case that $[T]_{\mathcal{B}}$ will be in Jordan canonical form for any basis of generalized-eigenvectors $\mathcal{B}$. One has to be a bit more careful—this is explained in more detail in (iii) and again after the proof of this result.

R In particular, T has at least one eigenvalue.

R In particular, generalized-eigenvectors with distinct eigenvalues are linearly-independent.

R This is one of the few times, and most likely the most significant time, where I was not able to remove the assumption of commutativity. The reason for this is that eigenvalues are central, and so you would need to assume that all nonconstant polynomials have *central* roots. But if you do that, then you automatically have a field![b]

[a] "The" is justified by the fact the the Jordan canonical form is essentially unique by (iv).

[b] For every $\alpha \in \mathbb{F}$, $x - \alpha$ would have a central root, implying that α is central.

Proof. (i) We proceed by (strong induction) on $\dim(V)$. If $\dim(V) = 0$, the statement is vacuously true.

So, let $d := \dim(V) \in \mathbb{Z}^+$ and suppose that the result is true whenever the dimension of the vector space is less than d.

Lemma 4.4.4.16 Let V be a finite-dimensional vector space over an algebraically closed field and let $T\colon V \to V$ be linear. Then, T has an eigenvalue.

Proof. Let $v \in V$ be nonzero.

$$\{v, T(v), T^2(v), \ldots, T^d(v)\} \tag{4.4.4.17}$$

is a set of $d+1$ vectors in a vector space of dimension d, and so it must be linearly-depend. Thus, there are $\alpha_0, \ldots, \alpha_d \in \mathbb{F}$, not all zero, such that

$$0 = \alpha_0 \cdot v + \cdots + \alpha_d \cdot T^d(v). \tag{4.4.4.18}$$

Note that it cannot be the case that $0 = \alpha_1 = \cdots = \alpha_d$, for then the above equation would in turn imply $\alpha_0 = 0$. Hence,

$$p(x) \coloneqq \alpha_0 + \alpha_1 x + \cdots + \alpha_d x^d \in \mathbb{F}[x] \tag{4.4.4.19}$$

is a nonconstant polynomial. As $\mathbb{F}$ is right algebraically closed, there is a root $\lambda_1 \in \mathbb{F}$ of p. Hence, by Proposition C.3.2.21, there is a polynomial $p_2 \in \mathbb{F}[x]$ such that

$$p(x) = p_2(x)(x - \lambda_1). \tag{4.4.4.20}$$

If p_2 is constant, stop. Otherwise, p_2 has another root $\lambda_2 \in \mathbb{F}$, in which case we can write

$$p(x) = p_3(x)(x - \lambda_2)(x - \lambda_1) \tag{4.4.4.21}$$

for some $p_3 \in \mathbb{F}[x]$. Continuing inductively, we eventually find

$$p(x) = \alpha(x - \lambda_d) \cdots (x - \lambda_1) \tag{4.4.4.22}$$

for some nonzero $\alpha \in \mathbb{F}$.

By (4.4.4.18), we have that $[p(T)](v) = 0$, and hence

$$0 = \alpha[T - \lambda_d]\left([T - \lambda_{d-1}]\left(\cdots([T - \lambda_1](v))\cdots\right)\right).$$

If $[T - \lambda_{d-1}](\cdots)$ is nonzero, then $T - \lambda_d$ has nonzero kernel. Otherwise, in fact we have $[T - \lambda_{d-1}](\cdots) = 0$. Now, if $[T - \lambda_{d-2}](\cdots)$ is nonzero, $T - \lambda_{d-1}$ has nonzero kernel. Continuing inductively, we eventually find some k such that $\mathrm{Ker}(T - \lambda_k) \neq 0$. Thus, λ_k is an eigenvalue of T. ■

So, let λ_1 be an eigenvalue of T. By Theorem 4.4.3.45, we have that $\mathrm{Eig}^{\infty,T}_{\lambda} = \mathrm{Ker}([T - \lambda]^{\dim(V)})$. Then, by Proposition 4.4.3.2, we have

$$V = \mathrm{Eig}^{\infty}_{\lambda,T} \oplus U, \tag{4.4.4.23}$$

where $U \coloneqq \mathrm{Im}([T - \lambda]^{\dim(V)})$ is T-invariant.

Enumerate all the eigenvalues of T by $\lambda_1, \ldots, \lambda_m$.

Exercise 4.4.4.24 Show that the eigenvalues of $T|_U : U \to U$ are $\lambda_2, \ldots, \lambda_m$.

By the induction hypothesis, we now have

$$U = \mathrm{Eig}^{\infty}_{\lambda_2,T|_U} \oplus \cdots \oplus \mathrm{Eig}^{\infty}_{\lambda_m,T|_U}. \tag{4.4.4.25}$$

Combining this with (4.4.4.23) will complete the proof if we can show that $\text{Eig}^{\infty}_{\lambda_k, T|_U} = \text{Eig}^{\infty}_{\lambda_k, T}$. As the proof is the same for all k, it suffices to prove this for $k = 2$.

So, let $u \in \text{Eig}^{\infty}_{\lambda_2, T|_U}$. There is then some $m \in \mathbb{N}$ such that $[T - \lambda_2]^m(u) = 0$, and so $u \in \text{Eig}^{\infty}_{\lambda_2, T}$. In the other direction, let $v \in \text{Eig}^{\infty}_{\lambda_2, T}$. As before, we know that there is some $m \in \mathbb{N}$ such that $[T - \lambda_2]^m(v) = 0$, but now we need to show additionally that $v \in U$.

By (4.4.4.23), we can write

$$v = v_1 + u \tag{4.4.4.26}$$

for unique $v_1 \in \text{Eig}^{\infty}_{\lambda_1, T}$ and $u \in U$. We wish to show that $v_1 = 0$.

By (4.4.4.25), we may write

$$u = u_2 + \cdots + u_m \tag{4.4.4.27}$$

for unique $u_k \in \text{Eig}^{\infty}_{\lambda_k, T|_U}$. Hence,

$$v = v_1 + u_2 + \cdots + u_m. \tag{4.4.4.28}$$

As generalized-eigenvectors with distinct eigenvalues are linearly-independent (Proposition 4.4.3.67), this implies that $v_1 = 0$, $u_2 = v$, and $u_3 = \cdots = u_m = 0$. Thus, $v \in U$, as desired.

(ii) As each generalized-eigenspace is invariant[a], the Fundamental Theorem of Blockdiagonalizability (Theorem 4.4.2.11) says that the matrix of T with respect to this direct-sum decomposition is

$$\begin{bmatrix} T|_{\text{Eig}^{\infty}_{\lambda_1}} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & T|_{\text{Eig}^{\infty}_{\lambda_m}} \end{bmatrix} \tag{4.4.4.29}$$

By definition of generalized-eigenspaces, $N_k := T|_{\mathrm{Eig}^\infty_{\lambda_k}} - \lambda_k \,\mathrm{id}^\infty_{\mathrm{Eig}_{\lambda_k}}$ is locally-nilpotent, hence nilpotent by finite-dimensionality (Proposition 4.4.3.32). We thus have that the matrix of T with respect to this direct-sum decomposition is indeed of the form

$$\begin{bmatrix} \lambda_1 \,\mathrm{id}_{\mathrm{Eig}^\infty_{\lambda_1}} + N_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_m \,\mathrm{id}_{\mathrm{Eig}^\infty_{\lambda_m}} + N_m \end{bmatrix}, \tag{4.4.4.30}$$

where $N_k \colon \mathrm{Eig}^\infty_{\lambda_k} \to \mathrm{Eig}^\infty_{\lambda_k}$ is nilpotent linear.

(iii) By Theorem 4.4.3.16, there is a basis $\mathcal{B}_k$ of $\mathrm{Eig}^\infty_{\lambda_k}$ such that

$$[T|_{\mathrm{Eig}^\infty_{\lambda_k}} - \lambda_k \,\mathrm{id}_{\mathrm{Eig}^\infty_{\lambda_k}}]_{\mathcal{B}_k \leftarrow \mathcal{B}_k} \tag{4.4.4.31}$$

is a direct-sum of Jordan blocks with eigenvalue 0, and hence

$$[T|_{\mathrm{Eig}^\infty_{\lambda_k}}]_{\mathcal{B}_k \leftarrow \mathcal{B}_k} \tag{4.4.4.32}$$

is a direct-sum of Jordan blocks with eigenvalue λ_k.

(iv) As $\mathcal{B}_k$ is a basis for $\mathrm{Eig}^\infty_{\lambda_k}$ and $V = \mathrm{Eig}^\infty_{\lambda_1} \oplus \cdots \oplus \mathrm{Eig}^\infty_{\lambda_m}$, $\mathcal{B} := \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m$ is a basis for V. Furthermore, $[T]_{\mathcal{B} \leftarrow \mathcal{B}}$ is a block-diagonal matrix whose k^{th} block is $[\lambda_k \,\mathrm{id}_{\mathrm{Eig}^\infty_{\lambda_k}} + N_k]_{\mathcal{B}_k \leftarrow \mathcal{B}_k}$.

Exercise 4.4.4.33 Check this.

(v) Let $\mathcal{C}$ is another basis of V that has the property that $[T]_{\mathcal{C} \leftarrow \mathcal{C}}$ is a direct-sum of Jordan blocks. The eigenvalues of such a direct-sum are the same as the eigenvalues of T, and so the eigenvalues appearing among the Jordan blocks are the same for both the bases $\mathcal{B}$ and $\mathcal{C}$. So, fix $\lambda \in \mathbb{F}$ an eigenvalue of T, and

for the moment consider only the restriction $S := T|_{\mathrm{Eig}^\infty_\lambda} : \mathrm{Eig}^\infty_\lambda$. As $[T]_{C\leftarrow C}$ is a direct-sum of Jordan blocks, the elements of C are all generalized-eigenvectors, and so $C_\lambda := C \cap \mathrm{Eig}^\infty_\lambda$ is a basis for $\mathrm{Eig}^\infty_\lambda$. Similarly for $\mathcal{B}_\lambda := \mathcal{B} \cap \mathrm{Eig}^\infty_\lambda$. Thus, $[S]_\mathcal{B}$ and $[S]_C$ are both direct-sums of Jordan blocks and we would like to prove that the size of the Jordan blocks appearing in this decomposition are the same (the eigenvalues are of course all equal to λ). Let $m \in \mathbb{Z}^+$ be the smallest positive integer such that $[S-\lambda]^m = 0$ (there is some such m as we know $S-\lambda$ is nilpotent). It follows that m is the smallest positive integer such that $[[S-\lambda]]_\mathcal{B}{}^m = 0$ and also the smallest positive integer such that $[[S-\lambda]]_C{}^m = 0$. It follows that the largest Jordan block appearing in both of these matrices is size m. Now, replace S with $S - \mathrm{Jord}_{\lambda,m}$ and apply the same logic again. We find again that the largest Jordan blocks appearing in these decompositions have the same size. Proceeding inductively, we see that they have the same Jordan blocks. ■

[a] By Proposition 4.4.3.63(ii).

This theorem says a lot, all of which is important and useful, but the short and sweet version can be summed up as saying

> Every linear operator on a finite-dimensional vector space over an algebraically closed field has a basis in which the associated matrix is a direct-sum of Jordan blocks.

How this works can be understood in three key steps. First, V is a direct-sum of the generalized-eigenspaces:

$$V = \mathrm{Eig}^\infty_{\lambda_1} \oplus \cdots \oplus \mathrm{Eig}^\infty_{\lambda_m} . \tag{4.4.4.34}$$

Second, we break up each generalized-eigenspace into indecomposable summands (Theorem 4.4.3.16). Finally, as $T - \lambda_k$ is nilpotent on the corresponding generalized-eigenspace, Proposition 4.4.2.16, whose statement (or part of it) we reproduce below for convenience, explains how $T - \lambda_k$ behaves on these indecomposable components.

Theorem 4.4.4.35. Let V be a finite-dimensional vector space and let $N\colon V \to V$ be nilpotent linear. Then, if V is N-indecomposable,

$$\mathcal{B} := \{v_0, N(v_0), \ldots, N^{\dim(V)-1}(v_0)\} \tag{4.4.4.36}$$

is a basis of V for any N-maximal $v_0 \in V$, that has the property that

$$[N]_{\mathcal{B}\leftarrow\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}. \tag{4.4.4.37}$$

Proof. This is a part of the conclusion of Theorem 4.4.3.16. ■

Of course, there is still the issue of how to actually *calculate* the damn thing, but we postpone that until the next section until after having discussed the *minimal polynomial*.

To give you an idea of what this means (don't worry—it's not hard), let's take a look at a couple examples of matrices in Jordan canonical form.

■ **Example 4.4.4.38**

$$\mathrm{Jord}_{3,2} \oplus \mathrm{Jord}_{4,1} \oplus \mathrm{Jord}_{-2,2} := \begin{bmatrix} 3 & 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}$$

is in Jordan canonical form.

Similarly,

$$\mathrm{Jord}_{5,3} \oplus \mathrm{Jord}_{-3,2} = \begin{bmatrix} 5 & 1 & 0 & 0 & 0 \\ 0 & 5 & 1 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & -3 & 1 \\ 0 & 0 & 0 & 0 & -3 \end{bmatrix} \quad (4.4.4.39)$$

is in Jordan canonical form.

Finally,

$$\mathrm{Jord}_{4,2} \oplus \mathrm{Jord}_{4,2} \oplus \mathrm{Jord}_{4,1} := \begin{bmatrix} 4 & 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}. \quad (4.4.4.40)$$

is also in Jordan canonical form.

R Note in particular that you have have *multiple Jordan blocks* corresponding to the *same eigenvalue*.

▪ **Example 4.4.4.41** Suppose I give you a linear operator T on $\mathbb{C}^4$ and I tell you that T has a single eigenvalue 3. This theorem tells us that the Jordan canonical form of T is going to be a direct-sum of Jordan blocks with eigenvalue 3, and furthermore, the size of these Jordan blocks must sum to 4. Thus, this theorem tells you that the possible Jordan canonical

forms of T are as follows.

$$\begin{bmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$
$$\begin{bmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} \qquad (4.4.4.42)$$
$$\begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

(These respectively, going across first, correspond to Jordan block sizes of $4 = 4$, $4 = 3 + 1$, $4 = 2 + 2$, $4 = 2 + 1 + 1$, and $4 = 1 + 1 + 1 + 1$.)

With just a bit of extra information, you can determine which of these five possibilities it is. For example, if $T - 3 = 0$, then of course it must the last choice. If $T - 3 \neq 0$ but $(T-3)^2 = 0$, then it must be the third or fourth choice, and you can distinguish between those two by looking at $\dim(\text{Eig}_3)$.[a] If $(T-3)^2 \neq 0$ but $(T-3)^3 = 0$, then it must be the second choice. Finally, if $(T-3)^3 \neq 0$, then it must be the first choice.

[a] While the dimension of the generalized-eigenspace is of course always 4, we have $\dim(\text{Eig}_3) = 2$ for the third matrix and $\dim(\text{Eig}_3) = 3$ for the third matrix.

Jordan canonical form of matrix linear-transformations

When studying diagonalization, it wasn't just of interest to know what the diagonalization itself was, but also what the relationship was between the original linear-transformation and its diagonalization. In general, this relationship is just "The diagonalization is the matrix with respect to a basis of eigenvectors.", but if the linear-transformation is defined by a matrix, we can be a bit more explicit. This was done

in Proposition 4.3.1.1, and we now present the analogous result for Jordan canonical form. Conceptually, it is essentially identical in nature, and if understand the previous result, you understand this one.

Proposition 4.4.4.43 Let A be an $m \times m$ matrix with entries in an algebraically-closed field $\mathbb{F}$ and let $\mathcal{B}$ be a Jordan basis of A. Then,

$$[A]_{\mathcal{B}\leftarrow\mathcal{B}} = [\mathrm{id}]_{\mathcal{B}\leftarrow\mathcal{S}}[A]_{\mathcal{S}\leftarrow\mathcal{S}}[\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}, \tag{4.4.4.44}$$

where $\mathcal{S}$ is the standard basis of $\mathbb{F}^m$.

R Note that $[A]_{\mathcal{S}\leftarrow\mathcal{S}} = A$ by Proposition 3.2.2.30.[a]

Furthermore, $[A]_{\mathcal{B}\leftarrow\mathcal{B}}$ is the Jordan canonical form of A (by the definition of "Jordan basis") and $[\mathrm{id}]_{\mathcal{B}\leftarrow\mathcal{S}} = [\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}^{-1}$. Thus, writing $J \coloneqq [A]_{\mathcal{B}\leftarrow\mathcal{B}}$ and $P \coloneqq [\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}$, this equation is sometimes written more concisely (but perhaps less transparently) as

$$J = P^{-1}AP. \tag{4.4.4.45}$$

R Note that, by Theorem 3.2.2.1, the columns of $[\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}$ are given by $[b_k]_{\mathcal{S}}$ for $b_k \in \mathcal{B}$. However, by Proposition 3.1.17,[b] this is just b_k itself. Thus,

> $P \coloneqq [\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}$ *is the matrix whose columns form a Jordan basis for* A.

[a] I wrote (4.3.1.2) using $[A]_{\mathcal{S}\leftarrow\mathcal{S}}$ instead of A because I feel as if writing it this way makes it more 'obviously' true.

[b] This is the result that says the coordinates of a column vector with respect to the standard basis is just that original column vector.

Proof. We leave this as an exercise.

Exercise 4.4.4.46 Prove the result yourself.

■

Similarity of linear operators

While we shall not really make use of the concept ourselves, as you continue in mathematics you will want to be able to determine when two linear operators are *conjugate* or *similar* to one another.[8] Jordan canonical form gives a characterization of when this is the case.

Definition 4.4.4.47 — Similar (linear operators) Let V be a $\mathbb{K}$-module and let $S, T : V \to V$ be linear operators. Then, S and T are ***similar*** iff the two $\mathbb{K}[x]$-module structures defined by S and T respectively are isomorphic.

Concretely, this means the following.

Proposition 4.4.4.48 Let V be a $\mathbb{K}$-module and let $S, T : V \to V$ be linear operators. Then, S and T are similar iff there is an invertible linear operator $P : V \to V$ such that

$$T = P \circ S \circ P^{-1}. \tag{4.4.4.49}$$

Proof. We leave this as an exercise.

Exercise 4.4.4.50 Prove the result yourself.

■

Another characterization of similarity that makes it more apparent what this concept have to do with Jordan canonical form is given by the following.

Proposition 4.4.4.51 Let V be a finite-dimensional vector space and let $S, T : V \to V$ be linear operators. Then, S and T

[8] For example, if you want to determine the conjugacy classes in certain matrix groups.

are similar iff there are bases $\mathcal{B}$ and C of V such that

$$[S]_{\mathcal{B}} = [T]_C. \tag{4.4.4.52}$$

Proof. ($\Rightarrow$) Suppose that S and T are similar. Then, there is an invertible linear operator $P\colon V \to V$ such that

$$T = P \circ S \circ P^{-1}. \tag{4.4.4.53}$$

Let $\mathcal{B}$ be any basis of V and define

$$C \coloneqq \{P(b) : b \in \mathcal{B}\}. \tag{4.4.4.54}$$

Exercise 4.4.4.55 Check that C is a basis of V.

Write $\mathcal{B} = \{b_1, \ldots, b_d\}$, so that $C = \{P(b_1), \ldots, P(b_d)\}$.

From the explicit expression given in the defining result of coordinates of linear-transformations (Theorem 3.2.2.1), we see that

$$[P]_{C\leftarrow\mathcal{B}} = \begin{bmatrix}[P(b_1)]_C & \cdots & [P(b_d)]_C\end{bmatrix} = \mathrm{id}_{d\times d}\,. \tag{4.4.4.56}$$

Hence,

$$\begin{aligned}[T]_C &\coloneqq [T]_{C\leftarrow C}\\ &= [P]_{C\leftarrow\mathcal{B}}[S]_{\mathcal{B}\leftarrow\mathcal{B}}[P^{-1}]_{\mathcal{B}\leftarrow C} = [S]_{\mathcal{B}}.\end{aligned} \tag{4.4.4.57}$$

($\Leftarrow$) Suppose there are bases $\mathcal{B}$ and C of V such that

$$[S]_{\mathcal{B}} = [T]_C. \tag{4.4.4.58}$$

Write $\mathcal{B} = \{b_1, \ldots, b_d\}$ and $C = \{c_1, \ldots, c_d\}$ (indexing in such a way that the above equality is true) and let $P\colon V \to V$ be the unique linear operator such that $P(b_k) = c_k$ for all $1 \leq k \leq m$.

Exercise 4.4.4.59 Show that P is invertible.

By construction, we have that $[P]_{C\leftarrow\mathcal{B}} = \mathrm{id}_{d\times d}$, and so

$$\begin{aligned}[T]_{C\leftarrow C} &= [P]_{C\leftarrow\mathcal{B}}[S]_{\mathcal{B}\leftarrow\mathcal{B}}[P^{-1}]_{\mathcal{B}\leftarrow C} \\ &= [P\circ S\circ P^{-1}]_{C\leftarrow C},\end{aligned} \tag{4.4.4.60}$$

and hence $T = P\circ S\circ P^{-1}$. ■

As mentioned before, Jordan canonical form gives a complete characterization of when linear operators are similar.

Theorem 4.4.4.61. Let V be a finite-dimensional vector space over an algebraically closed field and let $S, T\colon V \to V$ be linear-operators. Then, S and T are similar iff they have the same Jordan canonical form.

Proof. ($\Rightarrow$) Suppose that S and T are similar. Then, there is an invertible linear operator $P\colon V \to V$ such that $T = P\circ S\circ P^{-1}$. Let $\mathcal{B}$ be a basis for which $[S]_{\mathcal{B}}$ is in Jordan canonical form. Define $C := \{P(b) : b \in \mathcal{B}\}$. Then,

$$\begin{aligned}[T]_C &= [P\circ S\circ P^{-1}]_{C\leftarrow C} \\ &= [P]_{C\leftarrow\mathcal{B}}[S]_{\mathcal{B}\leftarrow\mathcal{B}}[P^{-1}]_{\mathcal{B}\leftarrow C} \\ &= [S]_{\mathcal{B}}.\end{aligned} \tag{4.4.4.62}$$

Thus, S and T have the same Jordan canonical form.

($\Leftarrow$) Suppose that S and T have the same Jordan canonical form. If $\mathcal{B}$ and C are bases of S and T respectively such that $[S]_{\mathcal{B}}$ and $[T]_C$ are the Jordan canonical forms of S and T respectively, then by hypothesis we have that $[S]_{\mathcal{B}} = [T]_C$, and so by the previous result S and T are similar. ■

4.4.5 Summary

We've already summarized the key elements of this section, so we shall not reproduce them here. (I thought it might still be helpful to have a "Summary" subsection that was easy to find.) If it's an actual summary you're looking for, check the paragraphs immediately preceding and immediately after Theorem 4.4.4.35.

4.5 The minimal polynomial

We've finally concluded that there is a basis for any linear-transformation on a finite-dimensional vector space over an algebraically closed field for which the corresponding matrix is "nice", that is, a direct-sum of Jordan blocks. That's great to know, but what we would like to be able to do is actually compute these things, that is, compute bases of the generalized-eigenspaces so that we may compute the corresponding matrix.

The first step in this process is to compute the eigenvalues, which we still have not really addressed how to do systematically yet. One (rather poor) answer to this is the *minimal polynomial* of a linear operator. The minimal polynomial of a linear operator is a polynomial that, among other things, has the property that its roots are precisely the eigenvalues of T. Thus, if you can compute the minimal polynomial, you can compute its roots,[9] and hence the eigenvalues. This isn't really where the minimal polynomial shines in its use, however. In addition to the the eigenvalues themselves, the minimal polynomial also gives you information about the Jordan canonical form.

We begin with the theorem that allows us to define the minimal polynomial.

Theorem 4.5.1 — Minimal polynomial. Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and let $T: V \to V$ be linear. Then, there is a unique monic polynomial $p_{\min,T}$, the ***minimal polynomial*** of T, such that

[9] Numerically anyways. I'm sure you've heard of the fact that you can't solve degree 5 polynomial equations or higher in general.

(i). $p_{\min,T}(T) = 0$; and
(ii). if $p(T) = 0$ for $p \in \mathbb{F}[x]$ nonzero, then $\deg(p_{\min,T}) \leq \deg(p)$.

Furthermore, for $p \in \mathbb{F}[x]$, $p(T) = 0$ iff there is some $q \in \mathbb{F}[x]$ such that

$$p = qp_{\min,T}. \tag{4.5.2}$$

R Recall that (Proposition C.3.2.1) a monic polynomial is a polynomial whose leading coefficient is 1.

R The proof makes use of the dimension of $\mathrm{End}_{\mathbf{Vect}_{\mathbb{F}}}(V)$, and in order for that to be a vector space, we require $\mathbb{F}$ to be a field—see Subsection 1.1.1 and Proposition 3.2.2.53.

R For the minority that care, I believe this can be generalized to $\mathbb{F}$ a centrally-finite division ring. In this case, the result would be true verbatim, except that in (4.5.2) the left and right quotients might be distinct.

Proof. Step 1: Establish existence
Regard V as a $\mathbb{K}[x]$-module as in Example 4.4.2.1. By Theorem 1.1.6, this is equivalent to the specification of a ring homomorphism $\rho\colon \mathbb{K}[x] \to \mathrm{End}_{\mathbf{Grp}}(V)$, precisely,

$$\rho(p) := p(T), \tag{4.5.3}$$

that is, $\rho(p)$ is the linear operator $p(T)\colon V \to V$. By Proposition C.1.3,

$$\mathrm{Ker}(\rho) := \{p \in \mathbb{F}[x] : p(T) = 0\} \tag{4.5.4}$$

is an ideal in $\mathbb{F}[x]$. In other words, $\mathrm{Ker}(\rho)$ is exactly the set of polynomials which satisfy our desired property (i).

We first check that $\mathrm{Ker}(\rho)$ is nonzero. To see this, it suffices to prove that there is some polynomial p such that $p(T) = 0$. However, consider the following set in $\mathrm{End}_{\mathbf{Vect}_{\mathbb{F}}}(V)$.

$$\left\{1, T, \ldots, T^{\dim(V)^2-1}, T^{\dim(V)^2}\right\} \tag{4.5.5}$$

This is a set of $\dim(V)^2 + 1$ elements in $\mathrm{End}_{\mathbf{Vect}_{\mathbb{F}}}(V)$. However, by Proposition 3.2.2.53, we know that $\dim(\mathrm{End}_{\mathbf{Vect}_{\mathbb{F}}}(V)) = \dim(V)^2$, and so we must have a linear-dependence relation:

$$\alpha_0 \cdot 1 + \alpha_1 \cdot T + \cdots + \alpha_{\dim(V)^2-1} \cdot T^{\dim(V)^2-1} + \alpha_{\dim(V)^2} \cdot T^{\dim(V)^2} = 0.$$

This of course gives us a polynomial p such that $p(T) = 0$.

Now, by Proposition C.3.2.8, $\mathbb{F}[x]$ is both a left and right PIR, and so as $\mathrm{Ker}(\rho) \neq 0$, there is some $p_0 \in \mathbb{F}[x]$ such that

$$\mathrm{Ker}(\rho) = \mathbb{F}[x]p_0. \tag{4.5.6}$$

Scaling p_0 if necessary, we may without loss of generality assume that it is monic—call the resulting polynomial $p_{\min,T}$, so that $p_{\min,T}$ is monic and

$$\mathrm{Ker}(\rho) = \mathbb{F}[x]p_{\min,T}. \tag{4.5.7}$$

Let $p \in \mathbb{F}[x]$ be another nonzero polynomial such that $p(T) = 0$. Then, by (4.5.4), $p \in \mathrm{Ker}(\rho) = \mathbb{F}[x]p_{\min,T}$. That is, there is some $q \in \mathbb{F}[x]$ such that $p = qp_{\min,T}$, which implies that $\deg(p) = \deg(q) + \deg(p_{\min,T}) \geq \deg(p_{\min,T})$ (as $q \geq 0$). This establishes (ii).

Step 2: Establish uniqueness

To see uniqueness, let $q \in \mathbb{F}[x]$ be another monic polynomial of minimum degree such that $q(T) = 0$. Then, $p_{\min,T} - q$ is a polynomial of degree strictly less than $\deg(p_{\min,T}) = \deg(q)^a$ and $[p_{\min,T} - q](T) := p_{\min,T}(T) - q(T) = 0$. According to

(ii), the only way this can happen is if $p_{\min,T} - q = 0$, that is $q = p_{\min,T}$.

STEP 3: ESTABLISH "FURTHERMORE..."
The existence of q_L above follows from the fact that $\mathrm{Ker}(\rho) = \mathbb{F}[x]p_{\min,T}$. To obtain this, we used the fact that $\mathbb{F}[x]$ is a *left* PIR, but we haven't yet used the fact that it is a *right* PIR. Using this, we see that there is some $p_0 \in \mathrm{Ker}(\rho)$ such that $\mathrm{Ker}(\rho) = p_0\mathbb{F}[x]$. Again, by scaling if necessary, we may without loss of generality assume that p_0 is monic. Then, preceding as before, we verify that p_0 satisfies (i) and (ii). Thus, by uniqueness, we have $p_0 = p_{\min,T}$, and hence that $\mathrm{Ker}(\rho) = p_{\min,T}\mathbb{F}[x]$, establishing the existence of q_R. ■

[a] The leading terms cancel as their coefficients are both 1.

Our first goal is to actually prove that the eigenvalues are precisely the roots of $p_{\min,T}$.

Theorem 4.5.8 — Roots of $p_{\min,T}$ are the eigenvalues. Let V be a a finite-dimensional vector space over a field $\mathbb{F}$, let $T: V \to V$ be linear, and let $\lambda \in \mathbb{F}$. Then, λ is an eigenvalue of T iff $p_{\min,T}(\lambda) = 0$.

R Warning: Keep in mind the ground field. For example, suppose that the ground field is $\mathbb{F}$ and that $p_{\min,T}(x) = x^2 + 1$. Don't think "Oh, i and $-$i are roots of $x^2 + 1$, and therefore they are eigenvalues of T.". Noooooooo. Over the *reals* they are neither roots of $x^2 + 1$ nor eigenvalues.

Proof. ($\Rightarrow$) Suppose that λ is an eigenvalue of T. Then (Corollary 4.2.51) $p(\lambda) = 0$ for every $p \in \mathbb{F}[x]$ such that $p(T) = 0$. As the minimal polynomial certainly satisfies this property, we have that $p_{\min,T}(\lambda) = 0$.

($\Leftarrow$) Suppose that $p_{\min,T}(\lambda) = 0$. It follows that (Proposition C.3.2.21) $p_{\min,T}(x) = (x - \lambda)q(x)$ for some $q \in \mathbb{F}[x]$. Plugging in T, we find

$$0 = p_{\min,T}(T) = [T - \lambda] \circ q(T). \tag{4.5.9}$$

Note that $\deg(q) = \deg(p_{\min,T}) - 1$, and so by the definition of the minimal polynomial, it *cannot* be the case that $q(T) = 0$. Thus, there is some $v \in V$ such that $[q(T)](v) \neq 0$, in which case we have

$$0 = [T - \lambda]([q(T)](v)), \tag{4.5.10}$$

that is, $[q(T)](v)$ is an eigenvector of T with eigenvalue λ. In particular, λ is an eigenvalue of T. ■

Awesome, right? Just compute $p_{\min,T}$ and find its roots. Done.

Uhm, sure. In principle, yes, in practice no. To see why this is pretty impractical (at least for computation), let's actually see how one might compute $p_{\min,T}$. The basic idea is as follows

Compute T.[10] Is there a linear-dependence relation between 1 and T? If so, great! That linear-dependence relation (upon scaling so that it's monic) gives you your minimal polynomial. If not, compute T^2. Is there a linear-dependence relation between 1, T, and T^2? If so, great! That gives you the polynomial. Now compute T^3. And so on.

Even as I describe this, it probably doesn't sound all that efficient. In any case, let's see this in action for real.

▪ **Example 4.5.11** Define

$$A := \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}. \tag{4.5.12}$$

[10] By which I mean, do literally nothing.

Hopefully it should be clear that there is no linear-dependence relation between this an the identity. Computation shows

$$A^2 = \begin{bmatrix} 7 & 10 \\ 15 & 22 \end{bmatrix}. \tag{4.5.13}$$

We how check for a linear-dependence relation among 1, A, A^2:

$$\begin{aligned} 0 &= \alpha_1 + \alpha_2 A + \alpha_3 A^2 \\ &= \begin{bmatrix} \alpha_1 + \alpha_2 + 7\alpha_3 & 2\alpha_2 + 10\alpha_3 \\ 3\alpha_2 + 15\alpha_3 & \alpha_1 + 4\alpha_2 + 22\alpha_3 \end{bmatrix}. \end{aligned} \tag{4.5.14}$$

This gives us 4 equations in $\alpha_1, \alpha_2, \alpha_3$. If it has a solution, we have our linear-dependence relation. Otherwise, onto A^3.[a]

Setting up the equations and using our ninja-level row-reduction skills[b], we find that

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \alpha_3 \begin{bmatrix} -2 \\ -5 \\ 1 \end{bmatrix}. \tag{4.5.15}$$

Any α_3 will give us a linear-dependence relation, but as we want the polynomial to be monic, we take $\alpha_3 = 1$. Thus,

$$p_{\min,T}(x) = x^2 - 5x - 2. \tag{4.5.16}$$

Using the quadratic formula, you can now compute the eigenvalues of T.[c]

Let's compare this with how one would compute the eigenvalues straight from the definition. $\lambda \in \mathbb{C}$ is going to be an eigenvalue iff $\text{Null}(A - \lambda) \neq 0$. To calculate the null space of $A - \lambda$, we row-reduce. A calculation shows that this matrix is row-equivalent to

$$\begin{bmatrix} 3 & 4 - \lambda \\ 0 & \frac{1}{3}(2 + 5\lambda - \lambda^2) \end{bmatrix}. \tag{4.5.17}$$

This null space is nonzero iff it has a free variable, which we see in this case is true iff $2 + 5\lambda - \lambda^2 = 0$.

Of the two methods, I think the direct row-reduction method is by far the better option. The strength of the minimal polynomial I think is more theoretical. For example, its mere existence tells us that in principle calculating eigenvalues is going to come down to solving a polynomial equation, even if in practice it's not usually the best idea to use the minimal polynomial to calculate them.

[a] Pro-tip: You'll only ever need to go as high as $\dim(V)$, so without doing anything, I know there's going to be a solution. We'll learn this when we cover the Cayley-Hamilton Theorem.

[b] Or Mathematica.

[c] Though they involve icky radicals so I won't reproduce them here. I trust you can solve quadratic equations on your own, yeah?

So, yes, certainly, one can compute $p_{\min,T}$ for the purpose of computing the eigenvalues, but if that's all it could do, it wouldn't be of much use. Of course, it has some theoretical uses,[11] but at the moment I would like to pay particular attention to what information the minimal polynomial gives you about the Jordan canonical form. To best understand this, I think it's helpful to first see what the minimal polynomial of matrices in Jordan canonical form are.

Proposition 4.5.18 — The minimal polynomial of a matrix in Jordan canonical form Let V be a finite-dimensional vector space over an algebraically closed field, let $T\colon V \to V$ be linear, and for every $\lambda \in \mathrm{Eig}(T)$ denote by n_λ the size of the largest Jordan block with eigenvalue λ appearing in the Jordan canonical form of T. Then,

$$p_{\min,T}(x) = \prod_{\lambda \in \mathrm{Eig}(T} (x - \lambda)^{n_\lambda}. \tag{4.5.19}$$

R In words, the minimal polynomial of T has a factor $x - \lambda$ for each eigenvalue λ of T, and the power of

[11] See, for example, Theorem C.5.11.

the factor is the size of the largest Jordan block with that eigenvalue.

R There is a rather easy generalization of this to the case when the ground field is not algebraically closed, though we can't yet state it officially because we haven't yet spoken of "extension of scalars"—see Section 5.6. Because of it's importance, we state the generalization here—it shouldn't be too hard to follow, and in any case, you can always come back once you've learned what $V^{\mathbb{A}}$ and $T^{\mathbb{A}}$ are.

Let V be a finite-dimensional vector space over a field $\mathbb{F}$, let $\mathbb{A}$ be an algebraic closure of $\mathbb{F}$, let $T: V \to V$ be linear, and for every $\lambda \in \text{Eig}(T^{\mathbb{A}})$ denote by n_λ the size of the largest Jordan block with eigenvalue λ appearing in the Jordan canonical form of $T^{\mathbb{A}}$. Then,

$$p_{\min,T}(x) = \prod_{\lambda \in \text{Eig}(T^{\mathbb{A}})} (x-\lambda)^{n_\lambda}. \tag{4.5.20}$$

R In particular, this tells us what the minimal polynomial of single Jordan blocks are.

$$p_{\min,\text{Jord}_{\lambda,m}}(x) = (x-\lambda)^m. \tag{4.5.21}$$

Proof. We leave this as an exercise.

Exercise 4.5.22 Prove the result.

■

■ **Example 4.5.23** The minimal polynomial of

$$A := \mathrm{Jord}_{3,2} \oplus \mathrm{Jord}_{4,1} \oplus \mathrm{Jord}_{-2,2} = \begin{bmatrix} 3 & 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} \tag{4.5.24}$$

is

$$p_{\min,A}(x) = (x-3)^2(x-4)(x+2)^2. \tag{4.5.25}$$

Similarly, the minimal polynomial of

$$B := \mathrm{Jord}_{5,3} \oplus \mathrm{Jord}_{-3,2} = \begin{bmatrix} 5 & 1 & 0 & 0 & 0 \\ 0 & 5 & 1 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & -3 & 1 \\ 0 & 0 & 0 & 0 & -3 \end{bmatrix} \tag{4.5.26}$$

is

$$p_{\min,B}(x) = (x-5)^3(x+3)^2. \tag{4.5.27}$$

Finally, the minimal polynomial of

$$C := \mathrm{Jord}_{4,2} \oplus \mathrm{Jord}_{4,2} \oplus \mathrm{Jord}_{4,1} := \begin{bmatrix} 4 & 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}. \tag{4.5.28}$$

is

$$p_{\min,C}(x) = (x-4)^2. \tag{4.5.29}$$

R Note how you only have a power of 2 here. This power of 2 corresponds to the size of the largest Jordan block and nothing else. You can have a 124398217958732987 dimensional matrix, all with one eigenvalue λ, but if all those Jordan blocks are just size 1, the minimal polynomial is still going to be just $x - \lambda$.

Having examined the minimal polynomial for matrices in Jordan canonical form, let's turn things around and see what information the minimal polynomial can tell us about a linear operator's as of yet unknown Jordan canonical form. In fact, let's just discuss how one might compute the Jordan canonical form (and the corresponding Jordan basis) in general.

Of course, we're going to start by computing the eigenvalues.[12] For a fixed eigenvalue λ, find a basis for $\text{Ker}(T - \lambda)$. If you have 'enough',[13] stop. Otherwise, compute a basis for $\text{Ker}([T - \lambda^2])$ by *extending* your basis of $\text{Ker}(T - \lambda)$—don't pick an entirely new basis. Again, if you have "enough", stop. Otherwise, extend your basis of $\text{Ker}([T-\lambda]^2)$ to a basis of $\text{Ker}([T-\lambda]^3)$, and so on. When you finally *do* stop, pick one of the 'newest' vectors that you just added to your basis at the last step. Call that guy v_0. v_0 is $[T-\lambda]$-*maximal*. So, apply $T-\lambda$ to v_0 over and over until you get 0: $[T - \lambda]^m(v_0), \ldots, [T - \lambda](v_0), v_0$. These vectors will form part of your final basis. Continue finding $[T - \lambda]$-maximal vectors in this way (for every eigenvalue) until you have a number of vectors equal to the dimension of your vector space. The matrix of T with respect to this basis will be in Jordan Canonical Form.[14]

[12]When we learn about the characteristic equation later one, we'll see that every eigenvalue has an *algebraic multiplicity*, and that the the dimension of the generalized-eigenspace coincides with that multiplicity. Thus, the algebraic multiplicity tells you exactly how many linearly-independent generalized-eigenvectors you need to find before you know you're 'done'.

[13]By "enough" I mean the number of elements in this basis is already equal to the algebraic multiplicity.

[14]Perhaps its worth mentioning that the matrix in any basis of generalized-eigenvectors will be relatively simple, but if you want the matrix to be exactly in Jordan Canonical Form, you can't just use any basis of generalized-eigenvectors—you have to do what was just explained previously.

■ **Example 4.5.30 — A computation of the Jordan Canonical form** Define

$$A := \begin{bmatrix} 5 & 4 & 2 & 1 \\ 0 & 1 & -1 & -1 \\ -1 & -1 & 3 & 0 \\ 1 & 1 & -1 & 2 \end{bmatrix}. \tag{4.5.31}$$

Proceeding as in the previous example Example 4.5.11, we find that the minimal polynomial is

$$\begin{aligned} p_{\min,A}(x) &= x^4 - 11x^3 + 42x^2 - 64x + 32 \\ &= (x-1)(x-2)(x-4)^2.^a \end{aligned} \tag{4.5.32}$$

Thus, we see that the eigenvalues are $\lambda_1 := 1$, $\lambda_2 := 2$, and $\lambda_3 := 4$. Furthermore, by virtue of Proposition 4.5.18, we know that the largest $\lambda = 1$ Jordan block has size 1, the largest $\lambda = 2$ Jordan block has size 1, and the largest $\lambda = 4$ Jordan block has size 2. For a 4×4 matrix, there is only one way for this to happen:

$$\mathrm{Jord}_{4,2} \oplus \mathrm{Jord}_{2,1} \oplus \mathrm{Jord}_{1,1} := \begin{bmatrix} 4 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4.5.33}$$

Thus, from the minimal polynomial alone, we know this *must* be the Jordan canonical form.

Sometimes this will be enough, but often we will not only want to know the Jordan canonical form itself, but also it's relationship to the original linear-transformation. According to Proposition 4.4.4.43, this means we need to compute a Jordan basis for A. We start by looking at the generalized-eigenspaces.

Row-reducing $A - 1$, we obtain the matrix

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{4.5.34}$$

Therefore,

$$\text{Null}(A-1) = \text{Span}\left(\left\{\begin{bmatrix}-1\\1\\0\\0\end{bmatrix}\right\}\right). \tag{4.5.35}$$

We already know from (4.5.33) that $\dim(\text{Eig}_1^\infty) = 1$, and so we're done for the $\lambda = 1$ generalized-eigenspace.

As for $\lambda = 2$, row-reducing $A - 2$ yields

$$\begin{bmatrix}1 & 0 & 0 & -1\\0 & 1 & 0 & 1\\0 & 0 & 1 & 0\\0 & 0 & 0 & 0\end{bmatrix}, \tag{4.5.36}$$

and hence

$$\text{Null}(A-2) = \text{Span}\left(\left\{\begin{bmatrix}1\\-1\\0\\1\end{bmatrix}\right\}\right). \tag{4.5.37}$$

As for $\lambda = 1$, (4.5.33) tells us that we're done for $\lambda = 2$.

Finally, row-reducing $A - 4$ yields

$$\begin{bmatrix}1 & 0 & 0 & -1\\0 & 1 & 0 & 0\\0 & 0 & 1 & 1\\0 & 0 & 0 & 0\end{bmatrix}, \tag{4.5.38}$$

and hence

$$\text{Null}(A-4) = \text{Span}\left(\left\{\begin{bmatrix}1\\0\\-1\\1\end{bmatrix}\right\}\right). \tag{4.5.39}$$

We're still not done however, as (4.5.33) tells us that we need to have at least one generalized-eigenvector of rank 2.[b] Thus,

in fact we need to compute $\text{Null}([A-4]^2)$. Row-reducing $(A-4)^2$ yields

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{4.5.40}$$

so that

$$\text{Null}([A-4]^2) = \text{Span}\left(\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ -1 \\ 1 \end{bmatrix}\right). \tag{4.5.41}$$

Okay, now, *pay attention*!

We might be tempted to take

$$\mathcal{B} := \left\{\begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ -1 \\ 1 \end{bmatrix}\right\}, \tag{4.5.42}$$

but this is *wrong*. If P is the matrix whose columns are these vectors, then we find that[c]

$$P^{-1}AP = \begin{bmatrix} 1 & 0 & 0 & \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 5 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix}. \tag{4.5.43}$$

Oopsies. Something went wrong.

Note, however, that the $\lambda = 1$ and $\lambda = 2$ parts *did* come out as they should have. Remember that we can just use any old basis of generalized-eigenvectors. For the $\lambda = 4$ generalized-eigenspace, instead what we want to do is find a rank 2 generalized-eigenvector v_0, in which case $[A-4](v_0)$ will be the other $\lambda = 4$ generalized-eigenvector going into our

basis. (4.5.41) describe the space of generalized-eigenvectors of rank *at most* 2 and we want one with rank *exactly* 2, so we have to be a bit careful. Basically, compare the rank 1 generalized-eigenspace (4.5.39) and the rank 2 generalized-eigenspace (4.5.41) and pick something that is in the latter but not the former. Inspection reveals that

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{4.5.44}$$

works, in which case the other element we want to use for the $\lambda = 4$ generalized-eigenspace is

$$[A - 4](\langle 1, 0, 0, 0 \rangle) = \begin{bmatrix} 1 \\ 0 \\ -1 \\ 1 \end{bmatrix}. \tag{4.5.45}$$

Now, let's try this again and use the basis[d]

$$\mathcal{B} := \left\{ \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}. \tag{4.5.46}$$

Again, let P be the matrix whose columns are these basis elements. This time, we find

$$P^{-1}AP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{bmatrix}, \tag{4.5.47}$$

as desired.

[d] Yes, this computation is exceptionally tedious to do by hand, at least given the knowledge we have now. See Example 5.7.2.127 to see how one might at least compute the eigenvalues.

[b]In fact, it's *important to note* that one could deduce this from the minimal polynomial itself—the existence of the power of 2 in $(x-4)^2$ tells us that the maximum size Jordan block is size 2, and in particular, there must be at least one Jordan block of size 2.

[c]Recall that (Proposition 4.4.4.43) the resulting matrix should be the Jordan canonical form of A, but, of course, it's not.

[d]Note the order of $\langle 1,0,0,0\rangle$ and $[A-4](\langle 1,0,0,0\rangle)$. For practical reasons, when doing the computation, it is important that you place them *in this order* (from lowest rank to highest).

4.6 The Jordan-Chevalley Decomposition

The Jordan-Chevalley Decomposition is what I would consider a variant of the Jordan Canonical Form decomposition. Essentially it says that we can write any linear operator T as a sum

$$T = D + N, \tag{4.6.1}$$

where D is "diagonalizable"[15] and N is nilpotent. For example,

$$\mathrm{Jord}_{4,3} := \begin{bmatrix} 4 & 1 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \tag{4.6.2}$$

is the Jordan-Chevalley decomposition of $\mathrm{Jord}_{4,3}$. Similarly,

$$\begin{aligned} \mathrm{Jord}_{5,2} \oplus \mathrm{Jord}_{-3,3} &:= \begin{bmatrix} 5 & 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{aligned} \tag{4.6.3}$$

[15]In quotes because this may not literally be true. Instead, what is true is that, if it does fail to be diagonalizable, it only does so because the ground field doesn't contain all the eigenvalues of T.

is the Jordan-Chevalley decomposition of $\text{Jord}_{5,2} \oplus \text{Jord}_{-3,3}$. The underlying intuition is that, because, in a suitable basis, any linear operator T is a direct-sum of Jordan blocks, we can use this trick to write T itself as a sum of a "diagonalizable" linear operator and a nilpotent one.

The Jordan-Chevalley Decomposition can perhaps be thought of as an alternative solution to the "Not every linear operator is diagonalizable problem.". It says that every linear operator is the sum of a "diagonalizable" operator and a "small" (i.e. nilpotent one). We briefly mentioned this before, and because it's so closely related to Jordan canonical form, I think it's probably more accurate to say the Jordan-Chevalley Decomposition is another way of looking at the same solution to the diagonalization problem.

The Jordan-Chevalley Decomposition has at least two advantages over the Jordan Canonical Form Theorem. The first is that it requires weaker hypotheses. For example, the Jordan-Chevalley Decomposition will work over $\mathbb{R}$ where the Jordan Canonical Form Theorem did not. Secondly, the statement of the result is a bit 'cleaner'. In particular, you can state the result with no mention of bases or matrices. The downside is that it's not quite as strong as the Jordan Canonical Form Theorem—all it tells you is that N is nilpotent, whereas the Jordan Canonical Form Theorem says that you can choose a basis in which N takes a particularly nice form. Despite this, quite often one doesn't need this extra strength, and the Jordan-Chevalley Decomposition proves to be more convenient.

Anyways, let's get to the result.

Theorem 4.6.4 — Jordan-Chevalley Decomposition. Let V be a finite-dimensional vector space over a perfect field and let $T : V \to V$ be linear. Then, there are unique linear operators $D, N : V \to V$ such that

(i). $T = D + N$;
(ii). D is semisimple;
(iii). N is nilpotent; and
(iv). $DN = ND$

Furthermore, D and N are expressible as polynomials in T.

R Unless you have a particularly remarkable background for someone taking a linear algebra course, I would not expect you to have much intuition for the definition of a perfect field (Definition C.4.2). But that's okay. For us, what's important is that "perfect" is a sufficiently weak hypothesis that this theorem will apply in all cases of interest (see, for example, Proposition C.4.5). Essentially, don't worry about it—if you know enough math to be working with fields that are not perfect then you know enough math to know when you might have to worry.

R In terms of intuition, you should think of "semisimple" as meaning "diagonalizable". Indeed, Theorem C.5.11 says in particular that being semisimple is equivalent to being diagonalizable when you 'enlarge' your field to an algebraic closure, and in particular, semisimple is actually equivalent to being diagonalizable when working over an algebraically closed field. The only reason it isn't literally the case that semisimple is the same as diagonalizable is simply because you may not have all your eigenvalues in the ground field you're working with. For example,

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \tag{4.6.5}$$

is semisimple over $\mathbb{R}$ even though it is not diagonalizable over $\mathbb{R}$. Indeed, Theorem C.5.11 says that this is semisimple *because* it is diagonalizable over $\mathbb{C}$ (an algebraic closure of $\mathbb{R}$).

R Note that T is "diagonalizable" iff $N = 0$. In this sense, you can view the nilpotent part of T as an "obstruction" to being diagonalizable. It is in this sense that nilpotency is the only reason linear-transformations can fail to be diagonalizable.

Proof. We leave this as an exercise.

Exercise 4.6.6 Prove the result.

■

■ **Example 4.6.7 — A counter-example of the Jordan-Chevalley Decomposition over an imperfect field** Let $p \in \mathbb{Z}^+$ be prime, write $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, and define $\mathbb{F} := \mathbb{F}_p(t)$. Note that $\mathbb{F}$ is imperfect by Example C.4.9. As $\mathbb{F}$ is imperfect (Theorem C.4.3), there is some $a \in \mathbb{F}$ that is not of the form $a = b^p$. Define $V := \mathbb{F}[x]/(x^p - a)$ and $T : V \to V$ by

$$T(f + (x^p - a)) := xf(x) + (x^p - a). \tag{4.6.8}$$

Exercise 4.6.9 Show that T fails the conclusion of the Jordan-Chevalley decomposition.

R Hint: See Wikipedia.

4.7 Summary

Okay, so that was a long chapter. Fortunately, the key ideas you really need to take note of are less in number than the length of the chapter alone might suggest.

Linear algebra is the study of vector spaces and linear-transformations. In the previous chapter, we learned that, after chooses bases, we can associate column-vectors to vectors and matrices to linear-transformations. The objective of this chapter was then "How do I pick a basis that makes the matrix as simple as possible?". The final answer to that is you pick a Jordan basis, in which the associated matrix will be a direct-sum of Jordan blocks. And that's

really it—if you learn nothing else from this course, remember the following.

> If $T: V \to V$ is a linear operator on a finite-dimensional vector space over an algebraically-closed field, then there is a basis $\mathcal{B}$ of V such that $[T]_{\mathcal{B}}$ is a direct-sum of Jordan blocks.

Essentially everything else in this chapter was either a build-up to this or very closely related to it. Eigenspaces were introduced in an attempt to diagonalize matrices, which were later generalized to generalized-eigenspaces when we realized that didn't always work. Direct-sums, coordinates with respect to direct-sum decompositions, invariant subspaces, indecomposable subspaces, and nilpotent operators were all part of the background necessary to either prove or state the Jordan Canonical Form Theorem (Theorem 4.4.4.11). The Jordan Canonical Form Theorem gave a characterization when two linear-transformations were similar. The minimal polynomial was used as a tool to give information about the Jordan canonical form. And finally The Jordan-Chevalley Decomposition was presented as what is essentially a variant of the Jordan Canonical Form Idea.

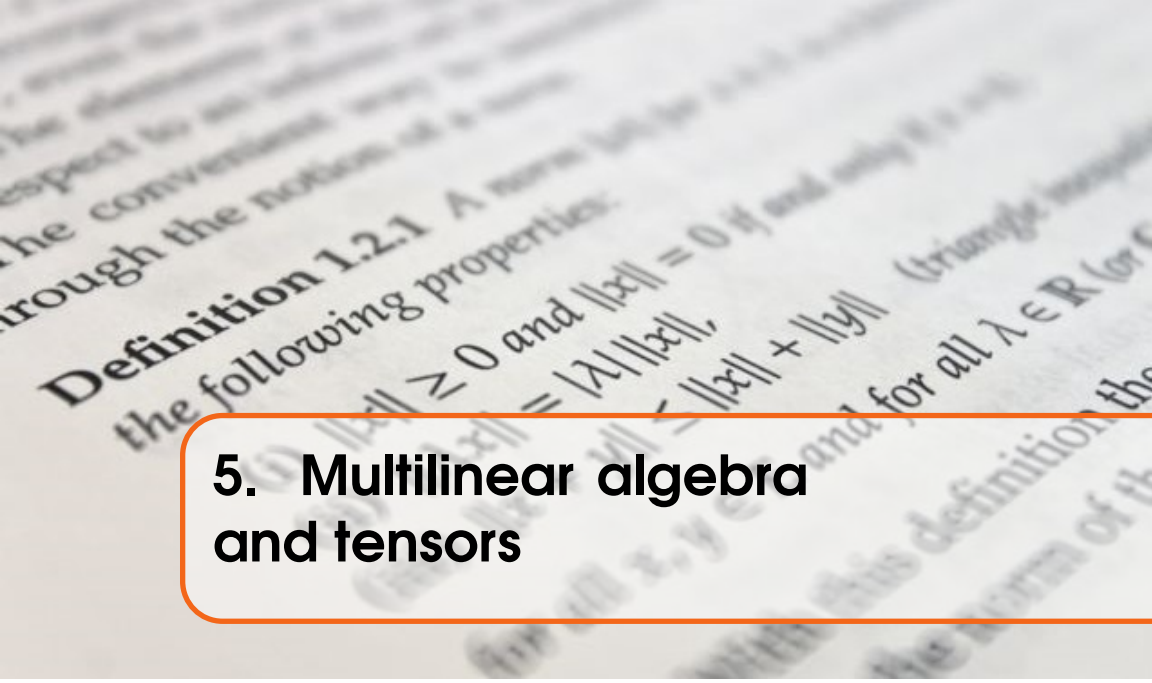
4.7.1 What now?

I regard the Jordan Canonical Form Theorem as the most important theorem in elementary linear algebra, and in some sense, everything we have done has been built up for the purpose of proving and stating it. Now that we've accomplished that primary goal, what to do?

The next big topic will be that of multilinear algebra. I'll leave for the next chapter the motivation for this, though for the moment let me mention that this content will included a discussion of the determinant, something that has thus far been noticeably absent.

Finally, we'll conclude with a study of inner-product spaces, which themselves are vector spaces equipped with additional structure. As such, I think it makes sense to cover pretty much everything there is about vector spaces themselves before introducing extra structure.

Anyways, let's get started. . .



5. Multilinear algebra and tensors

Multilinear algebra is, well, it's the study of multilinear maps. I realize that's not terribly enlightening, and for that to actually be a meaningful description at all, I had better first tell you what "multilinear map" actually means. Before I do so, however, I think it's best to start with some motivation.

5.1 Motivation

5.1.1 The derivative

You'll recall from multivariable calculus[1] the notion of the *gradient*, which really should be thought of as the derivative in higher dimensions. Given a smooth[2] function $f\colon \mathbb{R}^d \to \mathbb{R}$, you were probably taught something like "The gradient of a f is the vector (field) whose coordinates are given by the partial derivatives.". LIES!

[1] You have taken multivariable calculus, right? In case you haven't, the TL;DR version is: it's calculus, but when the functions have multiple variables.

[2] Recall that "smooth" means infinitely-differentiable with continuous derivatives. I assume this so that ∇f actually exists.

The gradient is *not* a vector field—it is a *co*vector field. The derivative $\nabla_a f(x)$ is a function which takes in a tangent vector[3] $v^a \in \mathrm{T}_x(\mathbb{R}^d)$ and spits out a number, the *directional derivative* of f at the point x in the direction v: $v^a \nabla_a f(x)$.[4] Thus, the derivative is not itself a vector, but rather, it's something that *takes in* vectors and *spits out* numbers. Such things are called *covectors* (or linear-functionals), and this will motivate us to introduce the *dual-space*.

So what about the second derivative then? Well, the second derivative is something that takes in *two* vectors and spits out a number, this number itself being the directional derivative in the direction of the first vector of the directional derivative in the direction of the second vector. The third derivative is a thing that takes in *three* vectors and spits out a number, and so on. The dual-space will give us things that takes in single vectors and spits out numbers, but to obtain objects that take in multiple vectors and spit out numbers, we'll need to discuss (higher rank) *tensors* and hence the *tensor product*.

5.1.2 Unification

If that's not satisfying to you, another motivation for the introduction of tensors is that they can be viewed as a unifying concept for all of linear algebra in the sense that nearly every concept one encounters can be thought of as a tensor. For example, scalars, vectors, covectors, linear-transformations, inner-products, pairings (in a dual-pair), etc.. . . all of these are tensors.

5.1.3 Multilinear-transformations

Okay, cool, so tensors are a thing we should care about. But what does that have to do with multilinear-transformations? I suppose the answer is that we ultimately need them to define tensors, and in particular, the tensor product—see Theorem 5.3.1.1. For example, this was already hinted at when we noted that the second derivative (which is supposed to be (and in fact will be) a tensor) takes in two vectors and spits out a number—as it does so in such a way that it is

[3] You don't need to know the precise definition of tangent vector or tangent space, only that v^a is supposed to indicate (at an intuitive level) a "direction".

[4] Don't worry about the indices fo now. They will be explained later—see Section 5.4.

linear in each of the vectors, this is one example of how a tensor is really just a type of multilinear map.

While we won't begin study of multilinear maps proper for a couple of sections, we introduce the definition here, as we shall occasionally make use of the terminology.

Definition 5.1.3.1 — Multilinear-transformation
Let $V_1, \ldots, V_m$ be respectively $\mathbb{K}_k$-$\mathbb{K}_{k+1}$-bimodules, let V be a $\mathbb{K}_1$-$\mathbb{K}_{m+1}$-bimodule, and let $T\colon V_1 \times \cdots \times V_m \to V$ be a function. Then, T is ***multilinear*** iff

(i).

$$V_k \ni v \mapsto T(v_1, \ldots, v_{k-1}, v, v_{k+1}, \ldots, v_m) \in V$$

is a group homomorphism for all $1 \leq k \leq m$;

(ii).

$$T(\alpha \cdot v_1, v_2, \ldots, v_{m-1}, v_m \cdot \beta) = \alpha \cdot T(v_1, v_2 \ldots, v_{m-1}, v_m) \cdot \beta$$

for $\alpha \in \mathbb{K}_1$ and $\beta \in \mathbb{K}_{m+1}$; and

(iii).

$$\begin{aligned} &T(v_1, \ldots, v_k \cdot \alpha, v_{k+1}, \ldots, v_m) \\ &\quad = T(v_1, \ldots, v_k, \alpha \cdot v_{k+1}, \ldots, v_m) \end{aligned} \tag{5.1.3.2}$$

for $\alpha \in \mathbb{K}_k$.

R If $m = 2$, the term ***bilinear*** is more commonly used instead of "multilinear-transformation". While I can't say I've heard the term before, it would stand to reason that ***trilinear*** would be used for the $m = 3$ case, etc..

R In essence, this means that (i) each argument preserves addition and (ii) you can move scalars around as you please just so long as you don't move scalars past vectors.

If you find this confusing, I wouldn't worry. Our interest is primarily in the commutative case, in which case these conditions simplify to something more understandable—see Proposition 5.1.3.3.

R At this level of generality, you might hear this concept being referred to as ***balanced***, in which case "multilinear-linear transformation" would only be used in the commutative case where the condition simplifies—see Proposition 5.1.3.3.

Recall that (Example 1.1.1.12) if $\mathbb{K}$ is commutative, then a left $\mathbb{K}$-module obtains a canonical right module structure and vice-versa, and does so in such a way so as to 'commute' with the vectors: $\alpha \cdot v = v \cdot \alpha$. Thus, in this case, the above condition simplifies to the following.

Proposition 5.1.3.3 Let $V_1, \dots, V_m, V$ be $\mathbb{K}$-modules, $\mathbb{K}$ a cring, and let $T : V_1 \times \cdots \times V_m \to V$ be a function. Then, T is multilinear iff

$$V_k \ni v \mapsto T(v_1, \dots, v_{k-1}, v, v_{k+1}, \dots, v_m) \in V \quad (5.1.3.4)$$

is linear for all $1 \leq k \leq m$.

R In other words, over commutative rings, multilinear is equivalent to being linear in every argument.

Proof. We leave this as an exercise.

Exercise 5.1.3.5 Prove the result.

■

5.2 Dual-pairs and dual-spaces

We've already stated why we should care about covectors and the dual-space. After having defined the dual-space $V^\dagger$ of a vector space V (over a ground ring $\mathbb{K}$), we will obtain a *bilinear* map $V^\dagger \times V \to \mathbb{K}$, yielding our first example of a *dual-pair*. In fact, it is essentially the only example of a dual-pair that we'll be interested in, but using this language will make the theory less 'clunky'. For example, working

with dual-spaces themselves, our definitions would have to be written in such a way that, for example, $[T^\dagger]^\dagger$ is map from $[V^\dagger]^\dagger$ to $[W^\dagger]^\dagger$, whereas using the language of dual-pairs, it is instead a map from V to W.

5.2.1 Dual-spaces

Definition 5.2.1.1 — Dual-space Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule. Then, the ***dual-space*** of V is the $\mathbb{K}$-$\mathbb{K}$-bimodule

$$V^\dagger := \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, \mathbb{K}). \tag{5.2.1.2}$$

R We also say simply that $V^\dagger$ is the ***dual*** of V.

R Elements of $V^\dagger$ are ***covectors*** or ***linear-functionals***. The terms are synonymous, though "covector" is more commonly used in the context of tensors while "linear-functional" tends to be used elsewhere.

R Warning: This definition is *tentative*. It will later be replaced by the more general definition given in Definition 6.4.3.15. What we really should have said is that the dual-space is the space of all *continuous* linear-transformations from V to $\mathbb{K}$.[a]

R In other words, the elements of $V^\dagger$ take in elements of V and spit out scalars. Recall that the motivating example of this was the derivative: this takes in a vector (the direction in which to differentiate) and spits out a number (the directional derivative in that direction).

R Recall that (Subsection 1.1.1) $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$ does not have the structure of a module if V and W are just modules. If we want morphism sets to have some sort of nontrivial module structure, we need to work with *bimodules* from the get-go. Requiring that V be a $\mathbb{K}$-$\mathbb{K}$-bimodule ensures that $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, \mathbb{K})$ is

a $\mathbb{K}$-$\mathbb{K}$-bimodule as well, so that V and $V^\dagger$ are the same type of object.[b]

That said, recall that (Example 1.1.1.12) modules over commutative rings have a canonical bimodule structure, and so if we're working over commutative rings, we can get away with just saying "$\mathbb{K}$-module" everywhere.

R The "†" is for "transpose"—we'll see why later. This is uncommon notation. More common notation includes V^* and V'. The former I choose not to use as I reserve this notation for the *conjugate*-dual, and the latter, well, V' just looks weird to me. There's also the fact that "†" kind of just looks like a "t".[c]

R If V comes with a topology, you're only going to want to look at the *continuous* linear functionals. Of course, you can look at all of them (including the discontinuous ones), but this is probably not going to be as useful.

R You might say that this is the "left dual-space" and that $\mathrm{Mor}_{\mathbf{Mod}\text{-}\mathbb{K}}(V, \mathbb{K})$ would be the "right dual-space". Just as we only worked with left modules by default (even though there was a corresponding notion of right module), we won't every worry about the right dual-space. Besides, if $\mathbb{K}$ is commutative, there isn't going to be any difference anyways.

---

[a] In fact, as V secretly has the discrete topology, all linear-transformations $V \to \mathbb{K}$ are continuous, and so in this case the two definitions agree. In general, however, they disagree, and in the general context, you want to consider only the *continuous* linear-functionals.

[b] Note that $\mathbb{K}$ is a $\mathbb{K}$-$\mathbb{K}$-bimodule (Example 1.1.1.11), and hence $V^\dagger := \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, \mathbb{K})$ is a $\mathbb{K}$-$\mathbb{K}$-bimodule by Example 1.1.1.17.

[c] In English, "†" is actually read as "dagger" (the TEX command for this is "`\dagger`, though I imagine the English usage came first).

You should note that we need to require $\mathbb{K}$ to be commutative in order to guarantee that $V^\dagger$ itself has the structure of a $\mathbb{K}$-module.[5] As we're going to be wanting to be considering V and $V^\dagger$ on more or less equal footings, it is awkward if V is a $\mathbb{K}$-module but $V^\dagger$ is just a commutative group. Therefore, you should keep in mind that we will be requiring $\mathbb{K}$ to be commutative more often than usual, and that this is the reason why.

▪ **Example 5.2.1.3 — Row-vectors** Let $\mathbb{K}$ be a ring, let $d \in \mathbb{N}$, and define $V := \mathbb{K}^d$. Recall that we can think of elements of V has $d \times 1$ matrices. Therefore, for every $1 \times d$ matrix $\phi \in \mathrm{Matrix}_{1\times d}(\mathbb{K})$, we have a linear map $V \to \mathbb{K}$ defined by

$$V \ni v \mapsto \phi v, \tag{5.2.1.4}$$

where ϕv is just matrix multiplication (and we are implicitly identifying 1×1 matrices with $\mathbb{K}$ itself).

This defines a map from $\mathrm{Matrix}_{1\times d}(\mathbb{K})$ to $V^\dagger$, which is an isomorphism.

Exercise 5.2.1.5 Check that this is indeed an isomorphism.

We thus hereafter identity $V^\dagger \cong \mathrm{Matrix}_{1,d}(\mathbb{K})$, in which case elements of $V^\dagger := [\mathbb{K}^d]^\dagger$ are referred to as ***row-vectors***.

For example, $\begin{bmatrix}1 & 2 & 3\end{bmatrix} \in [\mathbb{R}^3]^\dagger$ defines a linear-functional on $\mathbb{R}^3$ via

$$\mathbb{R}^3 \ni \begin{bmatrix}x\\y\\z\end{bmatrix} \mapsto \begin{bmatrix}1 & 2 & 3\end{bmatrix}\begin{bmatrix}x\\y\\z\end{bmatrix} := x + 2y + 3z. \tag{5.2.1.6}$$

R Thus, row-vectors should be thought not of as vectors but as *co*vectors.

[5] Recall from Subsection 1.1.1 that morphism sets are in general not themselves $\mathbb{K}$-modules unless $\mathbb{K}$ is commutative.

▪ **Example 5.2.1.7 —** $[\mathbb{K}^\infty]^\dagger = \mathbb{K}^\mathbb{N}$ Let $\mathbb{K}$ be a ring. Given $a \in \mathbb{K}^\mathbb{N}$, we obtain a linear-functional $\phi_a : \mathbb{K}^\infty \to \mathbb{K}$ defined by

$$\phi_a(b) := \sum_{k\in\mathbb{N}} b_k a_k. \tag{5.2.1.8}$$

Note that this sum is finite as $b \in \mathbb{K}^\infty$.

Exercise 5.2.1.9 Show that

$$\mathbb{K}^\mathbb{N} \ni a \mapsto \phi_a \in [\mathbb{K}^\infty]^\dagger \tag{5.2.1.10}$$

is an isomorphism of $\mathbb{K}$-$\mathbb{K}$-bimodules.

One reason the term "dual" is used is because, while on one hand, we can obviously view elements of $V^\dagger$ as linear-functionals on V, we can "dually" view elements of V as linear-functionals on $V^\dagger$.

Theorem 5.2.1.11 — Duality of the dual. Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule. Then, the map $V \to [V^\dagger]^\dagger$ defined by

$$v \mapsto (\phi \mapsto \phi(v)) \tag{5.2.1.12}$$

is linear and natural.

Furthermore,

(i). if V is a vector space, this map is injective; and
(ii). if V is a finite-dimensional vector space, this map is an isomorphism.

R See Appendix B.3.2 for a discussion of what is meant here by the term "natural". You should note, however, that it's not particularly important and could require a relatively large effort to fully understand, especially if you've never seen anything like this before. Thus, you might consider just pretending the word "natural" didn't appear anywhere in the statement above—you won't be missing out on all *that* much.

R For $v \in V$ and $\phi \in V^\dagger$, we write

$$(\phi \mid v) := \phi(v). \tag{5.2.1.13}$$

Using this notation, the map $V \to [V^\dagger]^\dagger$ can be written as

$$v \mapsto (\cdot \mid v), \tag{5.2.1.14}$$

where $(\cdot \mid v)$ is the linear-functional on $V^\dagger$ that sends $\phi \in V^\dagger$ to $(\phi \mid v) := \phi(v) \in \mathbb{K}$.

This notation is used suggestively when we want to think of V and $V^\dagger$ as 'on the same footing'—on one hand, we can view elements of $V^\dagger$ as linear-functionals on V (e.g. for $\phi \in V^\dagger$, $(\phi \mid \cdot)$ is a linear-functional on V), but on the other hand we can also view elements of V as linear-functional on $V^\dagger$ (e.g. for $v \in V$, $(\cdot \mid v)$ is a linear-functional on $V^\dagger$). Thinking of things in terms of this "duality" is particularly appropriate when V is a finite-dimensional vector space, so that, up to natural isomorphism, V is 'the same as' $[V^\dagger]^\dagger$.

R Warning: (i) need not hold if V is not a vector space and (ii) need not hold if V is a vector space but not finite-dimensional—see Examples 5.2.1.21 and 5.2.1.23 respectively.

Proof. We first check that it is linear. Let $v, w \in V$ and let $\alpha, \beta \in \mathbb{K}$. We wish to show that

$$(\cdot \mid \alpha v + \beta w) = \alpha(\cdot \mid v) + \beta(\cdot \mid w). \tag{5.2.1.15}$$

However, this will be the case iff for all $\phi \in V^\dagger$ we have

$$(\phi \mid \alpha v + \beta w) = \alpha(\phi \mid v) + \beta(\phi \mid w). \tag{5.2.1.16}$$

However, by definition of the notation $(\cdot \mid \cdot)$, this equation is the same as

$$\phi(\alpha v + \beta w) = \alpha\phi(v) + \beta\phi(w), \tag{5.2.1.17}$$

which is of course true as ϕ is linear.

We now check that it is natural.[a] Let $T\colon V \to W$ be a linear-transformation between $\mathbb{K}$-modules. By definition (Definition B.3.2.3), $V \mapsto [V^\dagger]^\dagger$ is natural iff the following diagram commutes.

$$\begin{array}{ccc} V & \longrightarrow & \left[V^\dagger\right]^\dagger \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle [T^\dagger]^\dagger} \\ W & \longrightarrow & \left[W^\dagger\right]^\dagger \end{array} \tag{5.2.1.18}$$

By definition, this means that we want to show that

$$(\psi \mid [[T^\dagger]^\dagger]((\cdot \mid v))) = (\psi \mid T(v)) \tag{5.2.1.19}$$

for all $v \in V$ and $\psi \in W^\dagger$. However, by definition of the transpose and $(\cdot \mid v)$,

$$\begin{aligned} (\psi \mid [[T^\dagger]^\dagger]((\cdot \mid v))) &\coloneqq ([T^\dagger](\psi) \mid (\cdot \mid v)) \\ &\coloneqq ([T^\dagger](\psi) \mid v) \coloneqq (\psi \mid T(v)), \end{aligned} \tag{5.2.1.20}$$

as desired.

(i) Suppose that V is a vector space. To show that it is injective, we check that the kernel is 0. So, let $v \in V$ suppose that $(\phi \mid v) = 0$ for all $\phi \in V^\dagger$. If $\mathbb{K} = 0$, then $V = 0$, and so we are immediately done. Otherwise, if $v \neq 0$, then there is a linear-functional $\phi\colon V \to \mathbb{K}$ that sends v to 1, in which case $(\phi \mid v) = 1 \neq 0$, a contradiction. Thus, it must be the case that $v = 0$.

(ii) Suppose that V is a finite-dimensional vector space. We know from the defining result of the dual basis (Proposition 5.2.2.40) that $\dim(V) = \dim(V^\dagger) = \dim([V^\dagger]^\dagger)$. Thus, we have a injective linear map $V \to [V^\dagger]^\dagger$ between two finite-dimensional vector spaces of the same dimension, and hence it must in fact be an isomorphism (Corollary 2.2.2.14). ■

[a] This part of the proof makes uses of things we have not yet encountered. You can verify it is not circular as these new things don't make use of this result. (It doesn't make sense to move this result so drastically just to avoid this small worry about potential circularity). It makes use of the Transpose (Definition 5.2.2.8), as well as the concept of a *commutative diagram*, which is explained in a remark of Theorem 5.3.1.1.

Thus, in this sense, if V is a finite-dimensional vector space, then V is "the same" as $[V^\dagger]^\dagger$, in which case V and $V^\dagger$ are "on the same footing" in the sense that the dual of V is $V^\dagger$ and the dual of $V^\dagger$ 'is' V.

Be careful however—this doesn't hold in infinite-dimensions.

▪ **Example 5.2.1.21 — A module V for which $V \to [V^\dagger]^\dagger$ is not injective** Define $\mathbb{K} := \mathbb{Z}$ and $V := \mathbb{Z}/2\mathbb{Z}$.

Exercise 5.2.1.22 Show that there is no $\mathbb{Z}$-linear map $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$.

R A "$\mathbb{Z}$-linear map" is the same as a group homomorphism—see Example 1.1.22.

Thus, $V^\dagger = 0$, and so certainly $[V^\dagger]^\dagger = 0$, and hence the map $V \to [V^\dagger]^\dagger$ cannot be injective.

▪ **Example 5.2.1.23 — A vector space V for which $V \to [V^\dagger]^\dagger$ is not an isomorphism** Define $\mathbb{K} := \mathbb{C}$ and $V := \mathbb{C}^\infty$. By Example 5.2.1.7, we know that $[\mathbb{C}^\infty]^\dagger \cong \mathbb{C}^\mathbb{N}$ via the map $\mathbb{C}^\mathbb{N} \ni a \mapsto (a \,|\, \cdot) \in [\mathbb{C}^\infty]^\dagger$. Hence, $[[\mathbb{C}^\infty]^\dagger]^\dagger = [\mathbb{C}^\mathbb{N}]^\dagger$ and the map $\mathbb{C}^\infty \to [\mathbb{C}^\mathbb{N}]^\dagger$ is given by $\mathbb{C}^\infty \ni b \mapsto (\cdot \,|\, b) \in [\mathbb{C}^\mathbb{N}]^\dagger$. We thus wish to find $\phi \in [\mathbb{C}^\mathbb{N}]^\dagger$ such that $\phi \neq (\cdot \,|\, b)$ for any $b \in \mathbb{C}^\infty$.

Let $e_k \in \mathbb{C}^\infty$ denote the sequence that is identically 0 except for a 1 at index k. Then, $(e_k \,|\, b) = b_k$, and so in particular, for every $b \in C^\infty$, there is some e_{k_b} such that $(e_{k_b} \,|\, b) = 0$ (recall that Example 1.1.18 the elements of $\mathbb{C}^\infty$ are those sequences which are eventually 0).

Using Theorem 2.2.25, let $\phi\colon \mathbb{C}^{\mathbb{N}} \to \mathbb{C}$ be a linear-functional such that $\phi(e_k) = 1$ for all $k \in \mathbb{N}$. We then cannot have that $\phi = (\cdot \mid b)$ for any $b \in \mathbb{C}^{\infty}$ as $\phi(e_k) \neq 0$ for all k, and so $V \to [V^{\dagger}]^{\dagger}$ is not surjective.

On the off chance this talk of dual-spaces has you thinking "Okay, but if $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, \mathbb{K})$ is so damn interesting, why don't we care about $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(\mathbb{K}, V)$.". The answer is that "We do care.", but there's no need to have a separate discussion—this 'is' just V itself.

Proposition 5.2.1.24 — $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(\mathbb{K}, V) \cong V$ Let V be a $\mathbb{K}$-module. Then, the map

$$\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(\mathbb{K}, V) \ni \phi \mapsto \phi(1) \in V \tag{5.2.1.25}$$

is a natural isomorphism.

Proof. It follows from the definition that it is linear. To check naturality, let $T\colon U \to V$ be linear. Then, this map is natural (Definition B.3.2.3) iff the following diagram commutes.

$$\begin{array}{ccc} \mathrm{Mor}(\mathbb{K}, U) & \longrightarrow & U \\ \downarrow & & \downarrow \\ \mathrm{Mor}(\mathbb{K}, V) & \longrightarrow & V \end{array} \tag{5.2.1.26}$$

Writing out the definitions of these maps, we see that this commutes for tautological reasons.

To show that it is an isomorphism, we construct an inverse. For every $v \in V$, there is a unique linear map $\phi_v : \mathbb{K} \to V$ such that $\phi_v(1) = v$. By construction, $V \ni V \mapsto \phi_v \in \mathrm{Mor}(\mathbb{K}, V)$ is an inverse to $\phi \mapsto \phi(1)$. ∎

Before moving on, we end this subsection with some more examples of dual-spaces and linear-functions.

■ **Example 5.2.1.27 — Evaluation maps** Let $x_0 \in \mathbb{R}$. Then, $\mathrm{ev}_{x_0} : \mathrm{Mor}_{\mathbf{Top}}(\mathbb{R}, \mathbb{C}) \to \mathbb{C}$, the ***evaluation map*** at x_0 defined by

$$\mathrm{ev}_{x_0}(f) := f(x_0), \tag{5.2.1.28}$$

is a linear-functional.

Of course, it restricts to $\mathbb{C}[x] \subseteq C^\infty(\mathbb{R}) \subseteq \mathrm{Mor}_{\mathbf{Top}}(\mathbb{R}, \mathbb{C})$ to give linear-functionals on $\mathbb{C}[x]$ and $C^\infty(\mathbb{R})$ as well.

R $\mathrm{Mor}_{\mathbf{Top}}(\mathbb{R}, \mathbb{C})$ is the category-theoretic notation for the set of all *continuous* functions from $\mathbb{R}$ to $\mathbb{C}$. ("**Top**" is the category of topological spaces,[a] and the morphisms in this category are by definition continuous functions.)

[a] Without giving the precise definition, the "point" of topological spaces is that they are one of the most general contexts in which the notion of continuity makes sense.

■ **Example 5.2.1.29 — Integration** Let X be a measure space. Then, the map $\mathrm{L}^1(X) \to \mathbb{C}$, $f \mapsto \int_X \mathrm{d}x\, f(x)$, is a linear-functional on $\mathrm{L}^1(X)$.

R $\mathrm{L}^1(X)$ is the set of all (complex-valued) *integrable* on X. If you've never studied measure theory before, you don't need to know the precise definition to understand what's going on here—integrable functions are essentially just those functions for which the integral is defined and the integral is a linear-functional simply because $\int_X \mathrm{d}x\, [f_1(x) + f_2(x)] = \int_X \mathrm{d}x\, f_1(x) + \int_X \mathrm{d}x\, f_2(x)$ and $\int_X \mathrm{d}x\, [\alpha f(x)] = \alpha \int_X \mathrm{d}x\, f(x)$.

■ **Example 5.2.1.30 — The trace** Let V be a finite-dimensional vector space over an algebraically-closed field $\mathbb{F}$.

Then,

$$\mathrm{End}_{\mathbf{Vect}_{\mathbb{F}}}(V) \ni T \mapsto \sum_{\lambda \in \mathrm{Eig}(T)} \dim(\mathrm{Eig}^{\infty}_{\lambda})\lambda \in \mathbb{F} \quad (5.2.1.31)$$

is a linear-functional on $\mathrm{End}_{\mathbf{Vect}_{\mathbb{F}}}(V)$.

R The dimension here is to account for the "multiplicity" of the eigenvalue.

Exercise 5.2.1.32 Let $\mathbb{K}$ be a ring. By Example 5.2.1.7, $[\mathbb{K}^{\infty}]^{\dagger} = \mathbb{K}^{\mathbb{N}}$. By the previous result, $\mathbb{K}^{\infty}$ embeds into $[\mathbb{K}^{\mathbb{N}}]^{\dagger}$. Show that $\mathbb{K}^{\infty} \to [\mathbb{K}^{\mathbb{N}}]^{\dagger}$ is not surjective.

5.2.2 Dual-pairs

The definition and basic facts

While it won't be true in general, in our case of interest, V and $V^{\dagger}$ will be 'on the same footing'. A priori, that just doesn't look like the case at all—you start with V and then $V^{\dagger}$ is a collection of functions with domain V. However, if we shift our perspective, it becomes clearer how this might work.

Consider instead the map $V^{\dagger} \times V \ni \langle \phi, v \rangle \mapsto \phi(v) \in \mathbb{K}$. In fact, we will suggestively write $(\phi \,|\, v) = \phi(v)$ to stress that we want to think of $V^{\dagger}$ "on the same footing" as V. Now the situation is more symmetric. This motivates us to define the notion of a *dual-pair*.[6]

Definition 5.2.2.1 — Dual-pair A ***dual-pair*** is

(I). two $\mathbb{K}$-$\mathbb{K}$-bimodules V and W; together with
(II). a bilinear map $(\cdot \,|\, \cdot) \colon W \times V \to \mathbb{K}$.

[6] You should also take note that (Theorem 5.2.1.11), at least for finite-dimensional vector spaces over fields, $[V^{\dagger}]^{\dagger}$ 'is' V. Thus, if you take the dual of V you get $V^{\dagger}$ (duh), but furthermore taking the dual of $V^{\dagger}$ gives you $[V^{\dagger}]^{\dagger} = V$ back as well. In brief, V and $V^{\dagger}$ are the duals of each other, which is perhaps a stronger argument that we should be thinking of V and $V^{\dagger}$ as "on the same footing". Be warned, however, this is very much special to the finite-dimensional case.

R $(\cdot \mid \cdot)$ is the ***pairing*** of V and W. As this in principle contains all the data of a dual-pair itself (V and W are 'encoded' in the domain of $(\cdot \mid \cdot)$", we may refer to "$(\cdot \mid \cdot)\colon W \times V \to \mathbb{K}$" itself as the "dual-pair".

R This notation is useful because it allows us to treat V and W "on the same footing" when they otherwise might not be. For example, if you look at the definition of orthogonal complement (Definition 5.2.2.17), if we had tried to define this using just V and $V^\dagger$ (so without using the language of "dual-pair"), then the orthogonal complement of $S \subseteq V^\dagger$ would be a subset $S^\perp \subseteq [V^\dagger]^\dagger$ of the double dual, whereas we want $S^\perp \subseteq V$.

R Warning: Some authors require $(\cdot \mid \cdot)$ to be *nondegenerate* (Definition 5.2.2.2), whereas we do not. If we want to consider a nondegenerate (or nonsingular) pairing, we will say so explicitly.

Note that, given a dual pair $(\cdot \mid \cdot)\colon W \times V \to \mathbb{K}$, we have maps $V \to W^\dagger$ and $W \to V^\dagger$, defined by $v \mapsto (\cdot \mid v)$ and $w \mapsto (w \mid \cdot)$ respectively.

Definition 5.2.2.2 — Nonsingular and nondegenerate
Let $(\cdot \mid \cdot)\colon W \times V \to \mathbb{K}$ be a dual-pair.

(i). $(\cdot \mid \cdot)$ is ***nonsingular*** iff the maps $V \to W^\dagger$ and $W \to V^\dagger$ are both isomorphisms.

(ii). $(\cdot \mid \cdot)$ is ***nondegenerate*** iff the maps $V \to W^\dagger$ and $W \to V^\dagger$ are both injective.

R Given $v \in V$, the linear-functional $(\cdot \mid v) \in W^\dagger$ is the ***dual-vector*** of v with respect to $(\cdot \mid \cdot)$. Similarly, given $w \in W$, the linear-functional $(w \mid \cdot) \in V^\dagger$ is the ***dual-vector*** of w with respect to $(\cdot \mid \cdot)$.

Using this language, nondegeneracy says that the dual-vector $(\cdot \mid v)$ is uniquely determined by v (and dually for $w \in W$). Similarly, nonsingularity says

that every element of $W^\dagger$ is of this form (and dually for $V^\dagger$).

The condition of nondegeneracy is usually stated in the following equivalent form.

Proposition 5.2.2.3 Let $(\cdot\,|\,\cdot)\colon W \times V \to \mathbb{K}$ be a dual-pair. Then, $(\cdot\,|\,\cdot)$ is nondegenerate iff $(w\,|\,v) = 0$ for all $w \in W$ implies $v = 0$ and $(w\,|\,v) = 0$ for all $v \in V$ implies $w = 0$.

Proof. We leave this as an exercise.

Exercise 5.2.2.4 Prove the result.

■

Proposition 5.2.2.5 Let $(\cdot\,|\,\cdot)\colon W \times V \to \mathbb{K}$ be a dual pair.

(i). If $(\cdot\,|\,\cdot)$ is nonsingular, then it is nondegenerate.
(ii). Suppose that V and W are finite-dimensional vectors spaces. Then, $(\cdot\,|\,\cdot)$ is nonsingular iff it is nondegenerate.

Proof. (i) Immediate from the definitions.

(ii) ($\Rightarrow$) This is (i).
($\Leftarrow$) Suppose that $(\cdot\,|\,\cdot)$ is nondegenerate. Then, it is nonsingular as injective is equivalent to bijective for finite-dimensional vector spaces (Corollary 2.2.2.14). ■

Proposition 5.2.2.6 Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule. Then, $(\cdot\,|\,\cdot)\colon V^\dagger \times V \to \mathbb{K}$ is a dual-pair.
Furthermore, it is nondegenerate if V is a vector space and nonsingular if V is a finite-dimensional vector space.

R A corollary of this is that $\dim(V) = \dim(V^\dagger)$ if V is a finite-dimensional vector space: The pairing is nonsingular, and so $\mathcal{B}^\dagger$ is a basis of $V^\dagger$ by

Proposition 5.2.2.40. As $|\mathcal{B}| = |\mathcal{B}^\dagger|$, it follows that $\dim(V) = \dim(V^\dagger)$.

Proof. We leave this as an exercise.

Exercise 5.2.2.7 Prove the result.

■

The transpose

We now have a notion of "dual" for vector spaces, and so, as you might expect, we also get a notion of "dual" for linear-transformations.

Definition 5.2.2.8 — Transpose Let V_1 and V_2 be $\mathbb{K}$-$\mathbb{K}$-bimodules and let $T\colon V_1 \to V_2$. Then, the ***transpose*** of T, $T^\dagger\colon V_2^\dagger \to V_1^\dagger$, is defined by

$$(T^\dagger(w_2) \,|\, v_1) := (w_2 \,|\, T(v_1)) \tag{5.2.2.9}$$

for $w_2 \in V_2^\dagger$ and $v_1 \in V_1$.

R $T^\dagger$ is also called the ***dual-map*** or just ***dual*** of T.

R Note that this definition doesn't actually require the existence of any dual-pairs. That said, we are going to be primarily interested in the case when there are pairings involved.[a]

Let $(\cdot\,|\,\cdot)\colon W_1 \times V_1 \to \mathbb{K}$ and $(\cdot\,|\,\cdot)\colon W_2 \times V_2 \to \mathbb{K}$ be *nonsingular* dual-pairs. Nonsingularity implies in particular that $W_2 \cong V_2^\dagger$ and $W_1 \cong V_1^\dagger$,[b] in which case we will readily make these identifications. We can then view $T^\dagger$ as a map $T^\dagger\colon W_2 \to W_1$. If we do have nonsingular dual-pairs like this, we will always make this identification.

[a] This is why we used "w_2" above instead of something like "ϕ_2".

[b] Note that this does not quite use the full strength of singularity—it is also the case that $W_2^\dagger \cong V_2$ and $W_1^\dagger \cong V_1$. However, if we want to take the

transpose twice to get back a map $V_1 \to V_2$ (which it turns out agrees with the original map—see Proposition 5.2.2.12), we will need the full strength of nonsingularity.

In case you were wondering, yes, this is the same "transpose" you have probably heard of before in the context of matrices, though we'll have to wait until we've discussed dual-bases to see exactly why—see Proposition 5.2.2.44. What follows is an example of the transpose for something besides matrix linear-transformations.

▪ **Example 5.2.2.10** Recall that (Example 5.2.1.7) $[\mathbb{K}^\infty]^\dagger \cong \mathbb{K}^{\mathbb{N}}$. Thus, regarding the left and right shift operators (Example 1.1.48) $L, R\colon \mathbb{K}^\infty \to \mathbb{K}^\infty$ as operators on $\mathbb{K}^\infty$, their transposes $L^\dagger, R^\dagger\colon \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$ are operators on $\mathbb{K}^{\mathbb{N}}$.

Exercise 5.2.2.11 Show that $L^\dagger = R$ and $R^\dagger = L$ as operators on $\mathbb{K}^{\mathbb{N}}$.

Proposition 5.2.2.12 — Properties of the transpose Let $(\cdot\,|\,\cdot)\colon W_0 \times V_0 \to$, $(\cdot\,|\,\cdot)\colon W_1 \times V_1 \to \mathbb{K}$, and $(\cdot\,|\,\cdot)\colon W_2 \times V_2 \to \mathbb{K}$ be nonsingular dual-pairs.

(i). $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}\text{-}\mathbb{K}}(V_1, V_2) \ni T \mapsto T^\dagger \in \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}\text{-}\mathbb{K}}(W_2, W_1)$ is linear.

(ii). $[T \circ S]^\dagger = S^\dagger \circ T^\dagger$ for $S\colon V_0 \to V_1$ and $T\colon V_1 \to V_2$ linear.

(iii). $[\mathrm{id}_{V_0}]^\dagger = \mathrm{id}_{V_0^\dagger}$.

(iv). $[T^\dagger]^\dagger = T$.

R For what it's worth, (ii) and (iii) are the statement that $-^\dagger$ is a *cofunctor* (Definition B.3.1.10), which explains why we use the same notation for $T^\dagger$ as we do for $V^\dagger$ (and in turn why $T^\dagger$ is sometimes called the "dual" of T).

Proof. We leave this as an exercise.

Exercise 5.2.2.13 Prove the result.

■

Proposition 5.2.2.14 Let V be a finite-dimensional vector space, let $T\colon V \to V$ be linear, let $v \in V$. Then,

$$\mathrm{Eig}(T) = \mathrm{Eig}(T^\dagger). \tag{5.2.2.15}$$

R Warning: This fails in infinite-dimensions—see Example 5.2.2.16.

Proof. $\lambda \in \mathrm{Eig}(T)$ iff $\mathrm{Ker}(T-\lambda) \neq 0$ iff[a] $T-\lambda$ is invertible iff there is a linear map $S\colon V \to V$ such that $S(T-\lambda) = \mathrm{id} = (T-\lambda S)$ iff[b,c] there is a linear map $R\colon V^\dagger \to V^\dagger$ such that $R(T^\dagger - \lambda) = \mathrm{id}_{V^\dagger} = (T^\dagger - \lambda)R$ iff $\ldots \lambda \in \mathrm{Eig}(T^\dagger)$. ■

[a] This requires finite-dimensionality.

[b] This uses finite-dimensionality again. Certainly, we have $\Rightarrow$ all the time, but to go backwards, we need to use the fact that $[A^\dagger]^\dagger = A$, which requires finite-dimensionality—see Proposition 5.2.2.6.

[c] Of course, we will have that $R = S^\dagger$.

■ **Example 5.2.2.16 — $\mathrm{Eig}(T) \neq \mathrm{Eig}(T^\dagger)$** Consider the right shift operator $R\colon \mathbb{K}^\infty \to \mathbb{K}^\infty$. By Example 4.2.36, $\mathrm{Eig}(R) = \emptyset$. On the other hand, from Example 5.2.2.10, we know that $R^\dagger = L$ as an operator on $\mathbb{K}^\mathbb{N} \cong [\mathbb{K}^\infty]^\dagger$, and again from Example 4.2.36 that $\mathrm{Eig}(R^\dagger) = \mathrm{Eig}(L) = \mathbb{K}$.

The orthogonal complement

The intuition behind the following concept will likely be easier to understand when we begin our study of inner-product spaces,[7] though one can see it's usefulness easily enough: it allows us to related the kernel and image of $T^\dagger$ to that of T—see Proposition 5.2.2.32.

Definition 5.2.2.17 — Orthogonal complement Let $(\cdot \mid \cdot)\colon W \times V \to \mathbb{K}$ be a dual-pair.

(i). For $S \subseteq V$, the ***orthogonal complement*** of S, $S^\perp$, is defined by

$$S^\perp := \{w \in W : (w \mid v) = 0 \text{ for all } v \in S.\}\,. \quad (5.2.2.18)$$

(ii). For $S \subseteq V^\dagger$, the ***orthogonal complement*** of S, $S^\perp$, is defined by

$$S^\perp := \{v \in V : (w \mid v) = 0 \text{ for all } w \in S.\}\,. \quad (5.2.2.19)$$

R Let $v \in \mathbb{K}^d$ and $\phi \in [\mathbb{K}^d]^\dagger$. Then,

$$(\phi \mid v) = \phi v := \sum_{k=1}^{d} \phi_k v_k, \quad (5.2.2.20)$$

where "ϕv" here denotes matrix multiplication (recall that (Example 5.2.1.3) ϕ is a row-vector, so a $1 \times d$ matrix, just as v is a $d \times 1$ matrix). This expression should remind you of the dot product. Of course, this won't literally be the case in general, but nevertheless, much of the intuition about the "pairing" $(w \mid v)$ in general comes from your intuition about the dot product.

For example, in this case, you'll recall that, by definition, two vectors are *orthogonal* iff their dot product vanishes, whence the term "orthogonal complement": $S^\perp$ is the set of vectors orthogonal to the set of 'covectors'[a] S (or dually if $S \subseteq V$).

[7] See Subsection 6.6.5.

R The symbol "⊥" in English is read (at least by me) as "perp" (as in "*perp*endicular"). We'll see later when we study inner-product spaces that, in a sense, "orthogonal" is essentially equivalent to "perpendicular", hence "perp".

R I have also seen the notation S^0 used. I've also seen this referred to as the *annihilator* of S,

[a] In quotes because unless $W = V^\dagger$, it need not literally be the case that the elements of S are linear-functionals on V.

Proposition 5.2.2.21 — Properties of the orthogonal complement Let $(\cdot\,|\,\cdot)\colon W \times V \to \mathbb{K}$ be a dual pair and let S and T either both be subsets of V or both be subsets of W.

(i). $S^\perp$ is a subspace.
(ii). If $S \subseteq T$, then $T^\perp \subseteq S^\perp$.
(iii). if $(\cdot\,|\,\cdot)$ is a nonsingular pairing of vector spaces, then $[S^\perp]^\perp = \mathrm{Span}(S)$.
(iv). $0^\perp = V$ and $0^\perp = W$.
(v). If the pairing is nondegenerate, then $V^\perp = 0$ and $W^\perp = 0$.
(vi). If V and W are finite-dimensional vector spaces, then

$$\dim(V) = \dim(U) + \dim(U^\perp) \tag{5.2.2.22}$$

if $U \subseteq V$ is a subspace; and

$$\dim(W) = \dim(U) + \dim(U^\perp) \tag{5.2.2.23}$$

if $U \subseteq W$ is a subspace.

R Note that this doesn't require S or T to be a subspaces themselves.

R As in Rank-Nullity Theorem (Theorem 2.2.2.2), (vi) generalizes to the statements that $U^\perp \to (V/U)^\dagger$ and $U^\perp \to (W/U)^\dagger$ are isomorphisms (at least for nonsingular pairings).[a]

R If you care, I suspect that (iii) holds if W and V are semisimple (Definition C.5.8) (this is automatic if $\mathbb{K}$ is a division ring by Proposition 4.4.1.47).

[a]Every $w \in U^\perp$ can be regarded as a linear map $V \to \mathbb{K}$ that vanishes on U, and hence descends to a well-defined linear map $V/U \to \mathbb{K}$. Dually for the case $U \subseteq W$.

Proof. (i) We leave this as an exercise.

Exercise 5.2.2.24 Prove this part.

(ii) We leave this as an exercise.

Exercise 5.2.2.25 Prove this part.

(iii) Without loss of generality, take $S \subseteq V$. Let $v \in S$. Then, by definition, $(w \mid v) = 0$ for all $w \in S^\perp$, and hence $v \in [S^\perp]^\perp$. Thus, $S \subseteq [S^\perp]^\perp$, and hence, as $[S^\perp]^\perp$ is a subspace, $\mathrm{Span}(S) \subseteq [S^\perp]^\perp$.

For the other inclusion, we first prove it in the case $S \subseteq V$ itself is a subspace, so that $\mathrm{Span}(S) = S$. Write $V = S \oplus T$ for some subspace $T \subseteq V$. We first check that $W = S^\perp \oplus T^\perp$. If $w \in S^\perp \cap T^\perp$, then $(w \mid s + t) = 0$ for all $s \in S$ and $t \in T$, and hence $w = 0$ by nondegeneracy. To show spanning, let $w \in W$. As $V = S \oplus T$, there is a unique linear-functional $w_s : V \to \mathbb{K}$ such $w_s|_S = (w \mid \cdot)|_S$ and $w_s|_T = 0$. Similarly there is a unique linear-functional $w_t : V \to \mathbb{K}$ such that $w_t|_S = 0$ and $w_t|_T = (w \mid \cdot)|_T$. By nonsingularity, every element of $V^\dagger$ is of the form $(u \mid \cdot)$ for a unique $u \in W$. By abuse of notation, let $w_s, w_t \in W$ be the unique elements such that $(w_s \mid s) = (w \mid s)$ for $s \in S$ and $(w_s \mid t) = 0$ for $t \in T$, and $(w_t \mid s) = 0$ for $s \in S$ and $(w_t \mid t) = (w \mid t)$ for $t \in T$. It follows immediately from this that $w_s \in T^\perp$ and $w_t \in S^\perp$. We claim that $w = w_s + w_t$.

So, let $v \in V$ and write $v = s + t$ for unique $s \in S$ and $t \in T$. Then,

$$\begin{aligned}(w \mid v) &= (w \mid s + t) = (w \mid s) + (w \mid t) \\ &= (w_s \mid s) + (w_t \mid t) \\ &= (w_s \mid s + t) + (w_t \mid s + t) \\ &= (w_s \mid v) + (w_t \mid v) = (w_s + w_t \mid v).\end{aligned} \tag{5.2.2.26}$$

By nondegeneracy, we have that $w = w_s + w_t$, as desired. Hence, $W = S^\perp \oplus T^\perp$.

We return to checking that $[S^\perp]^\perp \subseteq S$ if $S \subseteq V$ is a subspace. So, let $v \in [S^\perp]^\perp$ and write $v = s+t$ for unique $s \in S$ and $t \in T$. We wish to show that $t = 0$. To show this, by nondegeneracy, it suffices to show that $(w \mid t) = 0$ for all $w \in W$. So, let $w \in W$. We now know that we can write $w = w_s + w_t$ for unique $w_s \in T^\perp$ and $w_t \in S^\perp$. We then have

$$(w \mid t) = (w_t \mid t) = (w_t \mid s + t) = (w_t \mid v) = 0, \tag{5.2.2.27}$$

and so $t = 0$, as desired.

Finally, we prove that $[S^\perp]^\perp \subseteq \mathrm{Span}(S)$ for an arbitrary subset $S \subseteq V$. We have that $S \subseteq \mathrm{Span}(S)$, and so $\mathrm{Span}(S)^\perp \subseteq S^\perp$, and so

$$[S^\perp]^\perp \subseteq [\mathrm{Span}(S)^\perp]^\perp = \mathrm{Span}(S), \tag{5.2.2.28}$$

as desired.

(iv) We leave this as an exercise.

Exercise 5.2.2.29 Prove this part.

(v) We leave this as an exercise.

Exercise 5.2.2.30 Prove this part.

(vi) We prove the case $U \subseteq V$. The other case is essentially identical. Let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ be a basis for V with $\{b_1, \ldots, b_e\}$ a basis of U, so that $\mathcal{B}^\dagger := \{[b^1]^\dagger, \ldots, [b^d]^\dagger\}$ is a basis for $V^\dagger$.[a] As $([b^k]^\dagger \,|\, b_l) = \delta^k_{\ l}$, [b] $[b^k]^\dagger \in U^\perp$ iff $e+1 \leq m$. Furthermore, for $\phi \in U^\perp$, if we write $\phi = \phi_1 \cdot [b^1]^\dagger + \cdots + \phi_d \cdot [b^d]^\dagger$, plugging in b_k for $1 \leq k \leq e$ shows that we must have $\phi_k = 0$. Thus, $\phi \in \mathrm{Span}([b^{e+1}]^\dagger, \ldots, [b^d]^\dagger)$, and hence $\{[b^{e+1}]^\dagger, \ldots, [b^d]^\dagger)$ forms a basis for $U^\perp$. Hence,

$$\dim(U) + \dim(U)^\perp = e + (d-e) = d = \dim(V). \quad (5.2.2.31)$$

■

[a] This is the dual-basis which we will meet shortly—see Proposition 5.2.2.40.

[b]

Proposition 5.2.2.32 Let $(\cdot \,|\, \cdot)\colon W_1 \times V_1 \to \mathbb{K}$ and $(\cdot \,|\, \cdot)\colon W_2 \times V_2 \to \mathbb{K}$ be nonsingular dual-pairs, and let $T\colon V_1 \to V_2$ be linear. Then,

$$\mathrm{Ker}(T^\dagger) = \mathrm{Im}(T)^\perp \quad (5.2.2.33)$$

$$\mathrm{Im}(T^\dagger) = \mathrm{Ker}(T)^\perp \quad (5.2.2.34)$$

R I think this should be relatively easy to remember. † comes outside of Ker and Im, 'flips upside-down', and Ker gets replaced with Im and vice versa.

R In particular, this (together with Proposition 5.2.2.21) implies (for vector spaces anyways) that T is injective iff $T^\dagger$ is surjective and that T is surjective iff $T^\dagger$ is injective.

R Do take note of this. It is quite important.

Also, don't overlook the fact that *nonsingularity* is a hypothesis.

Proof. (5.2.2.33) $w_2 \in \mathrm{Ker}(T^\dagger)$ iff $T^\dagger(w_2) = 0$ iff $0 = (T^\dagger(w_2) \,|\, v_1) = (w_2 \,|\, T(v_1))$ for all $v_1 \in V_1$ iff $w_2 \in \mathrm{Im}(T)^\perp$.

(5.2.2.34) Replacing T with $T^\dagger$ in (5.2.2.33), we obtain

$$\mathrm{Ker}(T) = \mathrm{Ker}([T^\dagger]^\dagger) = \mathrm{Im}(T^\dagger)^\perp. \tag{5.2.2.35}$$

Taking the perp of this equation, we obtain

$$\mathrm{Ker}(T)^\perp = \mathrm{Span}(\mathrm{Im}(T^\dagger)) = \mathrm{Im}(T^\dagger), \tag{5.2.2.36}$$

as desired. ■

Among other things, this can be used to figure out the "row-space" of matrices as is often asked in elementary linear algebra courses.

▪ **Example 5.2.2.37 — Row-space** Let A be an $m \times n$ matrix. The ***row-space*** of A, $\mathrm{Row}(A)$, is the span of the rows of A. The first thing is to note that $\mathrm{Row}(A) = \mathrm{Col}(A^\dagger)$. Hence,

$$\mathrm{Row}(A) = \mathrm{Col}(A^\dagger) = \mathrm{Null}(A)^\perp. \tag{5.2.2.38}$$

As you already know how to compute null spaces, this gives you an alternative description of $\mathrm{Row}(A)$. In particular, from Proposition 5.2.2.21(vi),

$$\begin{aligned} \dim(\mathrm{Row}(A)) &= \dim(\mathrm{Null}(A)^\perp) \\ &= \dim(\mathbb{K}^n) - \dim(\mathrm{Null}(A)) =^a \dim(\mathrm{Col}(A)). \end{aligned} \tag{5.2.2.39}$$

Similarly, if you had been asked to calculate $\mathrm{Null}(A^\dagger)$ for whatever reason, you could use the fact that $\mathrm{Null}(A^\dagger) = \mathrm{Im}(A)^\perp$.

[a] By the Rank-Nullity Theorem (Theorem 2.2.2.2).

The dual basis

Given a dual-pair $(\cdot\,|\,\cdot)\colon W \times V \to \mathbb{K}$ and a basis $\mathcal{B} \subseteq V$, there will be a corresponding subset $\mathcal{B}^\dagger \subseteq W$ which is always linearly-independent and, in good cases, a basis of W, the *dual basis*.

Proposition 5.2.2.40 — The dual basis Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule, let $\mathcal{B}$ be a basis of V, for $b \in \mathcal{B}$ let $b^\dagger\colon V \to \mathbb{K}$ be the unique linear map such that

$$b^\dagger(c) = \begin{cases} 1 & \text{if } c = b \\ 0 & \text{otherwise,} \end{cases} \tag{5.2.2.41}$$

and define $\mathcal{B}^\dagger := \{b^\dagger : b \in \mathcal{B}\}$.

(i). If V is a vector space, then $\mathcal{B}^\dagger \subseteq V^\dagger$ is linearly-independent.

(ii). If V is a finite-dimensional vector space, then $\mathcal{B}^\dagger \subseteq V^\dagger$ is a basis.

R If $\mathcal{B}^\dagger$ is actually a basis of $V^\dagger$, then it is referred to as the ***dual basis*** of $\mathcal{B}$.

Proof. We leave this as an exercise.

Exercise 5.2.2.42 Prove the result.

■

Exercise 5.2.2.43 Find an example of a dual-pair with basis $\mathcal{B} \subseteq V$ such that $\mathcal{B}^\dagger$ does *not* span W.

It's now time to return to the issue of how this notion of transpose corresponds with the classical one you might already be familiar with.

Proposition 5.2.2.44 — Transpose of a matrix Let $(\cdot\,|\,\cdot)\colon W_1 \times V_1 \to \mathbb{K}$ and $(\cdot\,|\,\cdot)\colon W_2 \times V_2 \to \mathbb{K}$ be nonsin-

gular dual-pairs, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ and $C =: \{c_1, \ldots, c_e\}$ be bases for V_1 and V_2 respectively, and let $T\colon V_1 \to V_2$ be linear. Then,

$$[T^\dagger]_{\mathcal{B}^\dagger \leftarrow C^\dagger} = [T]_{C \leftarrow \mathcal{B}}{}^\dagger, \tag{5.2.2.45}$$

where we have defined

$$[A^\dagger]^i{}_j := A_j{}^i \tag{5.2.2.46}$$

for A an $e \times d$ matrix.

R $A^\dagger$ is the ***transpose*** of A. Intuitively, it is the matrix formed by 'flipping' A about its diagonal. For example,

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}^\dagger = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}. \tag{5.2.2.47}$$

That we have staggered the indices the way we have will be clear when we study index notation—see Notation 5.4.2.8. In the context of matrices, however, this staggering is just suggestive—the only thing that really matters is the ordering, and so we could have written $[A^\dagger]_{ij} := A_{ji}$, though this is probably not the best practice.

R In words, for any choice of bases, the matrix of the transpose is the transpose of the matrix. It is in this sense that the "transpose" of a linear-transformation and the "transpose" of a matrix coincide.

Proof. We leave this as an exercise.

Exercise 5.2.2.48 Prove the result.

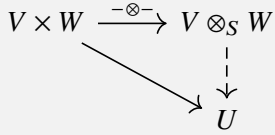
■

5.3 The tensor product

We said before that multilinear algebra is the study of multilinear maps. From the definition Definition 5.1.3.1, it is clear that (ordinary) linear algebra will be relevant to a study of linear maps, but what would be really awesome is if we could reduce the entire study of multilinear maps to just linear maps so that we can apply everything we've learned thus far. It is the *tensor product* that allows us to do this.

5.3.1 The definition

Theorem 5.3.1.1 — Tensor product (of bimodules). Let V be an R-S-bimodule and let W be an S-T-bimodule. Then, there is a unique bilinear map $-\otimes-\colon V\times W\to V\otimes_S W$ into the R-T-bimodule $V\otimes_S W$, the ***tensor product*** of V and W over S, such that if $V\times W\to U$ is any other bilinear map into an R-T-bimodule U, then there is a unique map of bimodules $V\otimes_S W\to U$ such that the following diagram commutes.



(5.3.1.2)

R For $v\in V$ and $w\in W$, the image under the bilinear map $V\times W\to V\otimes_S W$ is written $v\otimes w\in V\otimes_S W$ and is the ***tensor product*** of v and w.

R There is an analogous result for not just bilinear maps, but all types of multilinear maps. Specifically, if V_k is a $\mathbb{K}_k$-$\mathbb{K}_{k+1}$-bimodules, then we have a multilinear map $V_1\times\cdots\times V_m\to V_1\otimes_{\mathbb{K}_1}\cdots\otimes_{\mathbb{K}_{m-1}}V_m$ into a $\mathbb{K}_1$-$\mathbb{K}_m$-bimodule that is "universal" in a sense exactly analogous to (5.3.1.2).

Additionally, the empty tensor product over $\mathbb{K}$, that is, the tensor product of no spaces, is defined to be

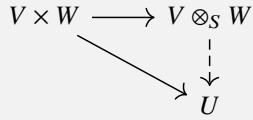
$\mathbb{K}$ itself, the motivation for which can be seen from Proposition 5.3.3.9(i)(ii). In symbols:

$$\underbrace{V \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} V}_{0} := \mathbb{K}. \tag{5.3.1.3}$$

R To clarify, there are tensor products of *bimodules*, and then there are tensor products of *vectors themselves*. The tensor product of two vectors 'lives in' the tensor product of the corresponding bimodules. And in fact, *everything* in $V \otimes_S W$, while *not* of the form $v \otimes w$ itself necessarily, can be written as a finite sum of elements of this form—see Proposition 5.3.3.1. (Elements of the form $v \otimes w$ are sometimes called ***pure*** or ***simple***, as opposed to, e.g. , $v_1 \otimes w_1 + v_2 \otimes w_2$).

R If S is clear from context, it may be omitted: $V \otimes W := V \otimes_S W$.

R As in Theorem C.3.2.12 (the defining result for polynomial algebras), $V \otimes_S W$ is not *literally* unique, but instead, it is "unique up to unique isomorphism". In this case, this means that if $V \times W \to U$ is another bilinear map into a R-T-bimodule satisfying the same property as $V \otimes_S W$, then there is a unique isomorphism of bimodules $V \otimes_S W \to U$ such that the following diagram commutes.



(5.3.1.4)

Thus, while people do often say "unique up to *unique* isomorphism", the isomorphism is itself not unique—it would be more accurate to say "unique up to unique isomorphisms which commute with blah blah blah diagram". That is to say, while there might be many isomorphisms between $V \otimes_S W$ and U, there is only one which makes the above diagram commute. Given that the latter option, while more accurate, is incredibly verbose, people just stick to "unique up to unique isomorphism".

R A common question I've gotten from students is "But what actually *is* $v \otimes w$?". I'm afraid there's not a terribly good answer for that. It is what it is: the image of $\langle v, w\rangle \in V \times W$ under the canonical bilinear map $V \times W \to V \otimes_S W$. As that's probably not very satisfying, I ask you to consider the following.

What if I asked you "But what actually *is* $\sqrt{2} \cdot \pi$?". The answer is that it is what it is: it's the product of $\sqrt{2}$ and π. You can't really reduce it to something simpler without going so far out of your way so as to not be worth it. For example, what are you going to do? Try to argue that the number $\sqrt{2} \cdot \pi$ is π added to itself $\sqrt{2}$ times? Good luck with that.

Anyways, I'm sure you probably don't feel very uncomfortable talking about "$\sqrt{2} \cdot \pi$", and my claim is that if you feel comfortable working with this, then you should feel comfortable working with $v \otimes w$.

That said, in special cases, one can be a bit more explicit—see the blue box in the remark of Definition 5.4.1.1. I personally don't find this perspective particularly useful, but I have found that some students to.

R Thus you can take the tensor product of an R-S-bimodule and an S-T-bimodule, the result being an R-T-bimodule. To remember this, you might note that this is exactly analogous to matrix multiplication: the 'inner' things have to be the same in which case the result has the structure coming from the 'outer' things.

This was one motivation for working with bimodules.[a] If I were working just with vector spaces, then you could take the tensor product of any two things you like, but in this context, you can only take the tensor product of an R×S-bimodule and an S-T-bimodule with the result being an R-T-bimodule—this makes it clearer what roles everything is playing.

R *This is important—do not ignore.* Essentially what this result says is that, instead of working with *bilinear* maps $V \times W \to U$, instead, we can work with *linear*

maps $V \otimes_S W \to U$. You'll find in time that this 'trade-off' is worth it.

In practice, this is often used in the following way. Suppose you want to define a function $T\colon V \otimes_S W \to U$. The definition of the tensor product says that *you only need to say where elements of the form $v \otimes w$ map to*. In practice, you will say something like "Let $T(v \otimes w) :=$ blah blah blah. . . ", and while superficially it doesn't look like you're defining T on all of $V \otimes_S W$ (because you're not), this is enough. As long as your "blah blah blah" is bilinear in $\langle v, w\rangle \in V \times W$, the definition of the tensor product says that this corresponds to a unique linear map $V \otimes_S W \to U$. This idea is similar to that Theorem 2.2.25, where you can define linear-transformations by only defining what it does to a basis. Similarly here, you can define a linear-transformation on all of $V \otimes_S W$ by only specifying what happens to elements of the form $v \otimes w$.

TL;DR:

> To define linear maps $V \otimes_S W \to U$, it suffices to say where elements of the form $v \otimes w \in V \otimes_S W$ get mapped to. As long as what you write down is bilinear in $\langle v, w\rangle$, the definition of the tensor product says that this serves to define a unique linear map on all of $V \otimes_S W$.

[a] The other big motivation is that you will need to learn tensor products in this level of generality at some point in your mathematical life, so may as well learn it now.

Proof. We leave this as an exercise.

Exercise 5.3.1.5 Prove the result.

■

This result says that if I every have a bilinear map $V \times W \to U$, I can 'replace' it with a linear map $V \otimes_S W \to U$. In this sense, the tensor product reduces the study of multilinear maps to linear maps.

There are a couple ways to think about $V \otimes_S W$ itself more intuitively. First of all, note that $- \otimes - \colon V \times W \to V \otimes_S W$ satisfying the following properties.

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2 \tag{5.3.1.6a}$$
$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w \tag{5.3.1.6b}$$
$$(\alpha \cdot v) \otimes w = \alpha \cdot (v \otimes w) \tag{5.3.1.6c}$$
$$v \otimes (w \cdot \alpha) = (v \otimes w) \cdot \alpha \tag{5.3.1.6d}$$
$$(v \cdot \alpha) \otimes w = v \otimes (\alpha \cdot w) \tag{5.3.1.6e}$$

Furthermore, $V \otimes_S W$ is the "freest" R-T-bimodule that satisfies these identities, that is, $- \otimes -$ satisfies only the above identities and those they imply. Thus, it is safe to think of $V \otimes_S W$ as the R-T-bimodule spanned by elements of the form $v \otimes w$, $v \in V$ and $w \in W$, with the only rules for 'simplification' given above. Note in particular, however, that there will most certainly be other elements in $V \otimes_S W$ besides just elements of the form $v \otimes w$. For example, $v_1 \oplus w_1 + v_2 \oplus w_2$ in general cannot be written as $v \otimes w$.

Another way of thinking about $V \otimes W$ that might help your intuition is in terms of bases. Though this is only true for vector spaces,[8] it essentially says the following: if you have a bunch of b_ks that are a basis for V and a bunch of c_ls that are a basis for W, then the collection of all $b_k \otimes c_l$s forms a basis for $V \otimes W$. Thus, the elements of $V \otimes W$ are precisely those things that can be written (uniquely) as a linear combinations of $b_k \otimes c_l$s.

Proposition 5.3.1.7 — Basis for $V \otimes W$ Let V and W be vector spaces over a field $\mathbb{F}$, and let $\mathcal{B}$ and C be bases for V and W respectively. Then,

$$\{b \otimes c : b \in \mathcal{B}, c \in C\} \tag{5.3.1.8}$$

is a basis for $V \otimes W$.

[8] Duh. We don't have bases for general modules.

R In particular, $\dim(V \otimes W) = \dim(V)\dim(W)$.

R We see immediately from working in the level of generality that we did that the ground division ring need be commutative, that is, a field. If it weren't, then V would be just an $\mathbb{F}$-$\mathbb{Z}$-bimodule and W would be a $\mathbb{F}$-$\mathbb{Z}$-bimodule, in which case we could not take their tensor product!

R This result can probably be generalized to the noncommutative case, but then we will need to take V to be a $\mathbb{K}_1$-$\mathbb{L}$-bimodule and W to be an $\mathbb{L}$-$\mathbb{K}_2$-bimodule, with $\mathbb{K}_1$ and $\mathbb{K}_2$ division rings. Furthermore, the statement would require us to have a notion of "basis" for bimodules. It's easy enough to write one down, but as we have not done so, we refrain from 'officially' giving this noncommutative version.

Proof. We leave this as an exercise.

Exercise 5.3.1.9 Prove the result.

■

Corollary 5.3.1.10 Let V and W be vector spaces over a field, and let $v \in V$ and $w \in W$. Then, if $v \otimes w = 0$, then $v = 0$ or $w = 0$.

R Warning: This may fail for general $\mathbb{K}$-modules—see Example 5.3.1.12.

R Just as the previous result should generalize to the noncommutative case, so to should this one.

Proof. We leave this as an exercise.

Exercise 5.3.1.11 Prove the result.

■

Not only can this corollary fail in general for modules, but something quite bit worse can happen.

▪ **Example 5.3.1.12 — $V \otimes W = 0$ with $V, W \neq 0$** Define $\mathbb{K} := \mathbb{Z}$, $V := \mathbb{Q}$, and $W := \mathbb{Z}/2\mathbb{Z}$. Then, for $v \otimes w \in V \otimes_{\mathbb{Z}} W$, we have

$$v \otimes w = \left(v\tfrac{1}{2}\right) \otimes (2w) = \left(v\tfrac{1}{2}\right) \otimes 0 = 0, \qquad (5.3.1.13)$$

and hence $V \otimes_{\mathbb{Z}} W = 0$.

Students tend to find the tensor product (and tensors in general) quite confusing. I get it. This definition, the first time you see it, is difficult to understand. My advice is to go on, even if you don't quite understand everything, and to not stress about it for now. What is more important the first time around is whether or not you can actually *work with* tensors. For example, I'm sure virtually everyone reading this learned how to compute integrals quite awhile before they were actually able to define the integral. In a similar way, to do more 'computational' things with tensors, you don't really need to have a complete understanding of the definition of the tensor product.[9] And pedagogically anyways, it does make sense to teach things in that order: you're going to have much more intuition for things (which is essential for coming up with proofs) if you've previously had hands-on concrete experience with it.

So, don't worry for the time being. Move on, and work out some "hands-on concrete" problems with tensors.[10] After you're more comfortable working with tensors, you can come back again to this definition to deepen your understanding.[11]

[9] Though, to be sure, if you want to *prove* things, you're likely going to need to understand the definition.

[10] For example, see Exercises 5.4.3.14 and 5.4.3.16.

[11] And maybe then, if things still don't make sense, you can begin to worry.

5.3.2 Tensor products of linear-transformations

When studying dual-spaces, we first defined $V^\dagger$, and subsequently defined $T^\dagger$, finding later that (Proposition 5.2.2.12) the common notation was justified as this defined a cofunctor (Definition B.3.1.10). We have now defined what it means to take the tensor product of spaces, and so it is natural to wonder whether there is a notion of tensor product of linear-transformations. Of course, there is.

Theorem 5.3.2.1 — Tensor product (of linear-transformations). Let V_1, W_1, V_2, and W_2 be $\mathbb{K}$-$\mathbb{K}$-bimodules, and let $S\colon V_1 \to W_1$ and $T\colon V_2 \to W_2$ be linear. Then, there is a unique linear-transformation $S \otimes T\colon V_1 \otimes V_2 \to W_1 \otimes W_2$, the ***tensor product (of linear-transformations)***, such that

$$[S \otimes T](v_1 \otimes v_2) = S(v_1) \otimes T(v_2). \tag{5.3.2.2}$$

R In particular, given $T\colon V \to V$ linear, we obtain maps

$$\bigotimes^k T\colon \bigotimes^k V \to \bigotimes^k V \tag{5.3.2.3}$$

for all $k \in \mathbb{N}$.

Proof. $V_1 \times V_2 \ni \langle v_1, v_2\rangle \mapsto S(v_1) \otimes T(v_2)$ is bilinear, and so by the definition of the tensor product (Theorem 5.3.1.1), there is a unique linear map $S \otimes T\colon V_1 \otimes V_2 \to W_1 \otimes W_2$ such that $[S \otimes T](v_1 \otimes v_2) = S(v_1) \otimes T(v_2)$. ∎

Theorem 5.3.2.4 — $- \otimes -$ is a functor. Let $S_1\colon V_1 \to V_2$, $S_2\colon V_2 \to V_3$, $T_1\colon W_1 \to W_2$, and $T_2\colon W_2 \to W_3$ be linear-transformations of $\mathbb{K}$-$\mathbb{K}$-bimodules. Then,

$$[S_2 \circ S_1] \otimes [T_2 \circ T_1] = [S_2 \otimes T_2] \circ [S_1 \otimes T_1] \tag{5.3.2.5}$$

as linear-transformations $V_1 \otimes_{\mathbb{K}} W_1 \to V_3 \otimes_{\mathbb{K}} W_3$.

R Of course, it is also true that $\mathrm{id}_V \otimes \mathrm{id}_W = \mathrm{id}_{V\otimes W}$.

Proof. We leave this as an exercise.

Exercise 5.3.2.6 We leave this as an exercise.

■

There is actually a slight notational ambiguity here—this notation conflicts with

$$S \otimes T \in \mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2 \otimes W_2). \tag{5.3.2.7}$$

We will see how to resolve this in Theorem 5.3.4.15.

5.3.3 Basic properties

We continue with an enumeration of some basic properties of the tensor product.

Proposition 5.3.3.1 Let R, S, and T be rings, let V be an R-S-bimodule and let W be an S-T-bimodule. Then,

$$V \otimes_S W = \mathrm{Span}\left\{v \otimes w : v \in V, w \in W\right\}. \tag{5.3.3.2}$$

Proof. We leave this as an exercise.

Exercise 5.3.3.3 Prove the result.

■

Proposition 5.3.3.4

(i). Let Q, R, S, and T be rings, let U be a Q-R-bimodule, let V be an R-S-bimodule, and let W be an S-T-bimodule. Then,

$$(U \otimes_R V) \otimes_S W \cong U \otimes_R V \otimes_S W \cong U \otimes_R (V \otimes_S W)$$

via the unique maps that has the property $(u \otimes v) \otimes w \mapsto u \otimes v \otimes w$ and $u \otimes v \otimes w \mapsto u \otimes (v \otimes w)$ respectively.

(ii). Let $\mathbb{K}$ is a cring, and let V and W be $\mathbb{K}$-modules. Then,

$$V \otimes_{\mathbb{K}} W \cong W \otimes_{\mathbb{K}} V \tag{5.3.3.5}$$

via the unique map that has the property $v \otimes w \mapsto w \otimes v$.

(iii). Let R, S, and T be rings, and let V be an R-S-bimodule and let W be an S-T-module. Then,

(a). if $W = \bigoplus_{U \in \mathscr{U}} U$, then

$$V \otimes_S \left(\bigoplus_{U \in \mathscr{U}} U \right) \cong \bigoplus_{U \in \mathscr{U}} (V \otimes_S U) \tag{5.3.3.6}$$

via the unique map that has the property $v \otimes w \mapsto \sum_{U \in \mathscr{U}} v \otimes \mathrm{proj}_U(w)$; and

(b). if $V = \bigoplus_{U \in \mathscr{U}} U$, then

$$\left(\bigoplus_{U \in \mathscr{U}} U \right) \otimes_S W \cong \bigoplus_{U \in \mathscr{U}} (U \otimes_S W) \tag{5.3.3.7}$$

via the unique map that has the property $v \otimes w \mapsto \sum_{U \in \mathscr{U}} \mathrm{proj}_U(v) \otimes w$.

R That is, (i) the tensor product is associative, (ii) commutative over commutative rings, and (iii) distributes over a direct sums.

Proof. We leave this as an exercise.

Exercise 5.3.3.8 Prove the result.

■

Proposition 5.3.3.9 Let R, S, and T be rings, let V be an R-S-bimodule and let W be an S-T-bimodule.

(i). $V \cong V \otimes_S S$ naturally via the map $v \mapsto v \otimes 1$.
(ii). $W \cong S \otimes_S W$ naturally via the map $w \mapsto 1 \otimes w$.
(iii). $V \otimes_S 0 \cong 0 \cong 0 \otimes_S W$.
(iv). $0 \otimes w = 0 = v \otimes 0 \in V \otimes_S W$ for all $v \in V$ and $w \in W$.

R Recall that (see the remark in the definition of the tensor product Theorem 5.3.1.1) that

$$\underbrace{V \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} V}_{0} := \mathbb{K}. \tag{5.3.3.10}$$

This definition is motivated by (i) and (ii), which state that the tensor product by $\mathbb{K}$ acts as the 'identity', and so we define the empty tensor product to be $\mathbb{K}$ for the same reason we define the empty product in, say, a ring, to be the multiplicative identity (Definition A.4.16).

Proof. We leave this as an exercise.

Exercise 5.3.3.11 Prove the result.

■

▪ **Example 5.3.3.12 — 'Injective on pure tensors' but not injective** We give an example of a linear-transformation $T\colon U \otimes V \to W$ such that $T(u \otimes v) = 0$ implies $u \otimes v = 0$ but yet is not injective.

Define $V := \mathbb{C}[x, y]/(x^2, xy, y^2)$ and define $T\colon V \otimes_{\mathbb{C}} V \to \mathbb{C}$ to be the unique linear map that sends $1 \otimes 1$, $1 \otimes x_2$, $1 \otimes y_2$, $x_1 \otimes 1$, $x_1 \otimes x_2$, $x_1 \otimes y_2$, $y_1 \otimes 1$, $y_1 \otimes x_2$, and $y_1 \otimes y_2$ all to 1.

Exercise 5.3.3.13 Determine if this example satisfies the property I claim it does, and if it does not, find an example that is actually correct.

5.3.4 Natural-isomorphisms

What follows is one of the most important properties of the tensor product.

Theorem 5.3.4.1 — Tensor-Hom Adjunction. Let R, S, and T be rings, and let U be an R-S bimodule, V and S-T bimodule, and W an R-T bimodule.

(i). The map

$$\begin{aligned}&\mathrm{Mor}_{R\text{-}\mathbf{Mod}\text{-}T}(U \otimes_S V, W) \leftarrow \\ &\quad \mathrm{Mor}_{S\text{-}\mathbf{Mod}\text{-}T}(V, \mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, W))\end{aligned} \tag{5.3.4.2}$$

defined by

$$(u \otimes v \mapsto [\phi(v)](u)) \leftarrow\!\shortmid \phi \tag{5.3.4.3}$$

is an isomorphism of commutative groups.

(ii). The map

$$\begin{aligned}&\mathrm{Mor}_{R\text{-}\mathbf{Mod}\text{-}T}(U \otimes_S V, W) \leftarrow \\ &\quad \mathrm{Mor}_{R\text{-}\mathbf{Mod}\text{-}S}(U, \mathrm{Mor}_{\mathbf{Mod}\text{-}T}(V, W))\end{aligned} \tag{5.3.4.4}$$

defined by

$$(u \otimes v \mapsto [\phi(u)](v)) \leftarrow\!\shortmid \phi \tag{5.3.4.5}$$

is an isomorphism of commutative groups.

R The R, S, and Ts everywhere clutter things up. Dropping all of the notational baggage, these become the more readable

$$\mathrm{Mor}(U \otimes V, W) \cong \mathrm{Mor}(V, \mathrm{Mor}(U, W))$$
$$\mathrm{Mor}(U \otimes V, W) \cong \mathrm{Mor}(U, \mathrm{Mor}(V, W)).$$

R To understand this, it might first help to understand an analogous result in a different category: the map defined analogously as above yields an isomorphism

$$\mathrm{Mor}_{\mathbf{Set}}(X \times Y, Z) \to \mathrm{Mor}_{\mathbf{Set}}(X, \mathrm{Mor}_{\mathbf{Set}}(Y, Z)).$$

In other words, functions from $X \times Y$ into Z are 'the same as' functions from X into $\mathrm{Mor}_{\mathbf{Set}}(Y, Z)$; given a function of two variables, we can instead think of it as a function-valued function $f \mapsto (x \mapsto (y \mapsto f(x, y)))$. In computer science, this concept is called *currying*. Thus, you could say that this result is just the linear algebraic analogue of currying.

R The "Hom" in "Tensor-Hom Adjunction" comes from the fact that "Mor" is often written as "Hom".

R Though you (probably) don't know what the term means yet, it turns out that this (by which I mean (i)) actually yields what is called an adjunction[a] between the functors $U \otimes_S - \colon S\text{-}\mathbf{Mod}\text{-}T \to R\text{-}\mathbf{Mod}\text{-}T$ and $\mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, -) \colon R\text{-}\mathbf{Mod}\text{-}T \to S\text{-}\mathbf{Mod}\text{-}T$, hence "Tensor-Hom Adjunction". In this case, we say that $U \otimes_S -$ is *left adjoint* to $\mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, -)$, and the other way around, that $\mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, -)$ is *right adjoint* to $U \otimes_S -$. Thus, as the tensor product is the *left* adjoint and the "Hom" is the *right* adjoint, I recommend you say "tensor-hom adjunction" and *not* "hom-tensor adjunction".

Dually, (ii) yields an adjunction between the functors $- \otimes_S V$ and $\mathrm{Mor}_{\mathbf{Mod}\text{-}T}(V, -)$.

[a] This means that not only is (5.3.4.3) an isomorphism, but it defines an isomorphism that is natural (Definition B.3.2.3) in both V and W.

Proof. We prove (i). The proof of (ii) is essentially identical.

Given $f \colon U \otimes_S V \to W$ a map of R-T-bimodules, define $g_f \colon V \to \mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, W)$ by

$$[g_f(v)](u) \coloneqq f(u \otimes v). \tag{5.3.4.6}$$

First of all, note that $g_f(v) \in \mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, W)$ as f is linear and the tensor product is bilinear.

To show that $g_f \colon V \to \mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, W)$ is a map of S-T-bimodules, we must show that

$$[g_f(s \cdot v \cdot t)](u) = [s \cdot [g_f(v)] \cdot t](u) \tag{5.3.4.7}$$

for all $u \in U$. However, recall from Example 1.1.1.17 that the S-T-bimodule action on $\mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, W)$ is given by

$$[s \cdot T \cdot t](u) \coloneqq T(u \cdot s) \cdot t, \tag{5.3.4.8}$$

and hence what we would actually like to show is that

$$[g_f(s \cdot v \cdot t)](u) = [g_f(v)](u \cdot s) \cdot t. \tag{5.3.4.9}$$

From the definition of g_f, this means we would like to show that

$$f(u \otimes (s \cdot v \cdot t)) = f((u \cdot s) \otimes v) \cdot t. \tag{5.3.4.10}$$

This is of course true because f is linear and because of properties of the tensor product ((5.3.1.6e)).

Finally, to check that $f \mapsto g_f$ is a group homomorphism

$$\mathrm{Mor}_{R\text{-}\mathbf{Mod}\text{-}T}(U \otimes_S V, W) \to \mathrm{Mor}_{S\text{-}\mathbf{Mod}\text{-}T}(V, \mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, W)),$$

we must show that $g_{f_1+f_2} = g_{f_1} + g_{f_2}$. In other words, we must show that

$$\begin{aligned}[f_1 + f_2](u \otimes v) &= [g_{f_1+f_2}(v)](u) \\ &= [[g_{f_1} + g_{f_2}](v)](u) \\ &= f_1(u \otimes v) + f_2(u \otimes v)\end{aligned} \tag{5.3.4.11}$$

for all $u \in U$ and $v \in U$. This is of course true because of the definition of addition of functions.

To show that $f \mapsto g_f$ is an isomorphism, we construct an inverse $g \mapsto f_g$ from $\mathrm{Mor}_{S\text{-}\mathbf{Mod}\text{-}T}(V, \mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, W))$ to $\mathrm{Mor}_{R\text{-}\mathbf{Mod}\text{-}T}(U \otimes_S V, W)$. So, let $g : V \to \mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, W)$ be a map of S-T-bimodules and define $f_g : \mathrm{Mor}_{R\text{-}\mathbf{Mod}\text{-}T}(U \otimes_S V, W)$ by

$$f_g(u \otimes v) \coloneqq [g(v)](u). \tag{5.3.4.12}$$

As this is bilinear in u and v, this serves to define a map of S-T-bimodules $U \otimes_S V \to W$—see the last remark in the

definition of the tensor product (Theorem 5.3.1.1). As the check that $g \mapsto f_g$ is a group homomorphism is similar to before, we omit it (it comes down to the definition of addition of functions).

It remains to check that $f \mapsto g_f$ and $g \mapsto f_g$ are inverse to each other. To do that, we must show that $g_{f_g} = g$ and $f_{g_f} = f$. For the first one, note that

$$[[g_{f_g}](v)](u) \coloneqq f_g(u \otimes v) \coloneqq [g(v)](u). \tag{5.3.4.13}$$

As this holds for all $u \in U$ and $v \in V$, we have $g_{f_g} = g$. For the other one, note that

$$[f_{g_f}](u \otimes v) \coloneqq [g_f(v)](u) \coloneqq f(u \otimes v), \tag{5.3.4.14}$$

and again we have that $f_{g_f} = f$, as desired. ∎

What follows are a couple of results similar in flavor to the tensor-hom adjunction. While the tensor-hom adjunction is probably more important in mathematics in general, for us, the following three results will be more important, and you should take note of them, especially the case of finite-dimensional vector spaces.

Theorem 5.3.4.15 — $\mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2) \cong \mathrm{Mor}(V_1 \otimes V_2, W_1 \otimes W_2)$. Let V_1, W_1, V_2, and W_2 be $\mathbb{K}$-$\mathbb{K}$-bimodules. Then, the map

$$\mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2) \to \mathrm{Mor}(V_1 \otimes V_2, W_1 \otimes W_2)$$

defined by

$$S \otimes T \mapsto (v_1 \otimes v_2 \mapsto S(v_1) \otimes T(v_2)) \tag{5.3.4.16}$$

is linear and natural.

Furthermore,

(i). if V_1, W_1, V_2, and W_2 are vector spaces, then this map is injective; and

(ii). if V_1, W_1, V_2, and W_2 are finite-dimensional vector spaces, then this map is an isomorphism.

R We will abuse notation write write $S \otimes T$ for both the element in the tensor product $\mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2)$ and the linear-transformation it defines $V_1 \otimes V_2 \to W_1 \otimes W_2$. Of course, this result says that this isn't even really an abuse of notation if everything involved is a vector space, but even if they weren't, this abuse should not cause any confusion.

R Warning: This need not be an isomorphism even for vector spaces if they are not finite-dimensional—see Example 5.3.4.27.

Proof. As this is bilinear in S and T, it defines a linear-transformation on the tensor product.

To show naturality, let $f : U_1 \to V_1$ be a linear-transformation. By definition (Definition B.3.2.3), this will be natural in the first space iff the following diagram commutes.

$$\begin{array}{ccc} \mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2) & \longrightarrow & \mathrm{Mor}(V_1 \otimes V_2, W_1 \otimes W_2) \\ \downarrow & & \downarrow \\ \mathrm{Mor}(U_1, W_1) \otimes \mathrm{Mor}(V_2, W_2) & \longrightarrow & \mathrm{Mor}(U_1 \otimes V_2, W_1 \otimes W_2) \end{array}$$

By definition, this commutes iff

$$S(f(u_1)) \otimes T(v_2) = S(f(u_1)) \otimes T(v_2), \tag{5.3.4.17}$$

which if tautologically true.[a] By $V_1 \leftrightarrow V_2$ symmetry, it is natural in V_2 as well. A similar check shows that it is natural in W_1, and hence W_2 as well.

(i) Suppose that V_1, W_1, V_2, and W_2 are vector spaces. Let $\sum_{k=1}^{m} \sum_{l=1}^{n} S_k \otimes T_l$ be an arbitrary nonzero element of $\mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2)$. Without loss of generality, let $m, n \in \mathbb{Z}^+$ be the smallest such positive integers. [b]

Now suppose that this element of $\mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2)$ is sent to 0. In other words,

$$\sum_{k=1}^{m} \sum_{l=1}^{n} S_k(v_1) \otimes T_l(v_2) = 0 \tag{5.3.4.18}$$

for all $v_1 \in V_1$ and $v_2 \in V_2$. Writing this as

$$\left(\sum_{k=1}^{m} S_k(v_1) \right) \left(\sum_{l=1}^{n} T_l(v_2) \right) = 0, \tag{5.3.4.19}$$

using Corollary 5.3.1.10, we deduce that either $\sum_{k=1}^{m} S_k(v_1) = 0$ or $\sum_{l=1}^{n} T_l = 0$. In the the former case, we can replace S_m in $\sum_{k=1}^{m} \sum_{l=1}^{n} S_k \otimes T_l$ with $-\sum_{k=1}^{n-1} S_k$, thereby writing this element with only $n-1$ w_ls: a contradiction. The latter case is identical. Thus, it cannot be the case that a nonzero element of $\mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2)$ is sent to 0, and this map is injective.

(ii) Suppose that V_1, W_1, V_2, and W_2 are finite-dimensional vector spaces. $\mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2)$ and $\mathrm{Mor}(V_1 \otimes V_2, W_1 \otimes W_2)$ have the same dimension, namely $\dim(V_1)\dim(W_1)\dim(V_2)\dim(W_2)$, and hence the injective map $\mathrm{Mor}(V_1, W_1) \otimes \mathrm{Mor}(V_2, W_2) \to \mathrm{Mor}(V_1 \otimes V_2, W_1 \otimes W_2)$ must in fact be an isomorphism (Corollary 2.2.2.14). ■

[a] Going right then down essentially gives $S(v_1) \otimes T(v_2)$ and then replaces v_1 with $f(u_1)$. Going down then right replaces v_1 with $f(u_1)$ and then takes $S(f(u_1)) \otimes T(u_1)$.

[b] So, for example, if you can simplify $S_1 \otimes T_1 + S_2 \otimes T_2$ to something of the form $S \otimes T$, do that, and take $m = 1 = n$ instead of $m = 2 = n2$.

Corollary 5.3.4.20 — $V^\dagger \otimes W \cong \mathrm{Mor}(V, W)$ Let V and W be $\mathbb{K}$-$\mathbb{K}$-bimodules. Then, the map

$$V^\dagger \otimes_{\mathbb{K}} W \ni \phi \otimes w \mapsto (v \mapsto \phi(v)w) \in \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$$

is linear and natural.

Furthermore,

(i). if V and W are vector spaces, this map is injective; and
(ii). if V and W are finite-dimensional vector spaces, this map is an isomorphism.

R In particular, for finite-dimensional vector spaces, using language that we will learn shortly (Definition 5.4.1.1), $\langle 1, 1\rangle$ tensors are 'the same as' linear-transformations.[a]

R Warning: This need not be an isomorphism even for vector spaces if they are not finite-dimensional—see Example 5.3.4.27.

R You've likely seen map before, albeit in a special case. To elaborate on this in the most insightful manner, we wait until we have index notation, and so postpone this to Example 5.4.2.28.

[a] We technically don't define "tensor" unless $W = V$, but that doesn't really affect what's going on here—this is just a matter of language.

Proof. Take $W_1 = \mathbb{K}$, $V_2 = \mathbb{K}$, $V_1 = V$, and $W_2 = W$ in the previous result (Theorem 5.3.4.15). Using the fact that $W \cong \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(\mathbb{K}, W)$ (Proposition 5.2.1.24), $V \cong V \otimes_{\mathbb{K}} \mathbb{K}$, and $W \cong \mathbb{K} \otimes_{\mathbb{K}} W$ naturally, Theorem 5.3.4.15 reduces to exactly the statement of this corollary. ∎

Corollary 5.3.4.21 — $\mathrm{Mor}(U \otimes V, W) \cong \mathrm{Mor}(U, V^\dagger \otimes W)$ Let U, V, and W be $\mathbb{K}$-$\mathbb{K}$-bimodules. Then, the map

$$\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(U, V^\dagger \otimes_{\mathbb{K}} W) \to \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(U \otimes V, W),$$

given by the composition of the maps

$$\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(U, V^\dagger \otimes_{\mathbb{K}} W) \to \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(U, \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W))$$

and

$$\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(U, \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)) \to \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(U \otimes V, W),$$

is linear and natural.

Furthermore,

(i). if V and W are vector spaces, this map is injective; and
(ii). if V and W are finite-dimensional vector space, this map is an isomorphism.

Proof. This map is a composition of the map from the previous corollary and the Tensor-Hom Adjunction (Theorem 5.3.4.1), and so this corollary follows immediately from those two results. ■

Corollary 5.3.4.23 — $V^\dagger \otimes W^\dagger \cong (W \otimes W)^\dagger$ Let V and W be $\mathbb{K}$-$\mathbb{K}$-bimodules. Then, the map

$$V^\dagger \otimes W^\dagger \ni \phi \otimes \chi \mapsto (v \otimes w \mapsto \phi(v)\chi(w)) \in (V \otimes W)^\dagger$$

is linear and natural.

Furthermore,

(i). if V and W are vector spaces, this map is injective; and
(ii). if V and W are finite-dimensional vector spaces, this map is an isomorphism.

Warning: This need not be an isomorphism even for vector spaces if they are not finite-dimensional—see Exercise 5.3.4.31.

Proof. Take $W = W^\dagger$ in Corollary 5.3.4.20. We thus obtain a natural linear map

$$V^\dagger \otimes_{\mathbb{K}} W^\dagger \to \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W^\dagger). \tag{5.3.4.24}$$

However, by the Tensor-Hom Adjunction (Theorem 5.3.4.1), we have a natural isomorphism

$$\begin{aligned}&\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W^\dagger)\\ &\quad := \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(W, \mathbb{K}))\\ &\quad \cong \mathrm{Mor}_{\text{-}\mathbf{Mod}\mathbb{K}}(V \otimes_{\mathbb{K}} W, \mathbb{K})\\ &\quad =: [V \otimes_{\mathbb{K}} W]^\dagger.\end{aligned} \tag{5.3.4.25}$$

Putting these together, we obtain a natural linear map $V^\dagger \otimes_{\mathbb{K}} W^\dagger \to [V \otimes_{\mathbb{K}} W]^\dagger$, which is injective if W and W are vector spaces and an isomorphism if V and W are finite-dimensional vector spaces (by Corollary 5.3.4.20 again). ■

Exercise 5.3.4.26 Can you find $\mathbb{K}$-modules V and W, $\mathbb{K}$ a cring, for which $V^\dagger \otimes W \to \mathrm{Mor}(V, W)$ is not injective.

▪ **Example 5.3.4.27 — Vector space V such that $V^\dagger \otimes V \to \mathrm{Mor}_{\mathbf{Vect}}(V, V)$ is not an isomorphism** Define $V := \mathbb{C}^\infty$. As $\{e_k : k \in \mathbb{N}\}$ is a basis for V, every element in $V^\dagger \otimes V$ can be written as a finite linear combination of elements in the set

$$\{\phi \otimes e_k : \phi \in V^\dagger, k \in \mathbb{N}\}. \tag{5.3.4.28}$$

The linear-transformation that $\sum_{k=1}^m \alpha\phi_k e_k$ defines sends $v \in V$ to

$$\sum_{k=0}^{m} \alpha\phi_k(v)e_k \in \mathrm{Span}(\{e_k : 0 \le k \le m\}) \tag{5.3.4.29}$$

In particular, the image of any such element is finite-dimensional. On the other hand, the identity $V \to V$ has infinite-dimensional image, and so can't possibly be of this form. Thus, the map $V^\dagger \otimes V \to \mathrm{Mor}_{\mathbf{Vect}}(V, V)$ is not surjective.

Exercise 5.3.4.30 Can you find $\mathbb{K}$-modules V and W, $\mathbb{K}$ a cring, for which $V^\dagger \otimes W \to [V \otimes W]^\dagger$ is not injective.

Exercise 5.3.4.31 Find a vector space V for which the canonical map $V^\dagger \otimes V^\dagger \to [V \otimes V]^\dagger$ is not an isomorphism.

5.4 Tensors and index notation

Roughly speaking, a tensor rank $\langle k, l\rangle$ is going to be something that takes in l vectors and spits out k vectors[12] in a multilinear manner. For example, linear-transformations are $\langle 1, 1\rangle$ tensors, covectors are $\langle 0, 1\rangle$ tensors, vectors are $\langle 1, 0\rangle$ tensors, and scalars are $\langle 0, 0\rangle$ tensors: linear-transformations take in 1 vector and spit out 1 vector, covectors take in 1 vector and spits out a scalar[13], vectors take in 0 vectors and spit out 1 vector, and scalars take in 0 vectors and spit out 0 vectors. Similarly, a pairing on a dual-pair will be a tensor of type $\langle 0, 2\rangle$: it takes in two vectors and spits out a scalar.

5.4.1 Tensors and the tensor algebra

We make this precise as follows.

Definition 5.4.1.1 — Tensor Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule. Then, a ***tensor*** of ***rank*** $\langle k, l\rangle$ over V is an element of

$$\bigotimes_l^k V := \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(\underbrace{V \otimes \cdots \otimes V}_{l}, \underbrace{V \otimes \cdots \otimes V}_{k}). \quad (5.4.1.2)$$

R k is the ***contravariant rank*** and l is the ***covariant rank***. If $l = 0$, then the tensor is ***contravariant***, and if $k = 0$, then the tensor is ***covariant***.

We write

$$\bigotimes^k V := \bigotimes_0^k V \quad (5.4.1.3)$$

[12] More accurately, a element of $V^{\otimes k}$.

[13] Which, for our purposes, is to be regarded as 'zero vectors'.

and

$$\bigotimes_l V := \bigotimes_l^0 V \tag{5.4.1.4}$$

respectively for the spaces of rank k contravariant tensors and rank l covariant tensors.

R Though uncommon, I have seen the term ***valence*** used synonymously with "rank" in this context.

R Instead of saying "T is a tensor of rank $\langle k.l\rangle$", we may use the less verbose "T is a $\langle k, l\rangle$ tensor".

R Thus, by the definition of the tensor product (Definition 5.4.1.1), a tensor of rank $\langle k, l\rangle$ is 'the same as' a multilinear map from $\underbrace{V \times \cdots \times V}_{l}$ to $\underbrace{V \otimes \cdots \otimes V}_{k}$.

Thus, a tensor of rank $\langle k, l\rangle$ is a thing that takes in l vectors and 'spits out' 'k vectors'[a] in a multilinear manner.

R If V is a finite-dimensional vector space, by virtue of Corollary 5.3.4.21, we have natural isomorphisms like, for example,

$$\begin{aligned}\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V \otimes V^\dagger \otimes V^\dagger, V \otimes V^\dagger) \cong \\ \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V \otimes V, V \otimes V \otimes V).\end{aligned} \tag{5.4.1.5}$$

Thus, it suffices to only look at elements of (5.4.1.2)—if a dual were to appear in that morphism set, we could always 'move it over' to the other side to get rid of the dual.

However, this does rely on the hypothesis that V is finite-dimensional, and in general one will need to look at maps, for example, $V \otimes V^\dagger \to V^\dagger$. I suppose we technically should have included this above in the 'official' definition, but this would really obfuscate what's going on. Just be aware that we may need to make this distinction if V is not a finite-dimensional vector space. For example, we work in this general case when introducing index notation (Notation 5.4.2.1).

R Using the same sort of isomorphisms referenced in the previous remark, for V a finite-dimensional vector space, there is a natural isomorphism

$$\bigotimes_l^k V := \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(\underbrace{V \otimes \cdots \otimes V}_{l}, \underbrace{V \otimes \cdots \otimes V}_{k})$$
$$\cong \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(\underbrace{V \otimes \cdots \otimes V}_{l} \otimes \underbrace{V^\dagger \otimes \cdots \otimes V^\dagger}_{k}, \mathbb{K}).$$

Thus, in regards to the question "But what actually *is* a tensor?", this says that, for V a finite-dimensional vector space anyways:

> A tensor of rank $\langle k, l\rangle$ is a multilinear map
>
> $$\underbrace{V \times \cdots \times V}_{l} \times \underbrace{V^\dagger \times \cdots \times V^\dagger}_{k} \to \mathbb{K}.$$

R Recall that (Theorem 5.3.1.1) the empty tensor product is defined to be $\mathbb{K}$. Thus, $\bigotimes_0^0 V \cong \mathbb{K}$, $\bigotimes_0^1 V \cong V$ (by Proposition 5.2.1.24), and $\bigotimes_1^0 V =: V^\dagger$.

R Note that the notation $\bigotimes_l^k V$ is nonstandard (though based on the standard notation $\Lambda^l V$ for something new which we will become acquainted with later on).

R If you still feel uncomfortable with this, you might consider taking a glance at Subsection 5.4.4. This subsection briefly explains the definition usually taken by physicists, and in particular reproduces (from another source) a precise version of this definition. I personally find this unenlightening, and it's technically not exactly the same thing as what we discuss, but I have had at least some students find it useful.

[a] More accurately, a contravariant tensor of rank k.

Theorem 5.4.1.6. Let V be a finite-dimensional vector space over a field. Then, the canonical map

$$\underbrace{V \otimes \cdots \otimes V}_{k} \otimes \underbrace{V^\dagger \otimes \cdots \otimes V^\dagger}_{l} \to \mathrm{Mor}_{\mathbf{Vect}}(\underbrace{V \otimes \cdots \otimes V}_{l}, \underbrace{V \otimes \cdots \otimes V}_{k}) \tag{5.4.1.7}$$

is a natural isomorphism.

R We write

$$V^{k\otimes,l\otimes\dagger} := V^{k\otimes} \otimes [V^\dagger]^{l\otimes} := \underbrace{V \otimes \cdots \otimes V}_{k} \otimes \underbrace{V^\dagger \otimes \cdots \otimes V^\dagger}_{l}. \tag{5.4.1.8}$$

Thus, in brief, we could say that $\bigotimes_l^k V$ and $V^{k\otimes,l\otimes\dagger}$ are naturally isomorphic (for V and W finite-dimensional vector spaces).

R We may, by abuse of language, refer to elements of $V^{k\otimes,l\otimes\dagger}$ as ***tensors***, even when this space isn't actually isomorphic, or even contained, in the space of 'actual' tensors $\bigotimes_l^k V$. Given $T \in V^{k\otimes,l\otimes\dagger}$, we can always consider it to be an 'actual' tensor if need be by considering its image in $\bigotimes_l^k V$ under the map appearing in the statement.

R Thus, in finite-dimensional vector spaces, $\langle k, l\rangle$ *tensors are the same as elements in the tensor product of V with itself k times and the tensor product of $V^\dagger$ with itself l times.*

Thus, in this context, we will not make a distinction between these two spaces, and both of them will be referred to as the "space of tensors of rank $\langle k, l\rangle$".

Proof. This follows from combining Corollary 5.3.4.20 and Corollary 5.3.4.23.[a] ■

[a] These respectively say in particular that $V^\dagger \otimes V \cong \mathrm{Mor}_{\mathbf{Vect}}(V,V)$ and that $V^\dagger \otimes V^\dagger \cong [V \otimes V]^\dagger$.

Theorem 5.4.1.9 — The tensor algebra. Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and define

$$\bigotimes_\bullet^\bullet V := \bigoplus_{k,l\in\mathbb{N}} \bigotimes_l^k V. \tag{5.4.1.10}$$

Then, $\bigotimes_\bullet^\bullet V$ is a $\mathbb{K}$-algebra with multiplication given by the tensor product.

R Elements of $\bigotimes_\bullet^\bullet V$ are ***tensors***.
Thus, for example, if S is a tensor of rank $\langle 2,3\rangle$ and T is a tensor of rank $\langle 4,1\rangle$, then $S+T$ now makes sense[a] and is considered a tensor (though it doesn't have a definite rank).

R $\bigotimes_\bullet^\bullet$ is the ***tensor algebra*** over V.

R If we ever have the need, then we shall write

$$\bigotimes^\bullet V := \bigoplus_{k\in\mathbb{N}} \bigotimes^k V \tag{5.4.1.11}$$

and

$$\bigotimes_\bullet V := \bigoplus_{l\in\mathbb{N}} \bigotimes_l V. \tag{5.4.1.12}$$

respectively for the subalgebras of contravariant and covariant tensors.

R If V is a finite-dimensional vector space, so that we have $V^{k\otimes,l\otimes\dagger} \cong \bigotimes_l^k V$, we may also write

$$V^{\otimes,\otimes\dagger} := \bigoplus_{k,l\in\mathbb{N}} V^{k\otimes,l\otimes\dagger} \cong \bigotimes_\bullet^\bullet V. \tag{5.4.1.13}$$

Similarly, in this case, we may also write

$$V^{\otimes} := \bigoplus_{k\in\mathbb{N}} V^{k\otimes} \cong \bigotimes^{\bullet} V \tag{5.4.1.14}$$

and

$$V^{\otimes\dagger} := \bigoplus_{l\in\mathbb{N}} V^{l\otimes\dagger} \cong \bigotimes_{\bullet} V. \tag{5.4.1.15}$$

R Warning: This notation is nonstandard. Usually people only look at the contravariant tensors, in which case the notation $T(V)$ is often used for the space of all contravariant tensors.

[a] Before introducing $\bigotimes_{\bullet}^{\bullet} V$ this notation would have been nonsense as you can't add things if they don't 'live in' the same module!

Proof. We leave this as an exercise.

Exercise 5.4.1.16 Prove the result.

■

Proposition 5.4.1.17 — Basis for $\bigotimes_{\bullet}^{\bullet} V$ Let V be a finite-dimensional vector space over a field, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ be a basis of V, denote the dual-basis by $\mathcal{B}^{\dagger} =: \{b^1, \ldots, b^d\}$, and let $k, l \in \mathbb{N}$. Then,

$$\bigotimes_l^k \mathcal{B} := \left\{ b_{i_1} \otimes \cdots \otimes b_{i_k} \otimes b^{j_1} \otimes \cdots \otimes b^{j_l} : 1 \leq i_1, \ldots, i_k, j_1, \ldots, j_n \leq d \right\} \tag{5.4.1.18}$$

is a basis for $\bigotimes_l^k V$.

R This says that all possible tensor products of k elements from $\mathcal{B}$ with all possible tensor products of l elements from $\mathcal{B}^{\dagger}$ is a basis for $\bigotimes_l^k V$. Putting

these all together for all $k, l \in \mathbb{N}$ then gives a basis for $\bigotimes_{\bullet}^{\bullet} V$.

R We require that V be a finite-dimensional vector space over a field here so that the "dual basis" is actually a basis—see Proposition 5.2.2.40.

R Note how the indices of the vectors in this case are written as *subscripts*. This is customary: if the *name* of a vector involves an index, then that index is written as a subscript; if the *name* of a covector involves an index, then that index is written as a superscript.

The reason for this is simply so that indices that are part of the name of the vector don't risk 'colliding' with indices used in the sense of index notation. For example, while we have not used index notation in this statement, we would have written

$$[b_i]^a \text{ and } [b^i]_a \tag{5.4.1.19}$$

respectively for elements in the basis and elements in the dual basis.

Another reason for doing this is to make equations like[a]

$$v = \sum_{k=1}^{d} v^k \cdot b_k \tag{5.4.1.20}$$

to adhere to the convention that identical pairs of indices, one upstairs and one downstairs, are to be summed over.

R Of course, it follows that the union of all these sets over $k, l \in \mathbb{N}$ then yields a basis for all of $\bigotimes_{\bullet}^{\bullet} V$ (by Proposition 4.4.1.44).

[a] This is the defining equation for the coordinates of v with respect to the basis $\mathcal{B}$.

Proof. We leave this as an exercise.

Exercise 5.4.1.21 Prove the result.

■

5.4.2 Index notation

The definition

Index notation is notation commonly used[14] when working with tensors. The basic idea is to "decorate" the name of the tensor with subscripts and superscripts that tell you the rank of the tensor. This is analogous to how one may write "$f(x, y, z)$" instead of just "f" to indicate that f is a function of three variables.

Notation 5.4.2.1 — Index notation Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and let

$$T \in \mathrm{Mor}\Big(\underbrace{V \otimes \cdots \otimes V}_{k_1} \otimes \underbrace{V^\dagger \otimes \cdots \otimes V^\dagger}_{k_2}, \underbrace{V \otimes \cdots \otimes V}_{l_1} \otimes \underbrace{V^\dagger \otimes \cdots \otimes V^\dagger}_{l_2}\Big) \tag{5.4.2.2}$$

be a tensor of rank $\langle\langle k_1, k_2\rangle, \langle l_1, l_2\rangle\rangle$. To indicate the rank of T, we shall write

$$\overset{a_1 \cdots a_{l_1}}{\underset{b_1 \cdots b_{l_2}}{T}}{}^{c_1 \cdots c_{k_2}}_{d_1 \cdots d_{k_1}}. \tag{5.4.2.3}$$

R *Important*: If V is a finite-dimensional vector space, then as explained in a remark of the definition of tensors (Definition 5.4.1.1), we may essentially move all copies of the dual space appearing in (5.4.2.2) to the "other side". This results in $k_1 \to k_1 + l_2$, $k_2 \to 0$, $l_1 \to l_1 + k_2$, and $l_2 \to 0$. In this case, it is

[14] At least by physicists.

customary to write all the indices to the right of T:

$$T^{a_1\cdots a_k}{}_{b_1\cdots b_l} \tag{5.4.2.4}$$

That said, even in this case, we may still sometimes write indices to the left of T if we feel that makes the intended meaning clearer.

The importance of this remark is a result of the fact that the vast majority of the time we will *not* be writing indices on the left.

If we are dealing with tensors over two distinct vector spaces, we will tend to use distinct scripts for the different vector spaces. For example, we will probably write something like $T^a{}_\alpha$ for an element of $V \otimes W^\dagger$ instead of $T^a{}_b$. We might also write capitals for one space, or perhaps start at different place in the same alphabet (e.g. α, β, γ, etc. for V vs. μ, ν, ρ, etc. for W).

This is called ***abstract index notation***, ***Penrose index notation***, or just ***index notation***. This is similar in form, but conceptually distinct, from *Einstein index notation*. In Einstein index notation, one has chosen a basis, and then the indices indicate the coordinates with respect to that basis. Note, however, that abstract index notation was designed so that one could do computations as if one was using Einstein index notation without actually picking a basis. Roughly speaking, abstract index notation is to Einstein index notation as linear-transformations are to matrices, though the distinction matters even less because the notation is designed to work so similarly. For this reason, the distinction is one that matters much more in theory than it does in practice.

Do not be sloppy by not staggering your indices! If you do, you will eventually make a mistake. For example, later we will be raising and lowering indices. Suppose I start with T^{ab}, I lower to obtain T^a_b, and then I raise again to obtain T^{ba}—I should obtain the same thing, but in general $T^{ab} \neq T^{ba}$, and so

I have made an error. It may seem obvious to the point of being silly when I point it out like this, but this is a mistake that is easy to make if there is a big long computation in between the raising and lowering (especially if it's more than just a and b floating around). And of course, you will never have this problem if you stagger: T^{ab} goes to $T^a{}_b$ goes back to T^{ab}.

R We emphasize that this is all "coordinate-free"—no need to pick bases—despite what the notation might superficially suggest.

Index notation tends to be confusing for students at first, but I claim that it is quite easy. First of all, a lot of the definitions that follow look exceedingly complicated because of all the indices and ellipses. Don't be intimidated—the only real complication here is the notation itself.[15]

As for some more concrete advice for understanding, as mentioned before, consider the notation $f(x)$ so often used for functions as roughly analogous to index notation for tensors. The function itself is technically just f, but people write "$f(x, y, z)$" all the time to denote the function. Similarly, while the tensor itself is just T, it is helpful to use indices to indicate the "variables" that T can take in, for example, $T^a{}_{bc}$.[16] The notation "$f(x, y, z)$" tells you that it takes in 3 "variables", whereas the notation "f" tells you nothing about this. Of course, this can be useful information which is often more convenient to indicate in this way than saying separately "f is a function of three variables". Similarly for $T^a{}_{bc}$.

There will be more more to say about the relationship between index notation and this analogous notation for functions, but we

[15]Index notation is admittedly pretty terrible when it comes to writing general statements, but when it comes to specific tensors (e.g. $T^{ab}{}_{cde}$), it's really quite manageable.

[16]Just a random example. Using a general tensor here would obfuscate the simplicity of what's going on, and in any case would be more directly analogous to something like $f(x_1, \ldots, x_m)$ than it would just $f(x, y, z)$.

postpone this discussion until having actually defined the relevant concepts.

Constructions in index notation

There are four key constructions involving tensors that we will need, the *transpose*, the *tensor product*, *contraction*, and the *dual-vector*.[17]

Notation 5.4.2.5 — The identity in index notation Let V be a $\mathbb{K}$-module. Then, we write

$$ {}^{a}[\mathrm{id}_V]_{b} =: {}^{a}\delta_{b}. \tag{5.4.2.6} $$

R The reason we use this notation is because of the *Kronecker delta symbol*. Strictly speaking, the ***Kronecker delta symbol*** is just the identity matrix, but it is given a separate name because of the notation used to denote it in practice:

$$ {}^{i}\delta_{j} := \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases} \tag{5.4.2.7} $$

(${}^{a}\delta_{b}$ is in abstract index notation, whereas ${}^{i}\delta_{j}$ as written here is in Einstein index notation. This is a good example of how the distinction doesn't matter that much in practice.)

The transpose we have already done in Definition 5.2.2.8, and so we simply explain how to write the transpose in index notation.

Notation 5.4.2.8 — Transpose in index notation Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and let $T : V \to V$ be linear. Then, the *transpose* of ${}^{a}T_{b}$ is denoted

$$ {}^{a}[T^{\dagger}]_{b} =: {}_{b}T^{a}. \tag{5.4.2.9} $$

[17] We briefly met the definition "dual-vector" back in Definition 5.2.2.2, but when the pairing in question is a metric (Definition 5.4.3.1), this concept takes on added importance.

R In case V is a finite-dimensional vector space, we also make use of a similar notation for higher rank tensors: If $T^{a_1\cdots a_k}{}_{b_1\cdots b_l}$ is a tensor of rank $\langle k, l\rangle$, then its transpose is similarly denoted

$$[T^\dagger]^{a_1\cdots a_k}{}_{b_1\cdots b_l} =: T_{b_1\cdots b_l}{}^{a_1\cdots a_k}.^a \quad (5.4.2.10)$$

We only use this notation for finite-dimensional vector spaces because otherwise the transpose would be, for example, a map

$$\mathrm{Mor}((W_1 \otimes W_2)^\dagger) \to \mathrm{Mor}((V_1 \otimes V_2)^\dagger), \quad (5.4.2.11)$$

whereas the index notation would imply that it is in fact a map

$$\mathrm{Mor}(W_1^\dagger \otimes W_2^\dagger) \to \mathrm{Mor}(V_1^\dagger \otimes V_2^\dagger). \quad (5.4.2.12)$$

These are of course the same if V is a finite-dimensional vector space by Corollary 5.3.4.23.

R In case we can get away with writing all the indices on the right, this same definition reads

$$[T^\dagger]^a{}_b := T_b{}^a. \quad (5.4.2.13)$$

R See (5.2.2.46)—this equation lists the coordinates of $T^\dagger$, and its relationship with the coordinates of T is superficially exactly as we have defined here.

[a] As V is a finite-dimensional vector space, we can get away with writing all the indices on the left—see the remark in Notation 5.4.2.1.

The tensor product we have already done in Theorem 5.3.1.1, and so we simply explain the how to write the tensor product in index notation.

Notation 5.4.2.14 — Tensor product in index notation
Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and let T_1 and T_2 respectively be

tensors over V of rank $\langle k_1, l_1\rangle$ and $\langle k_2, l_2\rangle$. The *tensor product* of $[T_1]^{a_1\dots a_{k_1}}{}_{b_1\dots b_{l_1}} \in \bigotimes_{l_1}^{k_1} V$ and $[T_2]^{a_1\dots a_{k_2}}{}_{b_1\dots b_{l_2}} \in \bigotimes_{l_2}^{k_2} V$ is denoted

$$[T_1 \otimes T_2]^{a_1\cdots a_{k_1} c_1\cdots c_{k_2}}{}_{b_1\cdots b_{l_1} d_1\cdots d_{l_2}} =: [T_1]^{a_1\dots a_{k_1}}{}_{b_1\dots b_{l_1}} [T_2]^{c_1\dots c_{k_2}}{}_{d_1\dots d_{l_2}}. \tag{5.4.2.15}$$

R To avoid obfuscating things even further, we omit the definition in case there are indices are the left, but it works exactly as one would expect—that is, as here, you literally just juxtapose them.

R In particular, if you ever see "⊗" used explicitly, this should be taken as an indication that we are *not* using index notation (and so subscripts and superscripts should not be interpreted as such).

R Note that *everything commutes with everything* in index notation.[a] For example,

$$T^a{}_b\, v^c = v^c T^a{}_b\,. \tag{5.4.2.16}$$

The letters keep track of what goes where—you don't need to use the order in which the symbols are written to do the same job.

[a] Assuming the ring you're working over is commutative of course. For example, it is common to use index notation in super-symmetry (and related subjects), in which case you have to be very careful about commuting things as you might have gotten use to. I once spent 8 hours looking for a minus sign to make everything in 40ish term expression cancel, and it turned out that I had accidentally commuted things without inserting a proper minus sign. Pro-tip: Don't do that.

We now turn to *contraction*.

Definition 5.4.2.17 — Contraction Let V be a $\mathbb{K}$-module, $\mathbb{K}$ a cring. Then, for $k, l \in \mathbb{N}$, and $1 \le i \le k$ and $1 \le j \le$

l, the $\langle i, j\rangle$ ***contraction*** of $\langle k, l\rangle$ tensors is the unique map $V^{k\otimes, l\otimes^\dagger} \to V^{(k-1)\otimes,(l-1)\otimes^\dagger}$ such that

$$\bigotimes_m v_m \otimes \bigotimes_n \phi_n \mapsto (\phi_j \mid v_i) \bigotimes_{m\neq i} v_m \otimes \bigotimes_{n\neq j} \phi_n. \quad (5.4.2.18)$$

R Warning: While this definition makes sense in general, we need V to be a finite-dimensional vector space over a field for $V^{k\otimes,l\otimes}$ be actually 'be' the space of $\langle k, l\rangle$ tensors—see Theorem 5.4.1.6.

R We need $\mathbb{K}$ to be commutative otherwise the defining equation (5.4.2.18) will not be multilinear, and hence not give a map on the tensor product.

R Consider $v\otimes\phi\otimes\psi \in V\otimes V^\dagger\otimes V^\dagger$. Its $\langle 1, 1\rangle$ contraction is then $\phi(v) \otimes \psi \in \mathbb{K} \otimes_{\mathbb{K}} V^\dagger$, and *not* $\phi(v)\psi$. This reason is because, if $\mathbb{K}$ is not commutative, then $\phi(v)\psi$ might not be a *linear*-functional anymore. This convention is justified by the fact that the tensor product of 0 spaces is just $\mathbb{K}$ itself—see the remark in Theorem 5.3.1.1.

R If this doesn't yet make sense, don't worry until you've read the upcoming Notation 5.4.2.19 and the remarks contained therein.

R If you want this to work for 'actual' tensors (instead of $V^{k\otimes,l\otimes^\dagger}$, the condition that V be finite-dimensional is fundamental—it is not just a matter of convenience. For example, we will see later that ${}^aT_a$ is the sum over the eigenvalues of T, which will be an infinite sum (and so will not make sense in general) if $\dim(V) = \infty$. On top of that, the definition is given for $V^{k\otimes,l\otimes^\dagger}$ which requires finite-dimensionality in order to be the 'same' as $\bigotimes_l^k V$—see Theorem 5.4.1.6.

Notation 5.4.2.19 — Contraction in index notation Let V be a $\mathbb{K}$-module, $\mathbb{K}$ a cring, let $k, l \in \mathbb{N}$, and $1 \leq i \leq k$ and $1 \leq j \leq l$. Then, the $\langle i, j \rangle$ *contraction* of the tensor $T^{a_1 \ldots a_k}{}_{b_1 \ldots b_l} \in V^{k\otimes, l\otimes\dagger}$ is denoted

$$T^{a_1 \ldots a_{i-1} c a_{i+1} \ldots a_k}{}_{b_1 \ldots b_{j-1} c b_{j+1} \ldots b_l} \tag{5.4.2.20}$$

R All these indices might make this seem unapproachable, but it's actually quite simple. Covectors take in vectors and spit out numbers, and so the contraction of a tensor product in its a_i and b_j index is formed by plugging in the i^{th} vector into the j^{th} covector, which is denoted by using the same letter for both the i^{th} index upstairs and the j^{th} index downstairs.

R Keep in mind that you can *only* contract upper-indices (contravariant) with lower (covariant) ones.

R Note that the letter you use for contraction doesn't matter—it just needs to be the same upstairs as it is downstairs and not conflict with other indices. This is analogous to the fact that

$$\int \mathrm{d}x\, f(x) = \int \mathrm{d}t\, f(t) : \tag{5.4.2.21}$$

it doesn't matter whether you use x or t, only that the letter in "d−" agree with the letter in "$f(-)$".

R Note that contraction of indices reduces both the contravariant and covariant rank by 1. For this reason, contracted indices are usually ignored when it comes to determine the type of the tensor. For example, people will say things like "The left-hand side of the following equation has only an a index upstairs.

$$T^{ab}{}_{b} = v^{a}\text{"}. \tag{5.4.2.22}$$

This is analogous to how $\int \mathrm{d}x\, f(x, y)$ is only a function of one variable.

R As contraction is so ubiquitous when working with index notation,[a] index notation is infrequently used outside the context of finite-dimensional vector spaces over fields. In infinite-dimensions can still be of limited use if you are careful to keep in mind that any contractions you might have written should *not* be interpreted using the definition, but rather, a dictionary (e.g. $\phi_a v^a$ corresponds to $\phi(v)$ and so on).

[a] For example, it appears even in expressions which don't actually require contraction to define (such a compositions of linear-transformations (Example 5.4.2.26)).

We mentioned some of the following examples before, but let's now do them 'officially'.

■ **Example 5.4.2.23**

(i). Vectors (written ${}^a v$ or v^a) themselves are tensors of type $\langle 1, 0\rangle$.

(ii). Covectors (or linear functionals) (written ω_a) are of type $\langle 0, 1\rangle$. For ω a linear functional and v a vector, $\omega(v)$ is written as $\omega_a {}^a v$.

(iii). The dot product (written temporarily as g_{ab}) is an example of a tensor of type $\langle 0, 2\rangle$—it takes in two vectors and spits out a number, written $v \cdot w = g_{ab} {}^a v {}^b w$ or $v\dot{w} = g_{ab} v^a w^b$.

(iv). Linear-transformations (written ${}^a T_b$ or $T^a{}_b$) are tensors of type $\langle 1, 1\rangle$—it takes in a single vector and spits out another vector (written ${}^a v \mapsto {}^a T_b {}^b v$ or $v^a \mapsto T^a{}_b v^b$).

R In accordance with the remark in Notation 5.4.2.1, as we are working over a finite-dimensional vector space, we are free to work with all indices on the right of the tensor. Here, however, in relevant cases, we use both notations (on the right and on the left) to illustrate the difference. Indeed, in some cases, I think having on the indices on the left makes things easier to read (e.g. in ${}^a T_b {}^b v$), though I don't know if

writing indices on the left is worth this small benefit when you can get away with not doing so.

My best guess is that, were one to get used to writing indices on the left, it wouldn't feel weird at all, but the reality is almost no one does this (because it's not necessary in the cases people use index notation), and as such, I personally find writing indices on the left a bit awkward, though I can't levy any strong objective objections to its use.

▪ **Example 5.4.2.24 — Linear-functionals in index notation** Let V be a $\mathbb{K}$-module, $\mathbb{K}$ a cring, let $v^a \in V$, and let $\phi_a \in V^\dagger$.

We can take their tensor product $v^a \phi_b$, which is a tensor of rank $\langle 1, 1\rangle$.

There is only one possible contraction of this tensor: $v^a \phi_a$, which is by definition equal to $(\phi \mid v) \coloneqq \phi(v)$. Compare what this would look like in coordinates: $\phi(v) = \sum_{k=1}^{d} v^k \phi_k$.

▪ **Example 5.4.2.25 — Linear-transformations in index notation** Let V and W be $\mathbb{K}$-modules, $\mathbb{K}$ a cring, let $T^\alpha{}_a \in V^\dagger \otimes W$,[a], and let $v^a \in V$.

We can take their tensor product $T^A{}_a\, v^b$, which is a tensor of rank $\langle 2, 1\rangle$.[b] There is only one possible contraction of this tensor:[c] $T^A{}_a\, v^a$, which is index notation for $T(v)$—compare (3.2.1.29).[d]

[a] Note that this is 'the same' as $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$ in the case of finite-dimensional vector spaces—see Corollary 5.3.4.20.

[b] Again, we technically haven't defined tensors that 'live in' more than module, but it should be clear what is meant.

[c] We cannot contract A and a as they are for different modules (hence the different scripts). Of course, if it so happens that $W = V$, then we could contract, and one finds that $T^b{}_b\, v^a = \mathrm{tr}(T)v$.

[d] This equation gives a formula for Av, A a matrix and v a column vector: $[Av]^i = \sum_{j=1}^{n} A^i{}_j v^j$.

▪ **Example 5.4.2.26 — Composition in index notation** Let U, V, and W be $\mathbb{K}$-modules, $\mathbb{K}$ a cring, and let ${S^A}_a \in U^\dagger \otimes V$ and ${T^\alpha}_A \in V^\dagger \otimes W$.[a]

We can take their tensor product ${T^\alpha}_A {S^B}_a$, which is a tensor of rank $\langle 2, 2\rangle$. There is only one possible contradiction of this tensor: ${T^\alpha}_A {S^A}_a$, which is index notation for $T \circ S$—compare (3.2.1.18).[b]

[a] Again, by Corollary 5.3.4.20, these are respectively the same as $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(U, V)$ and $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$ for finite-dimensional vector spaces.

[b] This equation gives a formula for AB, A and B matrices: $[AB]^i{}_k = \sum_{j=1}^n A^i{}_j B^j{}_k$. In fact, this similarity is exactly the reason we wrote the indices on the matrix the way we did (instead of the perhaps more common $[A]_{ij}$).

▪ **Example 5.4.2.27 — Bilinear forms in index notation** Let V be a $\mathbb{K}$-modules, $\mathbb{K}$ a cring, let $B \in V^\dagger \otimes V^\dagger$,[a] and let $v^a, w^a \in V$.

We can take their tensor product $v^a B_{bc} w^d$, which is a tensor of rank $\langle 2, 2\rangle$. Contracting in the 'obvious' way yields the scalar $v^a B_{ab} w^b$, which is index notation for $B(v, w)$—compare (5.8.2.5).

[a] A *bilinear form* is by definition a bilinear map $V \times V \to \mathbb{K}$—see Definition 5.8.1.1. By Corollary 5.3.4.23, this is the same as $V^\dagger \otimes V^\dagger$ for finite-dimensional vector spaces.

We now know enough about index notation to further elaborate on the map $V^\dagger \otimes W \to \mathrm{Mor}(V, W)$ of Corollary 5.3.4.20.

▪ **Example 5.4.2.28** In index notation, this map is written

$$\phi_a w^A \mapsto (v^a \mapsto \phi_a v^a w^A). \tag{5.4.2.29}$$

(Recall that in 'nonindex' notation this looks like $\phi \otimes w \mapsto (v \mapsto \phi(v)w)$.)

However, we've now seen in Example 5.4.2.25 that linear-transformations, being $\langle 1, 1\rangle$ tensors, are written in index no-

tation as $T^A{}_a$ (in which case $T(v)$ is written as $T^A{}_a\, v^a$). Thus, $T^A{}_a$ is the direct analog of T and $v^a \mapsto T^A{}_a\, v^a$ is the direct analogue of $v \mapsto T(v)$. So to, the linear-transformation $V \to W$ defined above in terms of ϕ and w in (5.4.2.29) in index notation can literally just be denoted $\phi_a w^A$, and it is understood that this is the name of the linear-transformation $v^a \mapsto \phi_a v^a w^A$ (just as T is the name of the linear-transformation $V \mapsto T(v)$). With this understanding, the map above can literally be written as

$$\phi_a w^A \mapsto \phi_a w^A. \tag{5.4.2.30}$$

Writing it this way I would say is technically a bit sloppy, but it should emphasize the point: whether you consider $\phi_a w^A$ as an element of $V^\dagger \otimes W$ or as a linear-transformation from V to W is a matter of perspective. If V and W are finite-dimensional vector spaces, this is *literally true* (the map is a natural isomorphism (Corollary 5.3.4.20)), but even when this isn't true, you can still think of $\phi_a w^A$ as defining a linear-transformation.[a]

Okay, so now that we've explained how this map can be written in index notation, let's give a concrete example.

Take $V := \mathbb{R}^d$ and $W := \mathbb{R}^e$, and let $\phi_a \in V^\dagger$ be a row vector and $w^A \in \mathbb{R}^e$ be a column vector. The linear-transformation is then $\phi_a w^A$. Want to take a wild guess as to what the matrix of this linear-transformation is with respect to the standard basis? Surprise, surprise, the $\langle i, j \rangle$ entry is $\phi_i w^j$.

For example, if

$$\phi = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \text{ and } v = \begin{bmatrix} 4 \\ 5 \end{bmatrix}, \tag{5.4.2.31}$$

then

$$\begin{aligned} [\phi \otimes w]_{\mathcal{S}_2 \leftarrow \mathcal{S}_3} &= \begin{bmatrix} 1 \cdot 4 & 2 \cdot 4 & 3 \cdot 4 \\ 1 \cdot 5 & 2 \cdot 5 & 3 \cdot 5 \end{bmatrix} \\ &= \begin{bmatrix} 4 & 8 & 12 \\ 5 & 10 & 15 \end{bmatrix}, \end{aligned} \tag{5.4.2.32}$$

where $\mathcal{S}_k$ is the standard basis of $\mathbb{R}^k$. Also, note how this is just the matrix product

$$v\phi. \tag{5.4.2.33}$$

The conclusion:

> Give a row vector $\phi \in [\mathbb{R}^d]^\dagger$ and a column vector $v \in \mathbb{R}^e$, then the matrix of the linear-transformation $\phi_a v^A$ with respect to the standard basis is just the $e \times d$ matrix given by the matrix product $v\phi$.

[a] In infinite-dimensions, it's just not the case that *every* linear-transformation is of this form. (Over general modules, things are a bit worse in that $\phi_a w^A$ and $\psi_a u^A$ can give the same linear-transformation even if $\phi \neq \psi$ and $w \neq u$, but this still doesn't change the fact that $\phi_a w^A$ defines a linear transformation.)

These examples suggest an important point that is quite helpful for intuition.

> It can help intuition to think of contracted indices being summed over.

Indeed, it's true generally that, upon picking a basis, contracted indices are summed over when computing with the coordinates of the tensors with respect to that basis.[18]

For this reason, I tend to think of index contraction as being a sort of dot product. The justification for this intuition of course comes from the fact that contracted indices are summed over in coordinates. In particular, I think of $v^a \nabla_a f(x)$ as the dot product of v^a with $\nabla_a f(x)$, which of course is just the directional derivative.[19]

[18] We're not going to define coordinates for arbitrary tensors because we don't really have any need. The idea is no different than it was with linear-transformations and writing it out in detail is not very enlightening with all the ellipses and such.

[19] This is yet another strength of index notation—it allows one to write more transparent expressions in some cases. The notation $v^a \nabla_a f(x)$ here has the advantage

Let's now take a look at a concrete example of the use of index notation.

▪ **Example 5.4.2.34 — Associativity in index notation** Let $\mathbb{K}$ be a ring and let A be a $\mathbb{K}$-algebra (Definition C.3.1.1). From the definition, multiplication $A \times A \to A$ is bilinear, and so is given by a tensor $m^a{}_{bc}$ of rank $\langle 1, 2\rangle$:

$$[X \cdot Y]^a = m^a{}_{bc} X^b Y^c. \tag{5.4.2.35}$$

For the sake of practice, let's try to determine what the condition of associativity looks like in index notation.[a] Associativity is 'normal' notation is the statement that

$$(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z). \tag{5.4.2.36}$$

In index notation, this becomes

$$m^a{}_{bc} [X \cdot Y]^b Z^c = m^a{}_{bc} X^b [Y \cdot Z]^c, \tag{5.4.2.37}$$

which in turn becomes

$$m^a{}_{bc} m^b{}_{de} X^d Y^e Z^c = m^a{}_{bc} X^b m^c{}_{de} Y^d Z^e. \tag{5.4.2.38}$$

Rearranging this and changing names of contracted indices,[b] this becomes

$$m^a{}_{bc} m^b{}_{de} X^d Y^e Z^c = m^a{}_{bd} m^b{}_{ec} X^d Y^e Z^c. \tag{5.4.2.39}$$

From this, we read off

$$m^a{}_{bc} m^b{}_{de} = m^a{}_{bd} m^b{}_{ec}, \tag{5.4.2.40}$$

which is the condition of associativity in index notation.

[a] To be honest, this is a case where using index notation is probably not very helpful (I think I've used this like once), but it is good practice.

[b] It will be easier to read off the condition on $m^a{}_{bc}$ if the indices on X, Y, and Z are the same on both sides of the equation.

that it looks exceedingly similar to how I would have written this in multivariable calculus ($\vec{v} \cdot \vec{\nabla} f(x)$). Without index notation, this might be written instead as $\mathrm{d}f(x)(v)$, which, at least for me, is relatively unintuitive and awkward.

5.4.3 Metrics

We need one more ingredient for the purposes of manipulating tensors, namely that of a *metric*.

Definition 5.4.3.1 — Metric (on a vector space) Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule. Then, a ***metric*** on V is a symmetric nonsingular pairing $(\cdot \mid \cdot) \colon V \times V \to \mathbb{K}$.

R By definition, $(\cdot \mid \cdot)$ is ***symmetric*** iff

$$(v_1 \mid v_2) = (v_2 \mid v_1) \tag{5.4.3.2}$$

for all $v_1, v_2 \in V$.

R The idea of a notion of a metric on a vector space and a metric on a set (in the context of uniform space theory) have little to nothing to do with each other.[a] It is merely a coincidence of terminology that is so ingrained that I dare not go against it.

The term "metric" in this sense of the word should really not be thought of as a sort of distance, but rather as a sort of dot product. Indeed, you can verify that the dot product is a metric, and furthermore, in a sense that we don't bother to make precise, every positive-definite metric (on a vector space) is equivalent to the usual euclidean dot product. There is *some* connection with the other notion of metric, however—positive-definite metrics give us norms (the square-root $(v \mid v)$), which in turn gives us a metric (in the other sense).

R Nonsingularity is usually replaced with nondegeneracy. In finite dimensions, this is equivalent to nonsingularity (Proposition 5.2.2.5). In infinite dimensions, however, they are not equivalent, and it is nonsingularity that we want (so that we can raise and lower indices—see Notation 5.4.3.3).

[a] If you haven't heard of this before, great! You won't be confused by the potential conflict of terminology.

Let V be a$\mathbb{K}$-$\mathbb{K}$-bimodule and let $(\cdot \mid \cdot)\colon V \times V \to \mathbb{K}$ be a metric on V. By definition (Definition 5.2.2.1), a pairing $(\cdot \mid \cdot)\colon V \times V \to \mathbb{K}$ is bilinear, and hence by the defining property of the tensor product (Theorem 5.3.1.1), is 'the same' as a linear map $V \otimes_{\mathbb{K}} V \to \mathbb{K}$, that is, a covariant tensor of rank 2, which in index notation is denoted g_{ab}. By (slight) abuse of terminology, g_{ab} itself is referred to as the "metric".

Notation 5.4.3.3 — Metric in index notation Let V be a finite-dimensional vector space over a field, and let g_{ab} be a metric on V.

(i). In terms of the original pairing, we have

$$(v \mid w) = v^a w^b g_{ab}. \tag{5.4.3.4}$$

(ii). The statement that g_{ab} is symmetric is equivalent to the equality

$$g_{ab} = g_{ba}{}^{.a} \tag{5.4.3.5}$$

(iii). The rank 2 contravariant tensor corresponding to the inverse map $V^\dagger \to V$ is denoted by g^{ab}. From the definition, we have that

$$g^{cb} g_{ba} = \delta^c{}_a \tag{5.4.3.6a}$$
$$g_{cb} g^{ba} = \delta_c{}^a. \tag{5.4.3.6b}$$

(iv). The *dual-vector* of $v^b \in V$ is defined by

$$v_a \coloneqq g_{ab} v^b \tag{5.4.3.7}$$

(v). The *dual-vector* of $\phi_b \in V^\dagger$ with respect to g_{ab} is defined by

$$\phi^a \coloneqq g^{ab} \omega_b \tag{5.4.3.8}$$

R Recall that given any dual-pair $V \times W \to \mathbb{K}$, we obtain maps $V \to W^\dagger$ and $W \to V^\dagger$. In the case of a metric g_{ab} on V, by *symmetry*, we have just one map $V \to V^\dagger$, which, in index notation, looks like

$$V \ni v^b \mapsto g_{ab}v^b = g_{ba}v^b \in V^\dagger. \qquad (5.4.3.9)$$

Nonsingularity says that this map has an inverse $V^\dagger \to V$, which is 'the same' (by Corollary 5.3.4.20) as an element of $V \otimes V$—this element is our g^{ab} in (iii).

R *Important*: g_{ab} of course starts out as a pairing on V, and so we could always talk about $g_{ab}v^a w^b$. Using our new notation raising and lowering indices, this can be written

$$v_a w^a = g_{ab}v^a w^b = v^a w_a. \qquad (5.4.3.10)$$

In particular, $v_a w^a = v^a w_a$—when you dot the 'dot product' of two vectors with respect to g_{ab}, it doesn't matter which one has an index downstairs vs. upstairs.

R Thus, using (iv) and (v), we may *raise and lower indices*.[b] Lowering an index corresponds to applying the isomorphism $V \to V^\dagger$ and raising an index corresponds to applying its inverse $V^\dagger \to V$.

R Warning: Recall that (Notation 5.4.2.8), in index notation we denoted the transpose $T^\dagger$ by $T_b{}^a$, which potentially conflicts with $g^{ac}g_{bd}T^d{}_c$. In fact, however, these two agree, but *only if* $T^\dagger$ *is the transpose with respect to the dual-pair defined by* g_{ab} *(Definition 5.2.2.8) not* $V^\dagger \times V \to \mathbb{K}$.

To see this, note that $T^\dagger$ is defined by the equality

$$([T^\dagger](w) \,|\, v) = (w \,|\, T(v)), \qquad (5.4.3.11)$$

which in index notation reads

$$\begin{aligned} g_{ab}[T^\dagger]^a{}_c w^c v^b &= g_{ab}w^a T^b{}_c v^c \\ &= T_{ac}w^a v^c \\ &= g_{ab}T_c{}^a w^c v^b, \end{aligned} \qquad (5.4.3.12)$$

from which we read off $[T^\dagger]^a{}_c = T_c{}^a$.

R In view of (5.4.3.6), note that

$$g^a{}_b = \delta^a{}_b = g_b{}^a. \tag{5.4.3.13}$$

[a] This highlights one of the strengths of index notation: it provides a convenient way to express equality of tensors without having to 'plug in' values for everything (as in $(v_1 \mid v_2) = (v_2 \mid v_1)$).

[b] Though we do need a metric to do so.

It's worth noting that, everything *except* raising and lowering indices we can do without a metric. To raise and lower indices, we do need that *extra* structure. In particular, if you pick a different metric, then your meaning of v_a will change even though the metric does not appear explicitly in this notation.

We end this section with a couple of exercises to get practice using index notation.

Exercise 5.4.3.14 — Einstein's Equation Let V be a finite-dimensional vector space over a field $\mathbb{F}$ with $\dim(V) \neq 2$ and $\mathrm{Char}(\mathbb{F}) \neq 2$, let g_{ab} be a metric on V, and let R_{ab} be two rank 2 covariant tensor on V. Show that

$$R_{ab} - \tfrac{1}{2} R^x{}_x g_{ab} = 0 \tag{5.4.3.15}$$

iff $R_{ab} = 0$.

R The above is ***Einstein's equation*** in vacuum (in general, there would be a nonzero tensor on the right-hand side proportional to the *stress-energy tensor*). This equation is the defining equation in general relativity in the sense that space-time is taken to be a Riemannian manifold with metric g_{ab} that satisfies this equation (actually, R_{ab} is defined in terms of g_{ab}, but you don't need to use that for this problem).

Exercise 5.4.3.16 — Clifford algebra Let V be a finite-dimensional vector space over a field $\mathbb{F}$ with $\mathrm{Char}(\mathbb{F}) = 0$, let

g_{ab} be a metric on V, let A be an $\mathbb{F}$-algebra, and let $\gamma\colon V \to A$ be linear and define

$$\gamma_{a_1\cdots a_k} \coloneqq \gamma_{[a_1}\cdot\cdots\cdot\gamma_{a_k]}. \tag{5.4.3.17}$$

Show that if

$$\gamma_a\cdot\gamma_b + \gamma_b\cdot\gamma_a = 2g_{ab}, \tag{5.4.3.18}$$

then

$$\gamma^{ab}\cdot\gamma_b = (\dim(V)-1)\gamma^a. \tag{5.4.3.19}$$

R Throughout, we have omitted the indices corresponding to A. For example, with these indices put in, (5.4.3.18) would read

$$m^A{}_{BC}\gamma^B{}_a\gamma^C{}_b + m^A{}_{BC}\gamma^B{}_b\gamma^C{}_a = 2g_{ab}1^A,$$

where we have used uppercase for the A-indices, $m^A{}_{BC}$ is the multiplication tensor of A (confer Example 5.4.2.34) and $1^A \in A$ is the multiplicative identity. We recommend you do not do this problem with the A-indices written explicitly.

R To clarify, for example

$$\gamma_{ab} \coloneqq \gamma_{[a}\gamma_{b]} \coloneqq \tfrac{1}{2}(\gamma_a\cdot\gamma_b - \gamma_b\cdot\gamma_a). \tag{5.4.3.20}$$

R A is not quite a "Clifford algebra". Additionally, in order for A to be a *Clifford algebra*, the map $V \to A$ should be "universal". Learning about Clifford algebras however is not the point of this exercises, though of course feel free to look up "Clifford algebra" or "gamma matrices" if you'd like to know more.

R We assume that $\mathrm{Char}(\mathbb{F}) = 0$ so that the antisymmetrization makes sense.

5.4.4 The physicists' definition

If you've studied physics before, there is a good chance that you encountered a definition of "tensor" that doesn't look much at all like the one we've just given.[20] Let us try to explain the sense in which these two different definitions are related.

First of all, the "physicists definition" I have in mind sounds something like the following.[21]

> A *tensor* is a multidimensional array of numbers that transforms in a certain way under a certain group action.

Of course, this is not precise, and so the exact definition you find will not be exactly this. For example, the definition from [R T05, pg. 659] reads verbatim:

> A four-tensor (strictly speaking a four-tensor of rank 2) is defined as a set of sixteen numbers $T_{\mu\nu}$ (defined for every inertial frame $\mathscr{S}$), where the indices μ and ν run from 1 to 4, which, when formed into a 4×4 matrix T, satisfy
>
> $$T' = \Lambda T \tilde{\Lambda} \tag{15.137}$$
>
> —a property that exactly parallels Equation (15.132) for three-tensors.

To give you perhaps a better idea of what Taylor means, we reproduce what is essentially the same definition made precise (from [I M63, pg. 175]).[22]

[20] If you've never studied physics, then there is no possibility for confusion, and you should feel free to skip this subsubsection.

[21] You might have also simply heard that a tensor is just a multidimensional array of numbers, like a matrix, but of higher dimension. This is even more incorrect, but there is a reason people say this: in coordinates, tensors are represented by multidimensional arrays of numbers, but one must keep in mind that some information is lost—for example, a 3 dimensional array of numbers can't distinguish between a $\langle 3, 0\rangle$ tensor, a $\langle 2, 1\rangle$ tensor, a $\langle 1, 2\rangle$ tensor, or a $\langle 0, 3\rangle$ tensor.

[22] Incidentally, Gel'fand is by any reasonable standard a fantastic mathematician. I'm not sure where he got this wacky idea to use bases, but Hermann Weyl would not have been pleased. (And yes, he most certainly is using "**R**" as the name of a vector space. And yes, he is not staggering (all of) his indices. Please don't do this.)

> Let **R** be an n-dimensional vector space. We say that a p times covariant and q times contravariant tensor is defined with every basis in **R** there is associated as set of n^{p+q} numbers $a_{ij\cdots}^{rs\cdots}$ (there are p lower indices and q upper indices) which under change of basis defined by some matrix $\|c_i^{\ j}\}$ transform according to the rule
>
> $$a'^{rs\cdots}_{ij\cdots} = c_i^{\ \alpha} c_j^{\ \beta} \cdots b_\sigma^{\ r} b_\tau^{\ s} \cdots a^{\sigma\tau\cdots}_{\alpha\beta\cdots} \tag{6}$$
>
> with $\|b_i^{\ j}\}$ the transpose of the inverse of $\|c_i^{\ j}\}$. The number $p + q$ is called the rank (valence) of the tensor. The numbers $a_{ij\cdots}^{rs\cdots}$ are called the components of the tensor.

First of all, let's be clear: *this concept of "tensor" is* not *the same as ours*—they are only related.[23]

In brief, a *representation* of a group G on a vector space V is a group action of G on V by linear operators. Using this language, a mathematician would say that the physicist's definition is the statement that T lies in a certain representation of the group (in the example from [R T05], the Lorentz group).

The relationship between these two definitions then stems from the fact that *the vector space of tensors* $V^{k\otimes,l\otimes^\dagger}$ *carries a canonical representation of* $\mathrm{Aut}_{\mathbf{Vect}}(V)$. From this point of view, the difference between the mathematician's point of view and the physicists is a matter of working in different categories: for mathematicians, tensors are elements of the *vector space* $V^{k\otimes,l\otimes^\dagger}$, whereas for physicists tensors are elements of the *representation* (of $\mathrm{Aut}_{\mathbf{Vect}}(V)$) on $V^{k\otimes,l\otimes^\dagger}$.

One should really keep these concepts distinct in one's mind, however. For example, one often wants to think of tensors are being in a representation of, say, the group of isometries of V if V comes with a metric. If in your definition of tensor it is implicit that it already 'lives' in a representation of $\mathrm{Aut}_{\mathbf{Vect}}(V)$, it's not clear how one changes the group. To be honest, most physicists probably don't think about the mathematical formalism enough to realize that this is not clear.

[23] Incidentally, don't have your indices run from 1 to 4. I don't know what he was thinking, but in relativity they should really be running from 0 to 3.

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

In any case, I would imagine most would not have a problem with it anyways—being absolutely mathematically precise about what sort of object a tensor is (element of vector space or representation) won't affect numerical predictions, so why bother worrying?

5.4.5 Summary

In summary:

(i). A tensor of rank $\langle k, l\rangle$ is a linear map from

$$\underbrace{V \otimes \cdots \otimes V}_{k} \to \underbrace{V \otimes \cdots \otimes V}_{k} \tag{5.4.5.1}$$

(Definition 5.4.1.1).

(ii). A general tensor is an element of the tensor algebra $\bigotimes^{\bullet}_{\bullet} V := \bigoplus_{k,l\in\mathbb{N}} \bigotimes^{k}_{l} V$ (Theorem 5.4.1.9).

(iii). In finite-dimensions, a tensor of rank $\langle k, l\rangle$ is the same as an element of $\underbrace{V \otimes \cdots \otimes V}_{k} \otimes \underbrace{V^\dagger \otimes \cdots \otimes V^\dagger}_{l}$ (Theorem 5.4.1.6).

(iv). The identity linear-transformation is denoted by $\delta^a{}_b$.

(v). The transpose of $T^a{}_b$ is denoted $[T^\dagger] =: T_a{}^b$.

(vi). The tensor product of two tensors is denoted simply by juxtaposition (Notation 5.4.2.14).

(vii). We can contract indices (Notation 5.4.2.19). This corresponds to 'plugging in' a specified vector into specified covector (Definition 5.4.2.17).

(viii). If we have a metric, we can also raise and lower indices (Notation 5.4.3.3). This corresponds to applying the isomorphism defined by the metric $V \to V^\dagger$ and its inverse.

5.5 (Anti)symmetric tensors

We've already encountered the concept of a metric tensor g_{ab}, which by definition is symmetric: $g_{ab} = g_{ba}$. The subject of this section is to study tensors that have a similar sort of symmetry (or antisymmetry).

Intuitively, a tensor is *symmetric* iff permuting the indices doesn't change the tensor (*antisymmetric* will mean it changes by a sign). To discuss this permuting, we need to introduce the *symmetric group*.

5.5.1 The symmetric group

Definition 5.5.1.1 — Symmetric group Let S be a set. Then, the ***symmetric group*** of S is $\mathrm{Aut}_{\mathbf{Set}}(S)$.

R In this context, elements of $\mathrm{Aut}_{\mathbf{Set}}(S)$ tend to be referred to as ***permutations*** of S.

R $\mathrm{Aut}_{\mathbf{Set}}(S)$ is our fancy-schmancy category-theoretic notation for the set of all bijections $S \to S$.

Definition 5.5.1.2 — Cycle notation Let $S = \{1, \dots, m\}$ be a finite set and let $x_1, \dots, x_n \in S$ be distinct. Then, $(x_1 \dots x_n) \in \mathrm{Aut}_{\mathbf{Set}}(S)$ is the unique bijection that sends x_k to x_{k+1} for $1 \leq k \leq n-1$, sends x_n to x_1, and fixes everything else.

R Permutations of the form $(x_1 \dots x_n)$ are ***cycles***.

R The ***length*** of $(x_1 \dots x_n)$ is n.

R A ***transposition*** is a cycle of length 2.

R For example, $(325) \in \mathrm{Aut}_{\mathbf{Set}}(\{1,2,3,4,5\})$ is shorthand for the function $\{1,2,3,4,5\} \to \{1,2,3,4,5\}$

$$1 \mapsto 1 \tag{5.5.1.3a}$$
$$2 \mapsto 5 \tag{5.5.1.3b}$$
$$3 \mapsto 2 \tag{5.5.1.3c}$$
$$4 \mapsto 4 \tag{5.5.1.3d}$$
$$5 \mapsto 3. \tag{5.5.1.3e}$$

To discuss antisymmetry, we're going to need to discuss the *sign* of a permutation.

Theorem 5.5.1.4 — Sign of a permutation. Let S be a finite set and let $\sigma \in \mathrm{Aut}_{\mathbf{Set}}(S)$.

(i). σ can be written as a product of transpositions.

(ii). If $s_1 \cdots s_m = \sigma = t_1 \cdots t_n$ with each s_k and t_k a transposition, then m and n have the same parity $\mathrm{sgn}(\sigma) \in \{1, -1\}$, the ***sign*** σ.[a]

(iii). $\mathrm{sgn}\colon \mathrm{Aut}_{\mathbf{Set}}(S) \to \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$ is a group homomorphism.

R This says that every permutation can be written as a product of transpositions, and furthermore, the number of these transpositions is unique modulo 2.

R For $X = \{1, \ldots, m\}$ a finite set and $S = \{i_1, \ldots, i_k\} \subseteq S$, write $S^{\mathsf{C}} =: \{j_{k+1}, \ldots, j_m\}$ with $j_1 < \cdots < j_m$. Then, we shall write $\mathrm{sgn}(S) := \mathrm{sgn}(\sigma_S)$ for the unique permutation $\sigma\colon X \to X$ such that

$$\sigma(x) := \begin{cases} i_x & \text{if } x \leq k \\ j_x & \text{if } x \geq k+1. \end{cases} \tag{5.5.1.5}$$

For example, for $S := \{2, 4, 5\} \subseteq \{1, 2, 3, 4, 5\}$, σ_S sends 1 to 2, 2 to 4, 3 to 5, 4 to 1, and 5 to 3, that is, $\sigma_S = (124)(35)$, and so

$$\mathrm{sgn}(S) = -1. \tag{5.5.1.6}$$

[a] That is, m is even/odd iff n is even/odd.

Proof. We leave this as an exercise.

Exercise 5.5.1.7 Prove the result.

■

5.5.2 Basic definitions

We are now able to begin discussing (anti)symmetric tensors themselves.

Definition 5.5.2.1 — (Anti)symmetric Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and let $T^{a_1\cdots a_k} \in \bigotimes^k V$.

(i). $T^{a_1\cdots a_k}$ is ***symmetric*** iff

$$T^{a_1\cdots a_k} = T^{a_{\sigma(1)}\cdots a_{\sigma(k)}} \tag{5.5.2.2}$$

for all $\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,k\})$.

(ii). $T^{a_1\cdots a_k}$ is ***antisymmetric*** iff

$$T^{a_1\cdots a_k} = \mathrm{sgn}(\sigma) T^{a_{\sigma(1)}\cdots a_{\sigma(k)}} \tag{5.5.2.3}$$

for all

$$\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,k\}). \tag{5.5.2.4}$$

R The condition of being ***(anti)symmetric*** is defined for covariant tensors in an essentially identical manner. A general tensor is then ***(anti)symmetric*** iff it is (anti)symmetric in both its contravariant and covariant indices.

R The set of symmetric tensors of rank $\langle k, l\rangle$ is a subspace of $\bigotimes^k_l$ which is denoted

$$\bigvee^k_l V. \tag{5.5.2.5}$$

The set of antisymmetric tensors of rank $\langle k, l\rangle$ is a subspace of $\bigotimes^k_l$ which is denoted

$$\bigwedge^k_l V. \tag{5.5.2.6}$$

R We write

$$\bigvee^k V := \bigvee_0^k V \tag{5.5.2.7}$$

and

$$\bigvee_l V := \bigvee_l^0 V \tag{5.5.2.8}$$

respectively for the spaces of symmetric rank k contravariant tensors and symmetric rank l covariant tensors.

Similarly, we write

$$\bigwedge^k V := \bigwedge_0^k V \tag{5.5.2.9}$$

and

$$\bigwedge_l V := \bigwedge_l^0 V \tag{5.5.2.10}$$

respectively for the spaces of antisymmetric rank k contravariant tensors and antisymmetric rank l covariant tensors.

R As we had with $\bigotimes_l^k V$ (Definition 5.4.1.1), we have that $\bigvee_0^0 V \cong \mathbb{K} \cong \bigwedge_0^0 V$, $\bigvee_0^1 V \cong V \cong \bigwedge_0^1 V$, and $\bigvee_1^0 V = V^\dagger = \bigwedge_1^0 V$—tensors of these ranks (along with $\bigvee_1^1 V = \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, V) = \bigwedge_1^1 V$) are vacuously (anti)symmetric.

R This is nonstandard notation. First of all, usually people only work with covariant tensors in this context, in which case they denote these respectively by $\mathrm{Sym}^l(V)$ and $\Lambda^l(V)$.

R Sometimes people will say ***totally symmetric*** and ***totally antisymmetric*** for these concepts respectively, presumably to emphasize that one is discussing *all* the indices.

R Elements of $\bigwedge_l V$ are sometimes called ***differential forms*** or just ***forms***, for reasons obviously having to do with calculus. As such, these terms are usually reserved when doing manifold theory, in which case they probably referred not to just a single tensor but a tensor *field*.[a]

[a] "Field" in this context intuitively means that you associate a different tensor to each point (e.g. "vector field").

The definition of an (anti)symmetric tensor states how the tensor must "transform" upon permuting the indices. As it turns out, it suffices to just check how the indices transform under permutations.

Proposition 5.5.2.11 Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and let $T^{a_1\cdots a_k} \in \bigotimes^k V$.

(i). $T^{a_1\cdots a_k}$ is symmetric iff $T^{a_1\cdots a_k} = T^{a_{\sigma(1)}\cdots a_{\sigma(k)}}$ for all transpositions $\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,k\})$.

(ii). $T^{a_1\cdots a_k}$ is antisymmetric iff $T^{a_1\cdots a_k} = -T^{a_{\sigma(1)}\cdots a_{\sigma(k)}}$ for all transpositions $\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,k\})$.

R That is, $T^{a_1\cdots a_k}$ is antisymmetric iff switching any two indices gives you the same thing, and it antisymmetric iff switching any two indices gives you the same thing with a minus sign.

Proof. We leave this as an exercise.

Exercise 5.5.2.12 Prove the result.

■

Given an arbitrary tensor, there is a canonical way of 'turning it into' an (anti)symmetric one.

Definition 5.5.2.13 — (Anti)symmetrization Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule with $\mathrm{Char}(\mathbb{K}) = 0$, and let $T^{a_1\cdots a_k} \in \bigotimes^k V$.

(i). The ***symmetrization*** $T^{(a_1\cdots a_k)}$ of $T^{a_1\cdots a_k}$ is defined by

$$T^{(a_1\cdots a_k)} := \frac{1}{k!}\sum_{\sigma\in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,k\})} T^{a_{\sigma(1)}\cdots a_{\sigma(k)}}.$$

The ***antisymmetrization*** $T^{[a_1\cdots a_k]}$ of $T^{a_1\cdots a_k}$ is defined by

$$T^{[a_1\cdots a_k]} := \frac{1}{k!}\sum_{\sigma\in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,k\})} \mathrm{sgn}(\sigma) T^{a_{\sigma(1)}\cdots a_{\sigma(k)}}.$$

R The (anti)symmetrization of covariant tensors is defined in an essentially identical manner. You can take the (anti)symmetrization of a tensor with both contravariant and covariant parts, but you do the contravariant and covariant indices separately (so that you might more accurately use the terms "contravariant (anti)symmetrization" and "covariant (anti)symmetrization"). For example, the expression $T^{ab}{}_{(cde)}$ is perfectly valid, as is $T^{[abc]}{}_{(cd)}$.

R One can also adapt this to (anti)symmetrization in only some of the indices. For example, given the above, it should be clear what one means by $T^{[ab]c}{}_{(cd)[ef]}{}^{a}$.

R The factor of $\frac{1}{k!}$ is so that we have $T^{(a_1\cdots a_k)} = T^{a_1\cdots a_k}$ iff T is symmetric (and similarly for antisymmetric)—see the following definition.

R Recall that (Definition A.4.18) the characteristic of a ring is the smallest positive integer m such that $m \cdot 1 = 0$, unless no such m exists, in which case the characteristic is taken to be 0. We require $\mathbb{K}$ to be characteristic 0 here so that we're not dividing by 0 with our factors of $\frac{1}{k!}$.

[a] Here we see another strength of index notation. To be honest, I'm not sure how one would write this without indices unless you essentially just define it from scratch all over again. With index notation, however, it's quite simple.

▪ **Example 5.5.2.14** For example,

$$T_{(ab)} = \frac{1}{2}(T_{ab} + T_{ba}) \tag{5.5.2.15}$$

and

$$T^{[abc]} = \frac{1}{6}(T^{abc} - T^{acb} - T^{bac} + T^{bca} + T^{cab} - T^{cba}).$$

You figure out the signs here by counting the number of 'flips' to go from $\langle a, b, c\rangle$ to the order of indices for that term. For example, to go from $\langle a, b, c\rangle$ to $\langle a, c, b\rangle$, I need to do just one flip ($b \leftrightarrow c$), and so the sign for the second term is $(-1)^1 = -1$. On the other hand, to go from $\langle a, b, c\rangle$ to $\langle b, c, a\rangle$ takes two flips ($a \leftrightarrow c$ and then $b \leftrightarrow c$), and so the sign for the fourth term is $(-1)^2 = 1$.

We may now characterize the (anti)symmetric tensors using the concept of (anti)symmetrization.

Proposition 5.5.2.16 Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule with $\mathrm{Char}(\mathbb{K}) = 0$, and let $T^{a_1\cdots a_k} \in \bigotimes^k V$.

(i). $T^{a_1\cdots a_k}$ is symmetric iff

$$T^{a_1\cdots a_k} = T^{(a_1\cdots a_k)}. \tag{5.5.2.17}$$

(ii). $T^{a_1\cdots a_k}$ is antisymmetric iff

$$T^{a_1\cdots a_k} = T^{[a_1\cdots a_k]}. \tag{5.5.2.18}$$

R The "Char($\mathbb{K}$) = 0" condition is imposed here only so that the (anti)symmetrizations make sense.

Proof. We leave this as an exercise.

Exercise 5.5.2.19 Prove the result.

■

Exercise 5.5.2.20 Let $S^{a_1\cdots a_k}$ and $T_{a_1\cdots a_k}$ be tensors over a $\mathbb{K}$-module, $\mathbb{K}$ a cring with $\mathrm{Char}(\mathbb{K}) = 0$.

(i). Show that if T is symmetric,[a] then

$$S^{a_1\cdots a_k}T_{a_1\cdots a_k} = S^{(a_1\cdots a_k)}T_{a_1\cdots a_k}. \qquad (5.5.2.21)$$

(ii). Let $k \geq 2$. Show that if S is symmetric, then $S^{[a_1\cdots a_k]} = 0$.[b]

(iii). Is the converse of the previous part true? If so prove it; if not, give a counter-example.

(iv). Let $k \geq 2$. Show that $S^{a_1\cdots a_k}T_{a_1\cdots a_k} = 0$ if S is symmetric and T is antisymmetric.

[a] The analogous thing is true for T antisymmetric, but no need for you to prove essentially the same thing twice.

[b] Again, an analogous result holds if S is antisymmetric.

5.5.3 The (anti)symmetric algebras

We will make it 'official' later, but let us tentatively write $\bigvee^\bullet_\bullet V$ and $\bigwedge^\bullet_\bullet V$ respectively for the algebra of symmetric and antisymmetric tensors. We saw in Theorem 5.4.1.9 that all tensors form an algebra $\bigotimes^\bullet_\bullet V$ with multiplication given by the tensor product. And while $\bigvee^\bullet_\bullet V$ and $\bigwedge^\bullet_\bullet V$ form subspaces of $\bigotimes^\bullet_\bullet V$, they don't form subalgebras—the tensor product of (anti)symmetric tensors need not be (anti)symmetric. The following products are solutions to this problem.[24]

Definition 5.5.3.1 — (Anti)symmetric product Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and let $S^{a_1\cdots a_k} \in \bigotimes^k V$ and $T^{a_1\cdots a_l} \in \bigotimes^l V$.

[24] Though note the remark with the "Warning"!

(i). The ***symmetric product*** $[S \vee T]^{a_1 \cdots a_{k+l}}$ of S and T is defined by

$$[S \vee T]^{a_1 \cdots a_{k+l}} := \sum_{\substack{\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,k+l\}) \\ \sigma \text{ is a } \langle k,l \rangle \text{ shuffle.}}} S^{a_{\sigma(1)} \cdots a_{\sigma(k)}} T^{a_{\sigma(k+1)} \cdots a_{\sigma(k+l)}}.$$

(ii). The ***antisymmetric product*** $[S \wedge T]^{a_1 \cdots a_{k+l}}$ of S and T is defined by

$$[S \wedge T]^{a_1 \cdots a_{k+l}} := \sum_{\substack{\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,k+l\}) \\ \sigma \text{ is a } \langle k,l \rangle \text{ shuffle.}}} \mathrm{sgn}(\sigma) S^{a_{\sigma(1)} \cdots a_{\sigma(k)}} T^{a_{\sigma(k+1)} \cdots a_{\sigma(k+l)}}.$$

R $\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1, \ldots, k+l\})$ is a $\langle k, l \rangle$ ***shuffle*** iff

$$\sigma(1) < \cdots < \sigma(k) \text{ and } \sigma(k+1) < \cdots < \sigma(k+l).$$

The term comes from the fact that if you break up a deck of $k + l$ cards into two piles, one with k cards and one with l cards, and you "shuffle" them, then the cards will be 'mixed up' in such a way so that the first pile of k cards is still 'in order' compared to other cards from that pile, and similarly for the second pile of l cards.

Note that the subset of shuffles is *not* a subgroup of the symmetric group—the composition of two shuffles need not be a shuffle.[a]

R As with everything else we've done so far, this can be extended to general tensors of mixed rank.

R The antisymmetric product is more commonly referred to as the ***wedge product***, simply because that is the symbol used to denote it.

R While our notation for the antisymmetric product is standard, our notation for the symmetric product is not. The symmetric product is more commonly denoted by $S \odot T$.

R Warning: We'll see in a bit that these do make $\bigvee^\bullet V$ and $\bigwedge^\bullet V$ respectively into algebras, however they are *not* subalgebras of $\bigotimes^\bullet V$. The reason is simply because the multiplications are not the same.

[a] And in fact, it had better not be if we're going to shuffle our cards like this!

▪ **Example 5.5.3.2** For example, if $S^a \in \bigwedge^1 V$ and $T^{bc} \in \bigwedge^2 V$, then

$$\begin{aligned}
[S \wedge T]^{abc} &:= \frac{3!}{2!1!} S^{[a} T^{bc]} \\
&:= \frac{3!}{2!1!} \cdot \frac{1}{3!} \left[S^a T^{bc} - S^a T^{cb} - S^b T^{ac} \right. \\
&\qquad \left. + S^b T^{ca} + S^c T^{ab} - S^c T^{ba} \right] \\
&= \frac{1}{2} \left[S^a T^{bc} + T^a T^{bc} + S^b T^{ca} \right. \\
&\qquad \left. + S^b T^{ca} + S^c T^{ab} + S^c T^{ab} \right] \\
&= \frac{1}{2} \left[2S^a T^{bc} + 2S^b T^{ca} + 2S^c T^{ab} \right] \\
&= S^a T^{bc} + S^b T^{ca} + S^c T^{ab}.
\end{aligned} \tag{5.5.3.3}$$

In case $\mathrm{Char}(\mathbb{K}) = 0$, this definition can be written in another, arguably simpler, form.

Proposition 5.5.3.4 Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule with $\mathrm{Char}(\mathbb{K}) = 0$, and let $S^{a_1 \cdots a_k} \in \bigotimes^k V$ and $T^{a_1 \cdots a_l} \in \bigotimes^l V$.

(i).

$$[S \vee T]^{a_1 \cdots a_{k+l}} = \frac{(k+l)!}{k!l!} S^{(a_1 \cdots a_k} T^{a_{k+1} \cdots a_{k+l})}. \tag{5.5.3.5}$$

(ii).

$$[S \wedge T]^{a_1 \cdots a_{k+l}} = \frac{(k+l)!}{k!l!} S^{[a_1 \cdots a_k} T^{a_{k+1} \cdots a_{k+l}]}. \tag{5.5.3.6}$$

R Char($\mathbb{K}$) = 0 is only needed so that we don't risk dividing by 0.

Proof. We leave this as an exercise.

Exercise 5.5.3.7 Prove the result.

■

A trivial but quite important corollary of the definition is that the antisymmetric product of two vectors vanishes.

Proposition 5.5.3.8 — $\wedge$ is super-commutative Let V be $\mathbb{K}$-module, $\mathbb{K}$ a cring, and let $S \in \bigwedge^p V$ and $T \in \bigwedge^q V$. Then,

$$S \wedge T = (-1)^{pq} T \wedge S. \tag{5.5.3.9}$$

R In particular, if the rank of T is odd, $T \wedge T = -T \wedge T$, and hence $T \wedge T = 0$.[a]

R Warning: It is *not* the case that $T \wedge T = 0$ all the time (even when $2 \in \mathbb{K}$ is a unit). For this to be the case, the rank of T should be odd.

R *Commutative* would mean of course that $ST = TS$. *Anticommutative* would mean that $ST = -TS$. ***Super-commutativity*** on the other hand refers to the fact that two tensors of definite rank[b] commute or anticommute depending on their ranks.

[a] Actually, if Char($\mathbb{K}$) = 2, it is still true, but not so immediate (because this rearranges to $2T \wedge T = 0$, but in characteristic 2 we cannot divide by 2 to obtain $T \wedge T = 0$)—see the following result.

[b] For example, the sum of a tensor of rank 2 with a tensor of rank 3 is still a tensor, but not one of definite rank.

Proof.

$$S^{[a_1\cdots a_p}T^{a_{p+1}\cdots a_{p+q}]} = (-1)^p S^{[a_{p+1}a_1\cdots a_{p-1}}T^{a_p a_{p+2}\cdots a_{p+q}]}.$$

In words, to move the index a_{p+1} all the way to the left, we move it past p other indices, picking up p minus signs along the way. Doing the same for a_{p+2} gives another p minus signs, and so on. Moving all the indices $a_{p+1},\dots,a_{p+q}$ all the way to the left thus generates $p\cdot q$ minus signs, giving

$$S^{[a_1\cdots a_p}T^{a_{p+1}\cdots a_{pq}]} = (-1)^{pq} S^{[a_{p+1}\cdots a_{p+q}}T^{a_1\cdots a_p]}.$$

As $\mathbb{K}$ is commutative (so that everything commutes in index notation), it follows that $S\wedge T = (-1)^{pq}T\wedge S$. ∎

Proposition 5.5.3.10 Let V be a $\mathbb{K}$-module, $\mathbb{K}$ a cring, and let $T\in\bigwedge^k V$. Then, if k is odd, then $T\wedge T = 0$.

Proof. Suppose that k is odd. Let $\sigma\in \mathrm{Aut}_{\mathbf{Set}}(\{1,\dots,2k\})$ and denote by $\breve{\sigma}\in\mathrm{Aut}_{\mathbf{Set}}(\{1,\dots,2k\})$ the permutation defined by

$$\breve{\sigma}(i) := (1(k+1))(2(k+2))\cdots((k-1)(2k-1))(k(2k))\sigma.^a$$

Note that $\breve{\breve{\sigma}} = \sigma$ and that $\breve{\sigma}$ is a $\langle k,k\rangle$ shuffle iff σ is. Furthermore, because k is odd, we have that $\operatorname{sgn}(\breve{\sigma}) = -\operatorname{sgn}(\sigma)$.

We now have that

$$\begin{aligned}
[T\wedge T]^{a_1\cdots a_{2k}} &:= \sum_{\substack{\sigma\in\mathrm{Aut}_{\mathbf{Set}}(\{1,\dots,2k\})\\ \sigma \text{ is a } \langle k,k\rangle \text{ shuffle.}}} \operatorname{sgn}(\sigma)T^{a_{\sigma(1)}\cdots a_{\sigma(k)}}T^{a_{\sigma(k+1)}\cdots a_{\sigma(2k)}}\\
&= \sum_{\substack{\sigma:\ \{1,\dots,k\}\to\{1,\dots,2k\}\\ \text{injective.}}} \Big[\operatorname{sgn}(\sigma)T^{a_{\sigma(1)}\cdots a_{\sigma(k)}}T^{a_{\sigma(k+1)}\cdots a_{\sigma(2k)}} +\\
&\qquad \operatorname{sgn}(\breve{\sigma})T^{a_{\breve{\sigma}(1)}\cdots a_{\breve{\sigma}(k)}}T^{a_{\breve{\sigma}(k+1)}\cdots a_{\breve{\sigma}(2k)}}\Big]\\
&= \sum_{\substack{\sigma:\ \{1,\dots,k\}\to\{1,\dots,2k\}\\ \text{injective.}}} \Big[\operatorname{sgn}(\sigma)T^{a_{\sigma(1)}\cdots a_{\sigma(k)}}T^{a_{\sigma(k+1)}\cdots a_{\sigma(2k)}} +\\
&\qquad -\operatorname{sgn}(\sigma)T^{a_{\sigma(k+1)}\cdots a_{\sigma(2k)}}T^{a_{\sigma(1)}\cdots a_{\sigma(k)}}\Big]\\
&= 0.
\end{aligned}$$

■

R The basic idea of the proof is that the terms in this sum come in pairs, one for σ and one for $\check{\sigma}$, which by definition of $\check{\sigma}$, are the same except for possibly $\operatorname{sgn}(\check{\sigma})$. As for k odd, $\operatorname{sgn}(\check{\sigma}) = -\operatorname{sgn}(\sigma)$, everything cancels to yield 0.

[a] That is, $\check{\sigma}$ is the product of σ by the k transpositions $(i(k+i))$ as i runs from 1 to k. Intuitively, $\check{\sigma}$ does to $\{1, \ldots, k\}$ what σ did to $\{k+1, \ldots, 2k\}$ and vice versa.

Theorem 5.5.3.11 — The symmetric algebra. Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and define

$$\bigvee_{\bullet}^{\bullet} V := \bigoplus_{k,l \in \mathbb{N}} \bigvee_{l}^{k} V. \tag{5.5.3.12}$$

Then, $\bigvee_{\bullet}^{\bullet} V$ is a $\mathbb{K}$-algebra with multiplication given by the symmetric product.

R $\bigvee_{\bullet}^{\bullet} V$ is the ***symmetric algebra*** over V.

R If we ever have the need, then we shall write

$$\bigvee^{\bullet} V := \bigoplus_{k \in \mathbb{N}} \bigvee^{k} V \tag{5.5.3.13}$$

and

$$\bigvee_{\bullet} V := \bigoplus_{l \in \mathbb{N}} \bigvee_{l} V \tag{5.5.3.14}$$

respectively for the subalgebras of contravariant and covariant symmetric tensors.

R This notation is nonstandard. Usually people only look at the contravariant tensors, in which case the notation $S(V)$ is often used for the space of all contravariant tensors.

Proof. We leave this as an exercise.

Exercise 5.5.3.15 Prove the result.

■

Theorem 5.5.3.16 — The antisymmetric algebra. Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and define

$$\bigwedge_{\bullet}^{\bullet} V := \bigoplus_{k,l\in\mathbb{N}} \bigwedge_{l}^{k} V \tag{5.5.3.17}$$

Then, $\bigwedge_{\bullet}^{\bullet} V$ is a $\mathbb{K}$-algebra with multiplication given by the antisymmetric product.

R $\bigwedge_{\bullet}^{\bullet} V$ is the ***antisymmetric algebra*** over V, though it is more commonly referred to as the ***exterior algebra***.[a]

R If we ever have the need, then we shall write

$$\bigwedge^{\bullet} V := \bigoplus_{k\in\mathbb{N}} \bigwedge^{k} V \tag{5.5.3.18}$$

and

$$\bigwedge_{\bullet} V := \bigoplus_{l\in\mathbb{N}} \bigwedge_{l} V \tag{5.5.3.19}$$

respectively for the subalgebras of contravariant and covariant antisymmetric tensors.

R This notation is nonstandard. Usually people only look at the contravariant tensors, in which case the notation $\Lambda(V)$ is often used for the space of all contravariant tensors.

[a] It is called this because of its relationship with the *exterior derivative*. The "exterior derivative" is in turn referred to as "exterior" to contrast it with the notion of *interior derivative*.

Proof. We leave this as an exercise.

Exercise 5.5.3.20 Prove the result.

■

We saw above in Proposition 5.4.1.17 an explicit description of a basis for $\bigotimes^\bullet_\bullet$ give a basis for V. We now present the analogous results for $\bigvee^\bullet_\bullet$ and $\bigwedge^\bullet_\bullet V$.

Proposition 5.5.3.21 — Basis for $\bigvee^\bullet_\bullet V$ Let V be a finite-dimensional vector space over a field, let $\mathcal{B} =: \{b_1, \dots, b_d\}$ be a basis of V, denote the dual-basis by $\mathcal{B}^\dagger =: \{b^1, \dots, b^d\}$, and let $k, l \in \mathbb{N}$. Then,

$$\bigvee^k_l \mathcal{B} := \{ b_{i_1} \vee \cdots \vee b_{i_k} \vee b^{j_1} \vee \cdots \vee b^{j_l} : 1 \leq i_1 \leq \cdots \leq i_k \leq d; \quad 1 \leq j_1 \leq \cdots \leq j_n \leq d \} \tag{5.5.3.22}$$

is a basis for $\bigvee^k_l V$.

R This says that all possible symmetric products of k elements from $\mathcal{B}$ with nondecreasing indices with all possible symmetric products of l elements from $\mathcal{B}^\dagger$ with nondecreasing indices is a basis for $\bigvee^k_l V$. Putting these all together for all $k, l \in \mathbb{N}$ then gives a basis for $\bigvee^\bullet_\bullet V$.

The reason we require the indices to be nondecreasing is because, for example, $b_3 \vee b_2 \vee b_4 = b_2 \vee b_3 \vee b_4$. Thus, we may always rearrange the elements so that this is the case.

R Of course, it follows that the union of all these sets over $k, l \in \mathbb{N}$ then yields a basis for all of $\bigvee^\bullet_\bullet V$ (by Proposition 4.4.1.44).

Proof. We leave this as an exercise.

Exercise 5.5.3.23 Prove the result.

■

Proposition 5.5.3.24 — Basis for $\bigwedge^\bullet_\bullet V$ Let V be a finite-dimensional vector space over a field, let $\mathcal{B} =: \{b_1, \dots, b_d\}$ be a basis of V, denote the dual-basis by $\mathcal{B}^\dagger =: \{b^1, \dots, b^d\}$, and let $k, l \in \mathbb{N}$. Then,

$$\bigwedge^k_l \mathcal{B} := \{b_{i_1} \wedge \cdots \wedge b_{i_k} \wedge b^{j_1} \wedge \cdots \wedge b^{j_l} : 1 \leq i_1 < \cdots < i_k \leq d; \quad 1 \leq j_1 < \cdots < j_n \leq d\} \tag{5.5.3.25}$$

is a basis for $\bigwedge^k_l V$.

R This says that all possible antisymmetric products of k elements from $\mathcal{B}$ with (strictly) increasing indices with all possible antisymmetric products of l elements from $\mathcal{B}^\dagger$ with (strictly) increasing indices is a basis for $\bigwedge^k_l V$. Putting these all together for all $k, l \in \mathbb{N}$ then gives a basis for $\bigwedge^k_l V$.

Note how this is exactly as it was in the symmetric case except now the indices are *strictly* increasing instead of just nondecreasing. This essentially follows from the fact that $b_i \wedge b_i = 0$, and so all the elements in the above wedge products must be distinct.

R Of course, it follows that the union of all these sets over $k, l \in \mathbb{N}$ then yields a basis for all of $\bigwedge^\bullet_\bullet V$ (by Proposition 4.4.1.44).

R For the antisymmetric algebra, there is alternative notation that can be used to list the basis elements that can be more transparent. For $S \subseteq \{1, \dots, d\}$, define

$$b_S := \bigwedge_{k \in S} b_k, \tag{5.5.3.26}$$

where the wedge product is taken in order of increasing i. For example,

$$b_{\{1,3,7\}} := b_1 \wedge b_3 \wedge b_7. \tag{5.5.3.27}$$

Using this notation, we have that

$$\bigwedge^k \mathcal{B} := \{b_S : S \subseteq \{1, \ldots, d\}, |S| = k\}, \tag{5.5.3.28}$$

that is, the basis for $\bigwedge^k \mathcal{B}$ is given by the set of b_S for which S has k elements.[a]

R It follows that

$$\dim\left(\bigwedge_l^k V\right) = \binom{\dim(V)}{k}\binom{\dim(V)}{l}, \tag{5.5.3.29}$$

and in particular that

$$\bigwedge_l^k V = 0 \text{ if } k > \dim(V) \text{ or } l > \dim(V). \tag{5.5.3.30}$$

Hence,

$$\begin{aligned}\dim\left(\bigwedge_\bullet^\bullet V\right) &= \sum_{k,l=0}^{\dim(V)} \binom{\dim(V)}{k}\binom{\dim(V)}{l} \\ &= 2^{\dim(V)} \cdot 2^{\dim(V)} = 2^{2\dim(V)}.\end{aligned}$$

Similar results hold for the purely contravariant and covariant cases.

[a] Of course you can do something similar with $\bigwedge_l^k \mathcal{B}$. We just did the contravariant case because it's less messy (and so hopefully more understandable) to write down.

Proof. We leave this as an exercise.

Exercise 5.5.3.31 Prove the result.

■

▪ **Example 5.5.3.32** Let V be a 3-dimensional vector space over a field $\mathbb{F}$ with basis $\{b_1, b_2, b_3\}$. Then,

(i). $\{1\}$ is a basis of $\bigwedge^0 V \cong \mathbb{F}$;
(ii). $\{b_1, b_2, b_3\}$ is a basis of $\bigwedge^1 V \cong V$;
(iii). $\{b_1 \wedge b_2, b_1 \wedge b_3, b_2 \wedge b_3\}$ is a basis of $\bigwedge^2 V$;
(iv). $\{b_1 \wedge b_2 \wedge b_3\}$ is a basis of $\bigwedge^3 V$;
(v). and $\bigwedge^k V = 0$ for $k > 3$.

R Feel free to write out bases for $\bigotimes^k V$ and $\bigvee^k V$ if you like. We only refrained from doing so as these are infinite-dimensional in general, which necessitates the use of ellipses, which means an explicit example isn't going to be significantly more readable than the general results (Propositions 5.4.1.17 and 5.5.3.24).

Note that $\bigotimes^\bullet V$ and $\bigvee^\bullet V$ are both infinite-dimensional (unless $V = 0$). For example, if $v \in V$ is nonzero, then

$$\{\underbrace{v \vee \cdots \vee v}_{k} : k \in \mathbb{Z}^+\} \tag{5.5.3.33}$$

is linearly-independent (and similarly for $\otimes$). This is one place where the antisymmetric differs from the symmetric case, and this difference is one reason why the antisymmetric algebra is more frequently encountered than the symmetric one.

Essentially this difference stems from the fact that $v \wedge v = 0$, and so $b_{i_1} \wedge \cdots \wedge b_{i_k} = 0$ if any of the b_{i_j}s coincide. This forces all the b_{i_j}s to be distinct, and so if the basis is finite with d elements, there are most $\binom{d}{k}$ nonzero elements of that form (and accordingly to the above, these nonzero elements constitute a basis for $\bigwedge^\bullet V$).

5.6 Extension of scalars

Because of its intimate connection with the antisymmetric algebra, our next objective is to investigate the *determinant*. However, before we do so, it will be convenient to first investigate something that is

important in its own right, the *algebraic closure* of a vector space,[25] which in turn is a specific example of the construction known as *extension of scalars*.

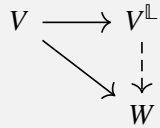
To see the motivation for this, recall the standard example of the matrix that is not diagonalizable.

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{5.6.1}$$

In some sense, it *should* be diagonalizable, but of course it can't be (over $\mathbb{R}$)—it doesn't have any eigenvalues! But we know that really, I mean, come on, this thing is diagonalizable. Just don't be an idiot and forget about the complex numbers! They exist, why would you ignore them!? Believe it or not, the tensor product gives us a tool to 'remember' the complex numbers, even if originally we are working over $\mathbb{R}$.

5.6.1 The definitions

Theorem 5.6.1.1 — Extension of scalars (for a module). Let V be a $\mathbb{K}$-module and let $\mathbb{L}$ be a $\mathbb{K}$-algebra. Then, there is a unique $\mathbb{K}$-linear map $V \to V^{\mathbb{L}}$ into the $\mathbb{L}$-module $V^{\mathbb{L}}$ such that if $V \to W$ is any other $\mathbb{K}$-linear map into an $\mathbb{L}$-module W, then there is a unique $\mathbb{L}$-linear map $V^{\mathbb{L}} \to W$ such that the following diagram commutes.



(5.6.1.2)

Furthermore,

(i). explicitly,

$$V^{\mathbb{L}} := \mathbb{L} \otimes_{\mathbb{K}} V; \tag{5.6.1.3}$$

[25] This term is nonstandard. I looked for awhile, but while the concept itself is ubiquitous, I couldn't actually find a name for the concept in general (though for $\mathbb{R}/\mathbb{C}$ it's called *complexification*.

and

(ii). if $\mathbb{K}$ and $\mathbb{L}$ are fields, then $V \to V^{\mathbb{L}}$ an embedding.

R Given a $\mathbb{K}$-module V and a $\mathbb{K}$-algebra $\mathbb{L}$, the passage from the $\mathbb{K}$-module V to the $\mathbb{L}$-module $\mathbb{L} \otimes_{\mathbb{K}} V$ is referred to as ***extension of scalars***.

R Let V be a vector space over a field $\mathbb{F}$ and let $\mathbb{A}$ be an algebraic closure of $\mathbb{A}$. In this case, $V^{\mathbb{A}}$ is the ***algebraic closure*** of V.

Recall that such an $\mathbb{A}$ exists by Theorem C.3.3.39. In brief, $\mathbb{A}$ (i) contains $\mathbb{F}$, (ii) is algebraically closed (Definition C.3.3.1), and (iii) is algebraic over $\mathbb{F}$ (Meta-definition C.3.3.17). The important point is (ii), which means that every nonconstant polynomial with coefficients in $\mathbb{A}$ can be written as a product of linear factors.

As mentioned above, the term "algebraic closure" is nonstandard here (this is essentially exclusively reserved for the contexts of fields), but I don't believe there is such a term used for this in general, and so I just made one up.

The exception is the case $\mathbb{F} = \mathbb{R}$, so that we may take $\mathbb{A} = \mathbb{C}$, in which case $V^{\mathbb{C}}$ is referred to as the ***complexification*** of V.

R As in Theorem 5.3.1.1, $V^{\mathbb{L}}$ is "unique up to unique isomorphism".

R In the case $\mathbb{K}$ and $\mathbb{L}$ are division rings, as the "universal" map $V \to V^{\mathbb{L}}$ is an embedding, we identify V with its image in $V^{\mathbb{L}}$, so that $V \subseteq V^{\mathbb{L}}$.

R Being a tensor product, $V^{\mathbb{L}}$ is spanned by elements of the form

$$\alpha \otimes v \tag{5.6.1.4}$$

for $\alpha \in \mathbb{L}$ and $v \in V$. Intuitively, just think of this as $\alpha \cdot v$, as if $\alpha \cdot v$ made sense all along. Thus, in a sense, you're just 'cheating' by 'throwing in' all possible

scalings of elements of V by elements in $\mathbb{L}$. For example, if V is a real vector space and $v \in V$, then $\mathrm{i} \cdot v \in V^{\mathbb{C}}$ and is literally defined to be $\mathrm{i} \cdot v := \mathrm{i} \otimes v$.

In fact, I would go so far as to say that this concept is so easy, that it's possible you would perform this construction do this construction without even realizing it. For example, if I tell you that $\langle 1, 2, 3\rangle \in \mathbb{R}^3$, and 5 minutes later you write something down like $\langle -2\mathrm{i}, -4\mathrm{i}, -6\mathrm{i}\rangle$, first of all, shame on you,[a] and second of all, you have implicitly just passed from $\mathbb{R}^3$ to $[\mathbb{R}^3]^{\mathbb{C}} \cong \mathbb{C}^3$.

R Note that we can always regard $V^{\mathbb{L}}$ as a $\mathbb{K}$-module if we like. In the case of fields, so that $\mathbb{K} \subseteq \mathbb{L}$, this is easily understood: because $\mathbb{K} \subseteq \mathbb{L}$, we can simply "forget" about the scaling by elements in $\mathbb{L} \setminus \mathbb{K}$.

[a] I told you to work over $\mathbb{R}$!

Proof. We leave this as an exercise.

Exercise 5.6.1.5 Prove the result.

■

We have an analogous construction for linear-transformations. We begin with a preliminary result of importance in its own right.

Theorem 5.6.1.6 — Extension of scalars (for a linear-transformation). Let V and W be $\mathbb{K}$-modules, let $\mathbb{L}$ be a $\mathbb{K}$-algebra, and let $T : V \to W$ be a linear-transformation. Then, there exists a unique linear-transformation $T^{\mathbb{L}} : V^{\mathbb{L}} \to W^{\mathbb{L}}$ such that $T^{\mathbb{L}}(v) = T(v)$ for $v \in V \subseteq V^{\mathbb{L}}$.

Furthermore,

(i). explicitly,

$$T^{\mathbb{L}}(\alpha \otimes v) = \alpha \otimes T(v);^{a}; \tag{5.6.1.7}$$

and

(ii). for any $\mathbb{L}$-module U, the map

$$\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V,U) \ni T \mapsto T^{\mathbb{L}} \mathrm{Mor}_{\mathbb{L}\text{-}\mathbf{Mod}}(V^{\mathbb{L}},U) \quad (5.6.1.8)$$

is a natural isomorphism of commutative groups.

R If $\mathbb{F}$ is a field and $\mathbb{A}$ is an algebraic closure, then $T^{\mathbb{A}}$ is the ***algebraic closure***. In case $\mathbb{F} = \mathbb{R}$ and $\mathbb{A} = \mathbb{C}$, $T^{\mathbb{A}}$ is the ***complexification*** of T.

R As in the previous case, in some sense this construction is so easy you might perform it without realizing it. For example, consider the real matrix

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}. \quad (5.6.1.9)$$

Now consider it as a complex matrix. Congratulations! You've just complexified the above matrix.

Seriously though, complexifying in this case essentially just changes the domain from $\mathbb{R}^2$ to $\mathbb{C}^2$. Superficially, things might seem pretty much the same, but you should know by now that the domain and codomain are integral parts to the definition of any function.

In fact, this works quite generally—see Proposition 5.6.2.8.

R Warning: Note how in (5.6.1.8) the $^{\mathbb{L}}$ is *not* applied to U. In the proof, to show that this is an isomorphism, we're going to construct an inverse. It turns out that this inverse will be simply restriction to $V \to V^{\mathbb{L}}$. However, if we had used $W^{\mathbb{L}}$ instead of U, there is no guarantee that the image of V lies in W: all we would know is that it lies in $W^{\mathbb{L}}$, and so restriction wouldn't actually yield a map $V \to W$.

R We met the tensor-hom adjunction in Theorem 5.3.4.1. It turns out that (5.6.1.8) is another example of this fancy thing called an "adjunction". Before, we saw[b] that $U \otimes_S -$ is left adjoint to its right adjoint

$\mathrm{Mor}_{R\text{-}\mathbf{Mod}}(U, -)$, and that $- \otimes_S V$ is left adjoint to its right adjoint $\mathrm{Mor}_{\mathbf{Mod}\text{-}T}(V, -)$. Here, $-^{\mathbb{L}}$ is left adjoint to its right adjoint the *forgetful functor* from L-**Mod** to K-**Mod**, that is, the functor that throws away the extra structure of being an $\mathbb{L}$-module and only looks at the $\mathbb{K}$-module structure.

Of course you don't need to know what that means yet. But hopefully this is getting you all excited "Oh boy I better dedicate my life to mathematics because, among all the other oodles and oodles of neat-o things there are to learn, I can study adjunctions in the future!." Yay!

R *Important*: Let $T\colon V \to V$ be a linear operator on a finite-dimensional vector space V over a field $\mathbb{F}$ and let $\mathbb{A}$ be an algebraic closure of $\mathbb{F}$. T itself may not have any eigenvalues, but we know from the previous chapter that $T^{\mathbb{A}}$ will. Thus, this allows us to discuss the 'eigenvalues' of T that should be there, even when they aren't: we will instead just refer to the eigenvalues of $T^{\mathbb{A}}$.

For us, this will be the most important application of extension of scalars.

[a] In other words, $T^{\mathbb{L}} = \mathrm{id}_{\mathbb{L}} \otimes T$.
[b] Or rather, I told you.

Proof. We leave this as an exercise.

Exercise 5.6.1.10 Prove the result.

■

5.6.2 The case of vector spaces

In a remark of the previous theorem (Theorem 5.6.1.6), we said that complexifying a matrix amounts to doing nothing to the matrix itself and just changing the domain of the corresponding linear-transformation. The precise statement of this says something like "The matrix with respect to a basis in V is the same as the matrix with respect to a basis in $V^{\mathbb{L}}$.". To make sense of this, however, we need to

know if, given a basis $\mathcal{B}$ of V, is $\mathcal{B} \subseteq V^{\mathbb{L}}$ also a basis of $V^{\mathbb{L}}$ (regarded as a vector space over $\mathbb{L}$). The answer, as it turns out, is "Yes.".

Proposition 5.6.2.1 Let $\mathbb{K}$ and $\mathbb{L}$ be division rings with $\mathbb{K} \subseteq \mathbb{L}$, and let V be a vector space over $\mathbb{K}$.

(i). Let $\mathcal{B} \subseteq V$ be a basis. Then, $\mathcal{B} \subseteq V^{\mathbb{L}}$ is a basis when $V^{\mathbb{L}}$ is regarded as a vector space over $\mathbb{L}$.

(ii). Let $\mathcal{B} \subseteq V$ be a basis and let $C \subseteq \mathbb{L}$ be a basis when $\mathbb{L}$ is regarded as a vector space over $\mathbb{K}$. Then,

$$\{\alpha \otimes b : \alpha \in C, b \in \mathcal{B}\} \subseteq V^{\mathbb{L}} \tag{5.6.2.2}$$

is a basis when $V^{\mathbb{L}}$ is regarded as a vector space over $\mathbb{L}$.

R In particular,

$$\dim_{\mathbb{L}}(V^{\mathbb{L}}) = \dim_{\mathbb{K}}(V) \tag{5.6.2.3}$$

$$\dim_{\mathbb{K}}(V^{\mathbb{L}}) = \dim_{\mathbb{K}}(V)\dim_{\mathbb{K}}(\mathbb{L}). \tag{5.6.2.4}$$

Proof. We leave this as an exercise.

Exercise 5.6.2.5

■

■ **Example 5.6.2.6** Let V be a d-dimensional vector space over $\mathbb{R}$ with basis $\{b_1, \ldots, b_d\}$.

Note that $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$ with a basis given by $\{1, \mathrm{i}\} \subseteq \mathbb{C}$.

Then, $V^{\mathbb{C}}$ is a d-dimensional vector space over $\mathbb{C}$ with basis $\{b_1, \ldots, b_d\}$ and is a $2d$-dimensional vector space over $\mathbb{R}$ with basis

$$\{b_1, \mathrm{i}\, b_1, \ldots, b_d, \mathrm{i}\, b_d\}. \tag{5.6.2.7}$$

Proposition 5.6.2.8 Let $\mathbb{K}$ and $\mathbb{L}$ be division rings with $\mathbb{K} \subseteq \mathbb{L}$, let V and W be finite-dimensional vector spaces over $\mathbb{K}$ with respective bases $\mathcal{B}$ and $\mathcal{C}$, and let $T\colon V \to W$ be a linear-transformation. Then,

$$[T^{\mathbb{L}}]_{\mathcal{C}\leftarrow\mathcal{B}} = [T]^{\mathbb{L}}_{\mathcal{C}\leftarrow\mathcal{B}}. \tag{5.6.2.9}$$

Proof. We leave this as an exercise.

Exercise 5.6.2.10 Prove the result.

■

In fact, this is just one way in which things "don't change" when passing from $\mathbb{K}$ to $\mathbb{L}$. Another is the minimal polynomial.

Proposition 5.6.2.11 Let $\mathbb{K}$ and $\mathbb{L}$ be division rings with $\mathbb{K} \subseteq \mathbb{L}$, let V be a finite-dimensional vector space over $\mathbb{K}$, and let $T\colon V \to V$ be linear. Then,

$$p_{\min,T^{\mathbb{L}}} = p_{\min,T}. \tag{5.6.2.12}$$

Proof. We leave this as an exercise.

Exercise 5.6.2.13 Prove the result.

■

This has a satisfying corollary.

Corollary 5.6.2.14 Let $\mathbb{K}$ and $\mathbb{L}$ be division rings with $\mathbb{K} \subseteq \mathbb{L}$, let V be a finite-dimensional vector space over $\mathbb{K}$, and let $T\colon V \to V$ be linear. Then,

$$\mathrm{Eig}(T) = \mathrm{Eig}(T^{\mathbb{L}}) \cap \mathbb{K}. \tag{5.6.2.15}$$

Proof. From Theorem 4.5.8, we know that $\lambda \in \mathbb{K}$ is an eigenvalue of T iff $p_{\min,T}(\lambda) = 0 = p_{\min,T^{\mathbb{L}}}$ iff λ is an eigenvalue of $T^{\mathbb{L}}$. ■

Before moving on, you might want to take a look at Theorem C.5.11 in the appendix. It requires a bit too much background to place here, but the result gives a characterization of what it means for $T^{\mathbb{A}}$ to be diagonalizable. Thus, we can make a distinction between things which are not diagonalizable only because there aren't enough eigenvalues, like the matrix

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \tag{5.6.2.16}$$

and things which are fundamentally not diagonalizable, like nonzero nilpotent operators.

5.7 The determinant

Related to the determinant is the *trace* of a linear operator. As it will be used when we discuss the determinant and characteristic polynomial, we investigate it first.

5.7.1 The trace

Given a matrix A, it turns out that the trace is going to be the sum of the diagonal elements, $\sum_{k=1}^{d} A^k{}_k$. That *could* work, but. . . matrices, ew. Fortunately, this suggests that we could instead define the trace of a linear-transformation T to be $T^a{}_a$, and if your intuition for index notation is as it should be by now, you'll find it obvious that this agrees with the previous notion (upon picking a basis to obtain a matrix) but is "coordinate-independent" and doesn't involve matrices. This is basically perfect, except for the fact that we've only defined contraction (Definition 5.4.2.17) when the ground ring is a field.

Definition 5.7.1.1 — Trace Let V be a finite-dimensional vector space over a field and let $T\colon V \to V$ be linear. Then, the ***trace*** of T, $\mathrm{tr}(T)$, is defined by

$$\mathrm{tr}(T) \coloneqq T^{a}{}_{a}\,. \tag{5.7.1.2}$$

R As a matter of fact, the same is true if instead V is a finite rank $\mathbb{K}$-module (Definition 2.2.1.29). The reason we didn't state it 'officially' this way is because we are implicitly using the result Theorem 5.4.1.6 so that we may identify T as an element of $V \otimes V^{\dagger}$, so that in turn the contraction (Definition 5.4.2.17) is defined. The conclusion of Theorem 5.4.1.6 should still remain true of V is a finite rank $\mathbb{K}$-module, but for reasons of keeping the exposition 'clean', we didn't state this.

In fact, throughout the entirety of these notes, when it came to anything that required finite-dimensionality of any sort, we always just worked over vector spaces, the logic being that one can only define the dimension for vector spaces. That's not quite true, however, in that you can define the "dimension" of *some* modules, even those not over division rings, though in this context it's not usually called "dimension" but rather *rank*. In any case, some of these instances, we could have gotten away with working with "finite-rank modules" instead of "finite-dimensional vector spaces", but in order to avoid complicating the exposition, we just didn't consider those cases.

Here we do, at least tangentially in this remark, so that you are aware one can define the trace over any ring, not just over fields or division rings.

Throughout this section, it should be assumed that things generalize to finite-rank modules unless otherwise indicated.

Theorem 5.7.1.3 — $\mathrm{tr}(T)$ = sum of eigenvalues. Let V be a finite-dimensional vector space over a field $\mathbb{F}$ with algebraic closure $\mathbb{A}$ and let $T: V \to V$ be linear. Then,

$$\mathrm{tr}(T) = \sum_{\lambda \in \mathrm{Eig}(T^{\mathbb{A}})} \dim(\mathrm{Eig}_{\lambda}^{\infty})\lambda. \tag{5.7.1.4}$$

R The dimension factor is there to take into account the "multiplicity" of the eigenvalue. For example, on a three-dimensional vector space, $\mathrm{tr}(2\,\mathrm{id}) = 2+2+2 = 6$, not just 2.

R As a linear-transformation on a finite-dimensional vector spaces has finitely many eigenvalues, this sum is finite and there are no worries of convergence.

R We actually met the trace briefly before as an example of a linear-functional—see Example 5.2.1.30.

Proof. We leave this as an exercise.

Exercise 5.7.1.5 Prove the result.

■

We finish this subsection with a couple of important properties of the trace.

Proposition 5.7.1.6 Let V be a finite-dimensional vector space over a field and let $S, T: V \to V$ be linear.

(i). $\mathrm{tr}(S+T) = \mathrm{tr}(S) + \mathrm{tr}(T)$.
(ii). $\mathrm{tr}(S \circ T) = \mathrm{tr}(T \circ S)$.

R Warning: (ii) does *not* imply that $\mathrm{tr}(R \circ S \circ T) = \mathrm{tr}(S \circ R \circ T)$. On the other hand, it *does* say that

$$\mathrm{tr}(R \circ S \circ T) = \mathrm{tr}(S \circ T \circ R) = \mathrm{tr}(T \circ R \circ S). \tag{5.7.1.7}$$

That is, inside a trace, you can "*cyclically*" permute the operators, but you can't permute them any way you like.

Proof. We leave this as an exercise.

Exercise 5.7.1.8 Prove the result.

■

Having seen the trace, we return to the determinant.

5.7.2 The determinant

Let V be a finite-dimensional vector space over a field and let $T\colon V \to V$ be linear. We may then take the tensor product of T with itself: $T \otimes T \in \mathrm{End}(V) \otimes \mathrm{End}(V) \cong \mathrm{End}(V \otimes V, V \otimes V)$, where we have used the natural isomorphism of Theorem 5.3.4.15. In index notation, this is written $T^a{}_b T^c{}_d$ and is defined in the obvious way: $v^b w^d \in V \otimes V \mapsto T^a{}_b T^c{}_d v^b v^d \in V \otimes V$. Looking at $T \otimes T \otimes T$, etc., we see that we obtain linear-transformations $\bigotimes^k T\colon \bigotimes^k V \to \bigotimes^k V$ for all $k \in \mathbb{N}$.[26]

What about for the symmetric and antisymmetric tensors? Do we have $\bigvee^k T$ and $\bigwedge^k T$? The answer is of course "Yes.".

Theorem 5.7.2.1 — $\bigvee^k T$ and $\bigwedge^k T$. Let V and W $\mathbb{K}$-$\mathbb{K}$-bimodules, let $T\colon V \to W$ be linear, and let $k \in \mathbb{N}$.

(i). There is a unique linear-transformation $\bigvee^k T\colon \bigvee^k V \to \bigvee^k W$ such that

$$v_1 \vee \cdots \vee v_k \mapsto T(v_1) \vee \cdots \vee T(v_k). \tag{5.7.2.2}$$

(ii). There is a unique linear-transformation $\bigwedge^k T\colon \bigwedge^k V \to \bigvee^k W$ such that

$$v_1 \wedge \cdots \wedge v_k \mapsto T(v_1) \wedge \cdots \wedge T(v_k). \tag{5.7.2.3}$$

[26] Recall that this was originally defined in Theorem 5.3.2.1.

R If it's clear from context, it's possible I may abuse notation and simply write "T" for "$\bigvee^k T$" or "$\bigwedge^k T$". For example, I can unambiguously write something like

$$T(v_1 \wedge v_2 \wedge v_2) := T(v_1) \wedge T(v_2) \wedge T(v_3), \quad (5.7.2.4)$$

for $v_1, v_2, v_3 \in V$, as it is clear from context that this must in fact be $\bigwedge^3 T$.

R Warning: This can be also be defined for covariant rank,[a] but *not* mixed rank. The reason is that $\bigwedge_l T$ will be a map from $\bigwedge_l W$ to $\bigwedge_l V$, *not* a map from $\bigwedge_l V$ to $\bigwedge_l W$. I suppose one could do mixed rank in the case $V = W$, but that's a bit awkward.

[a] $T^\dagger$ will be used in this case, e.g. $\phi \wedge \psi \mapsto T^\dagger(\phi) \wedge T^\dagger(\psi)$.

Proof. We leave this as an exercise.

Exercise 5.7.2.5 Prove the result.

■

Of course, $\bigotimes^0 T = \bigvee^0 T = \bigwedge^0 T = \mathrm{id}_V$ and $\bigotimes^1 T = \bigvee^1 T = \bigwedge^1 T = T$. If V is finite-dimensional, however, something special happens with $\bigwedge^{\dim(V)} T$. See, $\bigwedge^{\dim(V)} V$ is $\binom{\dim(V)}{\dim(V)} = 1$ dimensional vector space, which means that linear-transformations $\bigwedge^{\dim(V)} V \to \bigwedge^{\dim(V)} V$ are given by scalars.[27] This scalar has a name: it is the *determinant*.

Theorem 5.7.2.6 — Determinant. Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and let $T : V \to V$ be linear. Then, there is a unique scalar $\det(T) \in \mathbb{F}$, the

[27] A choice of basis associates to every such linear-transformation a 1×1 matrix, essentially just a scalar. Furthermore, this scalar is independent of the choice of basis (why?).

determinant of T, such that

$$\bigwedge^d T = \det(T)\,\mathrm{id}, \tag{5.7.2.7}$$

where $d := \dim(V)$ and id is the identity on $\bigwedge^d V$.

R As with the trace, we can use essentially the same definition here to define the determinant over any ring, but as this would involve discussion of finite rank modules, we refrained from stating this case 'officially' to not clutter the exposition with separate cases. See the remark in the definition of the trace (Definition 5.7.1.1) for an elaboration on this.

R Some authors write $|A|$ to denote the determinant of A. We shall not make use of this notation.

Proof. We leave this as an exercise.

Exercise 5.7.2.8 Prove the result.

■

It's quite likely that you've seen the determinant before, and that this doesn't at all look like the definition you've seen. Our first objective then is to show that this agrees with the definition (or a definition—there are many) you've seen before. Before we start, however, let's see an example of how one can actually compute the determinant using this definition.

■ **Example 5.7.2.9** Let $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be the unique linear-transformation such that

$$T(e_1) = e_1 + e_2 + e_3 \tag{5.7.2.10a}$$
$$T(e_2) = e_1 + 2e_2 + 3e_3 \tag{5.7.2.10b}$$
$$T(e_3) = e_1 - e_2 + e_3, \tag{5.7.2.10c}$$

where $\mathcal{S} := \{e_1, e_2, e_3\} \subseteq \mathbb{R}^3$ is the standard basis.

R As a check of understanding, make sure you can immediately read off

$$[T]_{\mathcal{S}} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{bmatrix}. \tag{5.7.2.11}$$

(See (3.2.2.3) if you've forgotten.)

$\{e_1 \wedge e_2 \wedge e_3\}$ is a basis for $\bigwedge^3 \mathbb{R}^3$ (see Example 5.5.3.32 for a slight elaboration), and so we compute

$$\begin{aligned}
[\textstyle\bigwedge^3 T](e_1 \wedge e_2 \wedge e_3) &:= T(e_1) \wedge T(e_2) \wedge T(e_3) \\
&= (e_1 + e_2 + e_3) \wedge (e_1 + 2e_2 + 3e_3) \wedge (e_1 - e_2 + e_3) \\
&= {}^a(2e_1 \wedge e_2 + 3e_1 \wedge e_3 + e_2 \wedge e_1 + 3e_2 \wedge e_3 \\
&\qquad + e_3 \wedge e_1 + 2e_3 \wedge e_2) \wedge (e_1 - e_2 + e_3) \\
&= {}^b(e_1 \wedge e_2 + 2e_1 \wedge e_3 + e_2 \wedge e_3) \wedge (e_1 - e_2 + e_3) \\
&= e_1 \wedge e_2 \wedge e_3 - 2e_1 \wedge e_3 \wedge e_2 + e_2 \wedge e_3 \wedge e_1 \\
&= e_1 \wedge e_2 \wedge e_3 + 2e_1 \wedge e_2 \wedge e_3 + e_1 \wedge e_2 \wedge e_3 \\
&= 4e_1 \wedge e_2 \wedge e_3.
\end{aligned}$$

Hence, it follows from the definition that

$$\det(T) = 4. \tag{5.7.2.12}$$

[a] Here I am using the fact that $v \wedge v = 0$ for vectors $v \in \mathbb{R}^3$.
[b] And here I am using the fact that $v \wedge w = -w \wedge v$ for vectors $v, w \in \mathbb{R}^3$.

Properties of the determinant

Before we see the equivalence of this definition to others you have more likely seen before, we will need to investigate some properties of the determinant.

One of the first properties of the determinant that we're going to be interested in is its relationship with composition of linear maps. The answer (Proposition 5.7.2.20) will following immediately from "functoriality" of $\bigwedge^k -$.

Theorem 5.7.2.13 — $\bigvee^k -$ and $\bigwedge^k -$ are functors. Let U, V, and W be $\mathbb{K}$-$\mathbb{K}$-bimodules, let $S\colon U \to V$ and $T\colon V \to W$ be linear, and let $k \in \mathbb{N}$.

(i).

$$\bigvee^k [T \circ S] = \bigvee^k T \circ \bigvee^k S. \tag{5.7.2.14}$$

(ii).

$$\bigvee^k \mathrm{id}_V = \mathrm{id}_{\bigvee^k V}. \tag{5.7.2.15}$$

(iii).

$$\bigwedge^k [T \circ S] = \bigwedge^k T \circ \bigwedge^l S. \tag{5.7.2.16}$$

(iv).

$$\bigwedge^k \mathrm{id}_V = \mathrm{id}_{\bigwedge^k V}. \tag{5.7.2.17}$$

R The covariant versions $\bigvee_l -$ and $\bigwedge_l -$ are *co*functors (so the same result is true, except the order of composition is reversed on the right-hand side).

Proof. (i) Let $u_1, \ldots, u_k \in U$. Then,

$$\begin{aligned}
&\left[\bigvee^k [T \circ S]\right](u_1 \vee \cdots \vee u_k) \\
&\quad := [T \circ S](u_1) \vee \cdots \vee [T \circ S](u_k) \\
&\quad := T(S(u_1)) \vee \cdots \vee T(S(u_k)) \\
&\quad =: \left[\bigvee^k T\right](S(u_1) \vee \cdots \vee S(u_k)) \\
&\quad =: \left[\bigvee^k T\right]\left(\left[\bigvee^k S\right](u_1 \vee \cdots \vee u_k)\right) \\
&\quad =: \left[\bigvee^k T \circ \bigvee^k S\right](u_1 \vee \cdots \vee u_k).
\end{aligned} \tag{5.7.2.18}$$

(ii) Let $v_1, \dots, v_k \in V$. Then,

$$\begin{aligned}[\textstyle\bigvee^k \mathrm{id}_V](v_1 \vee \cdots \vee v_k) &\coloneqq \mathrm{id}_v(v_1) \vee \cdots \vee \mathrm{id}_V(v_k) \\ &\coloneqq v_1 \vee \cdots \vee v_k \\ &=: \mathrm{id}_{\bigvee^k V}(v_1 \vee \cdots \vee v_k).\end{aligned} \tag{5.7.2.19}$$

(iii) Essentially the same as (i).

(iv) Essentially the same as (ii). ∎

Proposition 5.7.2.20 Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and let $S, T : V \to V$ be linear. Then,

$$\det(S \circ T) = \det(S)\det(T). \tag{5.7.2.21}$$

Proof. Write $d \coloneqq \dim(V)$. Then,

$$\begin{aligned}\det(S \circ T)\,\mathrm{id} &= \textstyle\bigwedge^d [T \circ S] = {}^a \bigwedge^d T \circ \bigwedge^d S \\ &= [\det(T)\,\mathrm{id}] \circ [\det(S)\,\mathrm{id}] \\ &= \det(T)\det(S)\,\mathrm{id}\,.\end{aligned} \tag{5.7.2.22}$$

Hence, $\det(S \circ T) = \det(S)\det(T)$. ∎

[a] By the previous result.

We now turn to show that this definition is equivalent to any definition you likely have seen before. There are a lot of equivalent definitions given, and we start with the one that does not require a reduction to the case of matrices.

Proposition 5.7.2.23 Let $S \oplus T : U \oplus V \to U \oplus V$ be a linear-transformation on a finite-dimensional vector space. Then,

$$\det(S \oplus T) = \det(S)\det(T). \tag{5.7.2.24}$$

R As mentioned in the remark of Theorem 5.7.2.6, most results hold here over finite-rank modules as well. This is one of them. Again, unless otherwise specified, this should be assumed throughout, and we will not provide a reminder again.

Proof. We leave this as an exercise.

Exercise 5.7.2.25 Prove the result.

■

Theorem 5.7.2.26 — det = product of eigenvalues. Let V be a finite-dimensional vector space over a field $\mathbb{F}$ with algebraic closure $\mathbb{A}$ and let $T : V \to V$ be linear. Then,

$$\det(T) = \prod_{\lambda \in \mathrm{Eig}(T^{\mathbb{A}})} \lambda^{d_\lambda}, \tag{5.7.2.27}$$

where $d_\lambda := \dim(\mathrm{Eig}^{\infty}_{\lambda, T^{\mathbb{A}}})$.

R The power here is to take into account the "multiplicity" of the eigenvalue. For example, on a three-dimensional vector space, $\det(2\,\mathrm{id}) = 2 \cdot 2 \cdot 2 = 8$, not just 2.

R As a linear-transformation on a finite-dimensional vector spaces has finitely many eigenvalues, this product is finite and there are no worries of convergence.

Proof. We first check that $\det(T) = \det(T^{\mathbb{A}})$. Let $\{b_1, \ldots, b_d\}$ be a basis for V. As $V \subseteq V^{\mathbb{A}}$, $\{b_1, \ldots, b_d\}$ is also a subset of $V^{\mathbb{A}}$, and in fact a basis for $V^{\mathbb{A}}$. From its defining result, we have $T^{\mathbb{A}}(b_k) = T(b_k)$. It thus follows from the definition of the determinant that $\det(T) = \det(T^{\mathbb{A}})$.

Thus, as $\det(T) = \det(T^{\mathbb{A}})$, without loss of generality assume that $\mathbb{F}$ itself is algebraically closed. Then, by the previous result, it suffices to show that the determinant of $T\colon \operatorname{Eig}_\lambda^\infty \to \operatorname{Eig}_\lambda^\infty$ is $\lambda^{\dim(\operatorname{Eig}_\lambda^\infty)}$. So, without loss of generality, assume that T only has a single eigenvalue $\lambda \in \mathbb{F}$.

Write $d := \dim(V) = \dim(\operatorname{Eig}_\lambda^\infty)$ and let $\mathcal{B} = \{b_1, \ldots, b_d\}$ be a Jordan basis of V for T so that either $[T - \lambda](b_k) = b_{k-1}$ or $[T - \lambda](b_k) = 0$ for $1 \leq k \leq d$.[a] Either way, we may write $T(b_k) = \lambda b_k + n_k b_{k-1}$, where $n_k = 0, 1$. Now, note that

$$T(b_1) \wedge T(b_2) = (\lambda b_1) \wedge (\lambda b_2 + n_1 b_1) = \lambda^2 b_1 \wedge b_2, \quad (5.7.2.28)$$

and hence

$$\begin{aligned} &T(b_1) \wedge T(b_2) \wedge T(b_3) \\ &\quad = (\lambda^2 b_1 \wedge b_2) \wedge (\lambda b_3 + n_2 b_2) \\ &\quad = \lambda^3 b_1 \wedge b_2 \wedge b_3. \end{aligned} \quad (5.7.2.29)$$

Proceeding inductively, we find that

$$\begin{aligned} [\textstyle\bigwedge^d T](b_1 \wedge \cdots \wedge b_d) &:= T(b_1) \wedge \cdots \wedge T(b_d) \\ &= \lambda^d b_1 \wedge \cdots \wedge b_d, \end{aligned} \quad (5.7.2.30)$$

and hence $\det(T) = \lambda^d$, as desired. ■

[a] These cases correspond respectively to the case where the corresponding column does and does not have a 1 above the diagonal.

This has a couple of important corollaries.

Corollary 5.7.2.31 Let V be a finite-dimensional vector space and let $T\colon V \to V$ be linear. Then, T is invertible iff $\det(T) \neq 0$.

R A linear-transformation with nonzero determinant is said to be ***nonsingular***. Thus, this theorem says that T is invertible iff it is nonsingular.

R Over a general commutative ring, this instead reads "T is invertible iff $\det(T)$ is invertible.".

Proof. We leave this as an exercise.

Exercise 5.7.2.32 Prove the result.

■

Corollary 5.7.2.33 — $\det(T^\dagger) = \det(T)$ Let V be a finite-dimensional vector space and let $T : V \to V$ be linear. Then,

$$\det(T^\dagger) = \det(T). \tag{5.7.2.34}$$

Proof. We leave this as an exercise.

Exercise 5.7.2.35 Prove the result.

R Hint: Use the previous result together with Proposition 5.2.2.14.

■

Exercise 5.7.2.36 Let V be a finite-dimensional vector space over a field. Show that $\{v_1, \ldots, v_m\} \subseteq V$ is linearly-dependent iff $v_1 \wedge \cdots \wedge v_m = 0$.

R You can probably do this without determinants, though the solution I have in mind uses them.

Determinants of matrices

We now take a look at the definitions of determinant in terms of matrices you might have seen before. The first and most important one says that the determinant is the unique scalar-valued function on

matrices that assigns 1 to the identity and transforms a certain way upon performing row operations (Definition 3.2.1.43).

Theorem 5.7.2.37. Let $\mathbb{K}$ be a cring and let $m \in \mathbb{N}$. Then, $\det\colon \mathrm{Matrix}_n(\mathbb{K}) \to \mathbb{K}$ is the unique function such that

$$\det(\mathrm{id}_n) = 1 \tag{5.7.2.38}$$

$$\det(\mathrm{Row}_{i_1 \to i_1 + \alpha i_2}(A)) = \det(A) \tag{5.7.2.39}$$

$$\det(\mathrm{Row}_{i_0 \to \alpha i_0}(A)) = \alpha \det(A) \tag{5.7.2.40}$$

$$\det(\mathrm{Row}_{i_1 \leftrightarrow i_2}(A)) = -\det(A). \tag{5.7.2.41}$$

R Thus, (i) the determinant of the identity matrix is 1, (ii) the determinant is invariant under adding a scalar multiple of one row to a different one, (iii) the determinant scales (by the same factor) upon scaling a row, and (iv) the determinant changes by a sign when you swap rows.

R This is both conceptually and practically significant. First of all, it gives a definition[a] of the determinant of matrices that doesn't look absolutely disgusting.[b] But besides being aesthetically pleasing, it's actually quite practical for calculating determinants: a common strategy is to row-reduce the given matrix to something simple enough you can compute the determinant directly (e.g. to an upper-triangular matrix), and then modify the determinant of that matrix as needed according to the row operations one used.

[a] Of course, it's a theorem for us, but one *could* take it as the definition (for matrices).

[b] Can you believe that some people actually define the determinant in terms of its cofactor expansion? Ew.

Proof. We leave this as an exercise.

Exercise 5.7.2.42 Prove the result.

■

There are still at least two other things I have seen taken as the definition of the determinant. We start with the more practical, though it will take a little bit to set-up—see Corollary 5.7.2.80.

Definition 5.7.2.43 — Minor Let V and W be a a finite-dimensional vector space over a field, let $\mathcal{B}$ and C be bases for V and W respectively, and let $T\colon V \to W$ be a linear-transformation. Then, the ***matrix of k-minors*** is $[\bigwedge^k T]_{\bigwedge^k C \leftarrow \bigwedge^k \mathcal{B}}$.

R The entries of the matrix of k-minors are themselves called ***minors***.

R Write $\mathcal{B} =: \{b_1, \dots, b_d\}$ and $C =: \{c_1, \dots, c_e\}$. Recall that (Proposition 5.5.3.24)

$$\bigwedge^k \mathcal{B} = \{b_S : S \subseteq \{1, \dots, d\}, |S| = k\} \quad (5.7.2.44)$$

and similarly for C, where

$$b_S := \bigwedge_{i \in S} b_i. \quad (5.7.2.45)$$

Thus, the entries of the matrix of minors are not indexed by numbers themselves, but rather *subsets* of numbers.[a] Thus, given a subset $S \subseteq \{1, \dots, d\}$ and $T \subseteq \{1, \dots, e\}$, we have a corresponding entry of the matrix $[\bigwedge^k T]^{T}_{\bigwedge^k C \leftarrow \bigwedge^k \mathcal{B}\ S}$. In fact, let's make this notation "official".

Given an $m \times n$ matrix A, $S \subseteq \{1, \dots, m\}$, and $T \subseteq \{1, \dots, n\}$, both with k elements, let us denote by

$$A^S{}_T \quad (5.7.2.46)$$

the $\langle S, T \rangle$-entry of the matrix of k-minors.[b]

R Note this is one of the few places in this section where we don't require the domain and codomain to coincide. In terms of matrices, this stems from three facts: (i) one can only talk about the determinant of square matrices, (ii) minors will be the determinants of "submatrices", and (iii) a nonsquare matrix can have submatrices that are square.

[a] I suppose more accurately they're indexed by basis elements, but those are in one-to-one correspondence with subsets of $\{1, \dots, d\}$ that have k elements.

[b] S corresponds to the rows that we keep and T corresponds to the columns that we keep when computing the determinant.

Okay, so as it stands, this definition is pretty impenetrable. Let's look at an example.

▪ **Example 5.7.2.47** Let $V := \mathbb{R}^3$, $W := \mathbb{R}^2$, take $\mathcal{B} := \{e_1, e_2, e_2\}$ and $C := \{e_1, e_2\}$ to be the standard bases, and let $T\colon V \to W$ be the linear-transformation defined by the matrix

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}. \tag{5.7.2.48}$$

$\bigwedge^0 T\colon \mathbb{R} \to \mathbb{R}$ is multiplication by 1, and not very interesting. On the other hand, $\bigwedge^1 T\colon V \to W$ is just T itself, which we already understand. So, let's take a look at $\bigwedge^2 T\colon \bigwedge^2 V \to \bigwedge^2 W$.

First of all, let's look at the bases $\bigwedge^2 \mathcal{B}$ and $\bigwedge^2 C$. According to Proposition 5.5.3.24, we have

$$\bigwedge^2 \mathcal{B} = \{e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3\} \tag{5.7.2.49}$$

and

$$\bigwedge^2 C = \{e_1 \wedge e_2\}. \tag{5.7.2.50}$$

We want to compute the matrix of $\bigwedge^2 T$ with respect to these two bases, so going all the way back to Theorem 3.2.2.1, we

compute what $\bigwedge^2 T$ does do the elements of the basis $\bigwedge^2 \mathcal{B}$.

$$\begin{aligned}[\bigwedge^2 T](e_1 \wedge e_2) &:= T(e_1) \wedge T(e_2) \\ &:= (e_1 + 4e_2) \wedge (2e_1 + 5e_2) \\ &= 5e_1 \wedge e_2 + 8e_2 \wedge e_1 \\ &= -3e_1 \wedge e_2.\end{aligned} \tag{5.7.2.51}$$

Similarly,

$$\begin{aligned}[\bigwedge^2 T](e_1 \wedge e_3) &:= T(e_1) \wedge T(e_3) \\ &:= (e_1 + 4e_2) \wedge (3e_1 + 6e_2) \\ &= 6e_1 \wedge e_2 + 12e_2 \wedge e_1 \\ &= -6e_1 \wedge e_2.\end{aligned} \tag{5.7.2.52}$$

Finally,

$$\begin{aligned}[\bigwedge^2 T](e_2 \wedge e_3) &:= T(e_2) \wedge T(e_3) \\ &:= (2e_1 + 5e_2) \wedge (3e_1 + 6e_2) \\ &= 12e_1 \wedge e_2 + 15e_2 \wedge e_1 \\ &= -3e_1 \wedge e_2.\end{aligned} \tag{5.7.2.53}$$

Thus,

$$[\bigwedge^2 T]_{\bigwedge^2 \mathcal{C} \leftarrow \bigwedge^2 \mathcal{B}} = \begin{bmatrix} -3 & -6 & -3 \end{bmatrix}. \tag{5.7.2.54}$$

Exercise 5.7.2.55 Check that $\bigwedge^k T = 0$ for $k \geq 3$, so there is nothing further to investigate.

We mentioned in a remark of the definition that minors are secretly determinants of "submatrices". Let us make this precise.

Theorem 5.7.2.56 — Minors as determinants of submatrices. Let V and W be a a finite-dimensional vector space over

a field, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ and $C =: \{c_1, \ldots, c_e\}$ be bases for V and W respectively, and let $T\colon V \to W$ be a linear-transformation. Then, the entry of $[\bigwedge^k T]_{\bigwedge^k C \leftarrow \bigwedge^k \mathcal{B}}$ corresponding to $c_{j_1} \wedge \cdots \wedge c_{j_k} \in \bigwedge^k C$ and $b_{i_1} \wedge \cdots \wedge b_{i_k} \in \bigwedge^k \mathcal{B}$ is the determinant of the $k \times k$ matrix obtained from $[T]_{C \leftarrow \mathcal{B}}$ by removing all the rows except for rows $j_1, \ldots, j_k$ and removing all columns except for columns $i_1, \ldots, i_k$.

R For example, suppose I compute $T(b_2 \wedge b_4 \wedge b_7)$, and when I write this as a linear combination of the elements of $\bigwedge^k C$, I find that the coefficient of $c_1 \wedge c_2 \wedge c_5$ is 20, this means that the determinant of the of the matrix formed from the 2^{nd}, 4^{th}, and 7^{th} columns and the 1^{st}, 2^{nd}, and 5^{th} rows is 20.

Proof. We leave this as an exercise.

Exercise 5.7.2.57 Prove the result.

■

Okay, again, impenetrable. So, again, an example.

▪ **Example 5.7.2.58** Let everything be as it was in Example 5.7.2.47, that is, Let $V := \mathbb{R}^3$, $W := \mathbb{R}^2$, take $\mathcal{B} := \{e_1, e_2, e_2\}$ and $C := \{e_1, e_2\}$ to be the standard bases, and let $T\colon V \to W$ be the linear-transformation defined by the matrix

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}. \tag{5.7.2.59}$$

The 0×0 submatrices are, well, not interesting, at least not to those of us who are not scholars of the empty matrix. The 1×1 submatrices are just the entries of the matrix themselves. Again, not so interesting. There are no square $k \times k$ submatrices

for $k \geq 3$. On the other hand, there are 3 2×2 submatrices:

$$\begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix} \qquad \begin{bmatrix} 1 & 3 \\ 4 & 6 \end{bmatrix} \qquad \begin{bmatrix} 2 & 3 \\ 5 & 6 \end{bmatrix}. \tag{5.7.2.60}$$

The determinant of these matrices are respectively -3, -6, and -3.[a]

On the other hand, recall from Example 5.7.2.47 that we found that

$$[\textstyle\bigwedge^2 T](e_1 \wedge e_2) = -3e_1 \wedge e_2 \tag{5.7.2.61}$$

$$[\textstyle\bigwedge^2 T](e_1 \wedge e_3) = -6e_1 \wedge e_2 \tag{5.7.2.62}$$

$$[\textstyle\bigwedge^2 T](e_2 \wedge e_3) = -3e_1 \wedge e_2. \tag{5.7.2.63}$$

In other words, the $\langle e_1 \wedge e_2, e_1 \wedge e_2 \rangle$ entry of the matrix is -3, the $\langle e_1 \wedge e_2, e_1 \wedge e_3 \rangle$ entry of the matrix is -6, and the $\langle e_1 \wedge e_2, e_2 \wedge e_3 \rangle$ entry of the matrix is -3.[b]

Sure enough, the first matrix in (5.7.2.60) is the one obtained from (5.7.2.59) by only retaining the first and second rows (corresponding to $e_1 \wedge e_2$) and the first and second columns (corresponding to $e_1 \wedge e_2$. The second matrix is the one obtained from (5.7.2.59) by only retaining the first and second rows (corresponding to $e_1 \wedge e_2$) and the first and third columns (corresponding to $e_1 \wedge e_3$). The third matrix is the one obtained from (5.7.2.59) by only retaining the first and second rows (corresponding to $e_1 \wedge e_2$) and the second and third columns (corresponding to $e_2 \wedge e_3$).

Thus, the entries of the 2-minor matrix

$$\begin{bmatrix} -3 & -6 & -3 \end{bmatrix} \tag{5.7.2.64}$$

do correspond to the determinants of the corresponding 2×2 submatrices.

[a] You can of course use the definition, though I (secretly) used facts we have yet to cover "officially"—see Corollary 5.7.2.83 (this tells you how to compute determinants of 2×2 matrices).

[b] Here, "the matrix" refers to the matrix of $\bigwedge^2 T$ with respect to the bases $\bigwedge^2 \mathcal{B}$ and $\bigwedge^2 C$.

Great. Minors. Fantastic. That's all good and dandy, and minors certainly have their uses, but right now we're interested in their relationship to the determinant of the *original* matrix, not submatrices. It turns out that you can calculate the determinant of the entire matrix by summing over products of determinants of submatrices, that is, the minors.

Theorem 5.7.2.65 — Laplace expansion. Let V be a finite-dimensional vector space over a field, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ be a basis for V, let $T\colon V \to V$ be a linear-transformation, and write $A := [T]_{\mathcal{B}}$.

(i). Let $S \subseteq \{1, \ldots, d\}$. Then,

$$\det(A) = \sum_{\substack{X \subseteq \{1,\ldots,d\} \\ |X|=|S|}} \operatorname{sgn}(S) A^S{}_X A^{S^c}{}_{X^c}. \quad (5.7.2.66)$$

(ii). Let $T \subseteq \{1, \ldots, d\}$. Then,

$$\det(A) = \sum_{\substack{X \subseteq \{1,\ldots,d\} \\ |X|=|T|}} \operatorname{sgn}(T) A^X{}_T A^{X^c}{}_{T^c}. \quad (5.7.2.67)$$

R I recommend you just look at an example (Example 5.7.2.69) to understand this.

R See the remark in Theorem 5.5.1.4 to recall the notation $\operatorname{sgn}(S)$ and $\operatorname{sgn}(T)$.

R See the remark in Definition 5.7.2.43 to recall the notation $A^S{}_X$, etc..

Proof. We leave this as an exercise.

Exercise 5.7.2.68 Prove the result.

■

So that's neat. But again, impenetrable. And so again, an example.

■ **Example 5.7.2.69** Define

$$A := \begin{bmatrix} 5 & 4 & 2 & 1 \\ 0 & 1 & -1 & -1 \\ -1 & -1 & 3 & 0 \\ 1 & 1 & -1 & 2 \end{bmatrix}. \tag{5.7.2.70}$$

We compute $\det(A)$ using the Laplace expansion (Theorem 5.7.2.65) of A across the first two rows ($S = \{1, 2\}$ in the notation of Theorem 5.7.2.65).[a]

$$\begin{aligned} \det(A) = &\det\left(\begin{bmatrix} 5 & 4 \\ 0 & 1 \end{bmatrix}\right) \det\left(\begin{bmatrix} 3 & 0 \\ -1 & 2 \end{bmatrix}\right) \\ &- \det\left(\begin{bmatrix} 5 & 2 \\ 0 & -1 \end{bmatrix}\right) \det\left(\begin{bmatrix} -1 & 0 \\ 1 & 2 \end{bmatrix}\right) \\ &+ \det\left(\begin{bmatrix} 5 & 1 \\ 0 & -1 \end{bmatrix}\right) \det\left(\begin{bmatrix} -1 & 3 \\ 1 & -1 \end{bmatrix}\right) \\ &+ \det\left(\begin{bmatrix} 4 & 2 \\ 1 & -1 \end{bmatrix}\right) \det\left(\begin{bmatrix} -1 & 0 \\ 1 & 2 \end{bmatrix}\right) \\ &- \det\left(\begin{bmatrix} 4 & 1 \\ 1 & -1 \end{bmatrix}\right) \det\left(\begin{bmatrix} -1 & 3 \\ 1 & -1 \end{bmatrix}\right) \\ &+ \det\left(\begin{bmatrix} 2 & 1 \\ -1 & -1 \end{bmatrix}\right) \det\left(\begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix}\right) \\ = &\, 5 \cdot 6 - (-5) \cdot (-2) \\ &+ (-5) \cdot (-2) + (-6) \cdot (-2) \\ &- (-5) \cdot (-2) + (-1) \cdot 0 \\ = &\, 32. \end{aligned} \tag{5.7.2.71}$$

[a] We make use of Corollary 5.7.2.83 to do the 2×2 determinants 'in our heads'.

As neat is it may be, I've never seen this general result used, and in fact, have only seen a special case used, which itself is called the *cofactor expansion*. Before we see that, however, we must first introduce *cofactors* themselves.

Definition 5.7.2.72 — Cofactor Let V be a finite-dimensional vector space over a field, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ be a basis for V, let $T\colon V \to V$ be a linear-transformation, and let $1 \leq i, j \leq d$. Then, the $\langle i, j\rangle$***-cofactor***, $\mathrm{Cof}_{\mathcal{B}}(T)_j^{\ i}$ of T with respect to $\mathcal{B}$ is defined by

$$\mathrm{Cof}_{\mathcal{B}}(T)_j^{\ i} := (-1)^{i+j}[\textstyle\bigwedge^{d-1} T]_{\bigwedge^{d-1}\mathcal{B}}^{\ \ \hat{b}_i}{}_{\hat{b}_j}, \tag{5.7.2.73}$$

where

$$\hat{b}_k := b_1 \wedge \cdots \wedge b_{k-1} \wedge b_{k+1} \wedge \cdots \wedge b_d \in \textstyle\bigwedge^{d-1}\mathcal{B}. \tag{5.7.2.74}$$

R If T itself is defined by a matrix A, then we shall simply write $\mathrm{Cof}(A)_i^{\ j} := \mathrm{Cof}_{\mathcal{S}}(T_A)_i^{\ j}$, where T_A is the linear-transformation defined by A and $\mathcal{S}$ is the standard basis.

R In words, (5.7.2.73) says that the $\langle i, j\rangle$-cofactor is obtained by taking the determinant of the $(d-1)\times(d-1)$ submatrices obtained by 'deleting' the i^{th} row and j^{th} column from $[T]_{\mathcal{B}}$ and multiplying the result by $(-1)^{i+j}$—see the following example.

R The signs coming from the $(-1)^{i+j}$ look like, for a 3×3 matrix, for example,

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}. \tag{5.7.2.75}$$

That is, the signs alternate going down rows and across columns starting from + at the top-left. So, for example, the "−" in the $\langle 2, 3\rangle$ entry means that, when you remove the 2^{nd} row and 3^{rd} column and take the determinant, you multiply the result by -1.

R Note the way in which the indices are staggered. To see why it's natural to stagger them in this way, see Corollary 5.7.2.80 and Definition 5.7.2.90.

Again, we should look at an example.

▪ **Example 5.7.2.76** Define

$$A := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}. \tag{5.7.2.77}$$

Suppose we want to compute the $\langle 2, 3\rangle$-cofactor. We start by removing the 2^{nd} row and 3^{rd} column to obtain the matrix

$$\begin{bmatrix} 1 & 2 \\ 7 & 8 \end{bmatrix}. \tag{5.7.2.78}$$

The determinant of this is -6, and hence

$$\mathrm{Cof}(A)_2{}^3 = (-1)^{2+3} \cdot (-6) = 6. \tag{5.7.2.79}$$

Finally, we are able to state how this allows us to compute determinants.

Corollary 5.7.2.80 — Cofactor expansion Let V be a finite-dimensional vector space over a field, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ be a basis for V, let $T\colon V \to V$ be a linear-transformation, write $A := [T]_{\mathcal{B}}$, and let $1 \leq i, j \leq d$. Then,

$$\sum_{k=1}^{d} A^i{}_k \, \mathrm{Cof}(A)_i^k = \det(A) = \sum_{k=1}^{d} A^k{}_j \, \mathrm{Cof}(A)_k{}^j. \tag{5.7.2.81}$$

R The left equality says that we can pick any row of A, and them sum across the row multiplying the entry of A by the corresponding cofactor. The right equality says essentially the same thing, but for columns.

R I have also see this referred to as the Laplace expansion.

Proof. We leave this as an exercise.

Exercise 5.7.2.82 Prove the result.

■

Corollary 5.7.2.83 Let $\mathbb{K}$ be a cring and let $a, b, c, d \in \mathbb{K}$. Then,

$$\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc. \tag{5.7.2.84}$$

Proof. We leave this as an exercise.

Exercise 5.7.2.85 Prove the result.

■

▪ **Example 5.7.2.86** Define

$$A := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}. \tag{5.7.2.87}$$

This theorem says that, using the first *row*,

$$\begin{aligned} \det(A) &= 1 \cdot \det\left(\begin{bmatrix} 5 & 6 \\ 8 & 9 \end{bmatrix}\right) - 2 \cdot \det\left(\begin{bmatrix} 4 & 6 \\ 7 & 9 \end{bmatrix}\right) \\ &\quad + 3 \cdot \det\left(\begin{bmatrix} 4 & 5 \\ 7 & 8 \end{bmatrix}\right) \\ &= 1 \cdot (-3) - 2 \cdot (-6) + 3 \cdot (-3) = 0. \end{aligned} \tag{5.7.2.88}$$

On the other hand, using, for example, the second *column*,

$$\begin{aligned}\det(A) &= -2\cdot\det\left(\begin{bmatrix}4 & 6\\ 7 & 9\end{bmatrix}\right) + 5\cdot\det\left(\begin{bmatrix}1 & 3\\ 7 & 9\end{bmatrix}\right)\\ &\quad - 8\cdot\det\left(\begin{bmatrix}1 & 3\\ 4 & 6\end{bmatrix}\right) \qquad (5.7.2.89)\\ &= -2\cdot(-6) + 5\cdot(-12) - 8\cdot(-6) = 0.\end{aligned}$$

There is one more variant that is sometimes taken as the definition of the determinant that we must cover, but while we're talking about cofactors, it makes sense to discuss the *adjugate matrix*.

Definition 5.7.2.90 — Adjugate Let $\mathbb{F}$ be a field and let A be an $n\times n$ matrix with entries in $\mathbb{F}$. Then, the ***adjugate*** of A, $\mathrm{Adj}(A)$, is defined by

$$\mathrm{Adj}(A) := \mathrm{Cof}(A)^{\dagger}. \qquad (5.7.2.91)$$

R Warning: The "adjugate" is *not* the same as the "adjoint", which we will come to when we study inner-product spaces.

R That is, the adjugate matrix is the transpose of the matrix of cofactors. Incidentally, we see now why the indicates on $\mathrm{Cof}(A)_i^{\ j}$ are staggered the way they are—according to Notation 5.4.2.8, this implies that the indices on $\mathrm{Adj}(A)$ should be staggered like $\mathrm{Adj}(A)^i_{\ j}$. That we want this will be clear when we get to Theorem 5.7.2.92

Theorem 5.7.2.92. Let $\mathbb{F}$ be a field and let A be an $n\times n$ matrix with entries in $\mathbb{F}$. Then,

$$A\,\mathrm{Adj}(A) = \det(A)\,\mathrm{id}_n = \mathrm{Adj}(A)A. \qquad (5.7.2.93)$$

R In particular, if A is invertible, then

$$A^{-1} = \det(A)^{-1} \operatorname{Adj}(A). \tag{5.7.2.94}$$

Proof. We leave this as an exercise.

Exercise 5.7.2.95 Prove the result.

■

Related to this is *Cramer's rule*.

Theorem 5.7.2.96 — Cramer's Rule. Let $\mathbb{F}$ be a field, let A be an invertible $n \times n$ matrix with entires in $\mathbb{F}$, and let $x, b \in \mathbb{F}^n$. Then, if $Ax = b$, it follows that

$$x^k = \frac{\det(A_k)}{\det(A)}, \tag{5.7.2.97}$$

where here A_k is the matrix obtain from A by replacing its k^{th} column with the vector $b \in \mathbb{F}^n$.

Proof. We leave this as an exercise.

Exercise 5.7.2.98 Prove the result.

■

Finally, we return to the last statement that is sometimes taken as the definition of the determinant.[28]

Theorem 5.7.2.99. Let $\mathbb{F}$ be a field and let A be an $n \times n$ matrix with entries in $\mathbb{F}$.

[28] Or rather, the last one that I'll be covering.

(i).

$$\det(A) = \sum_{\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,n\})} \mathrm{sgn}(\sigma) A^{\sigma(1)}{}_1 \cdots A^{\sigma(n)}{}_n.$$

(ii).

$$\det(A) = \sum_{\sigma \in \mathrm{Aut}_{\mathbf{Set}}(\{1,\ldots,n\})} \mathrm{sgn}(\sigma) A^1{}_{\sigma(1)} \cdots A^n{}_{\sigma(n)}.$$

R In words (for (ii)): Pick an entry from every column of A. Multiply these entries, together with possibly a minus sign depending on the order you chose the entries. Add up all the numbers found in this way for each way of picking entries.[a]

(i) is of course similar with the rows and columns switching roles.

[a] Of course, there are many ways (in fact, $n!$ ways) to pick exactly one entry from each column.

Proof. We leave this as an exercise.

Exercise 5.7.2.100 Prove the result.

■

The geometric interpretation of the determinant

In $\mathbb{R}^d$, the determinant can be given a geometric interpretation. The absolute value tells us by how much the volume scales and the sign tells us whether the orientation changes or not.

We begin with the former.

Theorem 5.7.2.101. Let $T\colon \mathbb{R}^d \to \mathbb{R}^d$ be linear and let $S \subseteq \mathbb{R}^d$. Then,

$$\text{vol}(T(S)) = |\det(T)|\,\text{vol}(S), \tag{5.7.2.102}$$

where $\text{vol}(S)$ is the Lebesgue measure of S.

R You don't need to know the precise definition of Lebesgue measure to understand the meaning of this statement (or even to use it). Lebesgue measure is a generalization of volume to any subset of $\mathbb{R}^d$, but the interpretation is really still just "volume".[a] Certainly, it gives you the answer you would expect for any set of which you thought you previously knew the volume.

For example, if S is the "unit cube", then this statement reads $\text{vol}(T(S)) = |\det(T)|$—no specific knowledge of Lebesgue measure required.

R Yes, S can be *any* set, measurable or not (though in this case it's usually called Lebesgue *outer* measure).

[a] Though for $d = 1$ and $d = 2$, this is more commonly referred to as "length" and "area" respectively. Additionally, people might say "hyper-volume" for $d \geq 4$.

Proof. We leave this as an exercise.

Exercise 5.7.2.103 Prove the result.

■

So that's what the absolute value of the determinant means. It turns out that the sign tells you what happens to the orientation. To state this result, however, we had first better way what we actually mean by "orientation".

Definition 5.7.2.104 — Volume form Let V be a d-dimensional vector space over a field. Then, a ***volume form*** on V is a nonzero element of $\bigwedge_d V$.

R Note how this is a *covariant* tensor. For our purposes, we could have used contravariant, but for reasons having to do with calculus, "volume form" refers to a, well, a *form*—see the remark in Definition 5.5.2.1.

Proposition 5.7.2.105 — Orientation Let V be a d-dimensional real vector space, let $\omega_1, \omega_2 \in \bigwedge^d V$ be volume forms, and let us say that $\omega_1 \sim \omega_2$ iff there is some $a > 0$ such that $\omega_1 = a\omega_2$. Then, $\sim$ is an equivalence relation on the volume forms on V.

R An ***orientation*** of V is an equivalence class of volume forms on V.

R The intuition is roughly that a choice of ordered basis should give an orientation. Given such an ordered basis $\{b_1, \dots, b_d\}$, this determines the volume form $b_1 \wedge \cdots \wedge b_d \in \bigwedge^d V$. Intuitively, if we swap the order of two basis elements, this should change the orientation.[a] As swapping two basis elements changes the sign of this volume form, we are lead to declaring two volume forms to be equivalent iff they are a scalar multiple of one another.[b]

[a] In two dimensions, imagining your copy of $\mathbb{R}^2$ embedded in $\mathbb{R}^3$, you can think of an orientation as a choice of which side of the plane counts as "up". This is determined by picking an ordered basis of $\mathbb{R}^2$ and using the right-hand rule to the "up" direction. Because of how the right-hand rule works, if you swap the order of these two vectors, you're going to change the "up" direction.

[b] Note that, as $\dim(\bigwedge^d V) = 1$, they have to be scalar multiples of one another—it is then just an issue of whether or not that scalar multiple if positive or negative.

Proof. We leave this as an exercise.

Exercise 5.7.2.106 Prove the result.

■

Definition 5.7.2.107 — Oriented An ***oriented vector space*** is a finite-dimensional real vector space V together with an orientation $\omega/\sim$ on V.

As now we can state the theorem giving the relationship between orientation and the sign of the determinant.

Theorem 5.7.2.108. Let $\langle V, \omega/\sim\rangle$ be an oriented vector space and let $T: V \to V$ be linear. Then, $[\bigwedge_d T^\dagger](\omega)/\sim = \omega/\sim$ iff $\det(T) > 0$.

R T sends the original orientation $\omega/\sim$ to a new orientation $[\bigwedge_d T^\dagger](\omega)/\sim$. Thus, this is the statement that $\det(T) > 0$ iff T "preserves" the orientation.

R Up until now, we have only been dealing with the contravariant versions $\bigwedge^k T$. Here, we need to use the covariant version $\bigwedge_d T^\dagger$ as ω is a covariant tensor.

Proof. We leave this as an exercise.

Exercise 5.7.2.109 Prove the result.

■

The characteristic polynomial

Let V be a finite-dimensional vector space over a field $\mathbb{F}$, let $T: V \to V$ be linear, and let $\lambda \in \mathbb{F}$. From the last chapter, hopefully you have no trouble remembering that λ is an eigenvalue of T iff $\mathrm{Ker}(T - \lambda) \neq 0$. This is of course the statement that $T - \lambda$ is *not* injective, which, as we are in finite dimensions, is equivalent to the statement that $T - \lambda$

is *not* invertible. But we've just discovered that (Corollary 5.7.2.31) $T - \lambda$ is not invertible iff $\det(T - \lambda) = 0$. Hm. I wonder what happens if we try to compute $\det(T - \lambda)$.

Theorem 5.7.2.110 — Characteristic polynomial. Let V be a d-dimensional vector space over a field $\mathbb{F}$, let $T\colon V \to V$ be linear, let $\lambda \in \mathbb{F}$. Then,

$$\det(T - \lambda) = \sum_{k=0}^{d} (-1)^k \operatorname{tr}(\textstyle\bigwedge^{d-k} T)\lambda^k. \tag{5.7.2.111}$$

R

$$p_{\text{char},T}(\lambda) \coloneqq \det(T - \lambda) \tag{5.7.2.112}$$

is the ***characteristic polynomial*** of T. As per usual, we shall write $p_{\text{char}} \coloneqq p_{\text{char},T}$ if T is clear from context.

R

In particular, note that the coefficient of λ^d is $(-1)^d$, the coefficient of λ^{d-1} is $(-1)^{d-1}\operatorname{tr}(T)$, and the constant term is $\det(T)$.

In general, the coefficient of λ^k is, up to a sign, the trace of the matrix of $(d-k)$-minors, though this isn't quite as useful for other values of k.

R

Warning: Some others take the characteristic polynomial to be $\det(\lambda - T)$ instead. Of course, these are the same up to a minus sign, and so it makes no difference. The advantage this other definition has is that the resulting polynomial is always monic. I chose the convention I did because I find it just slightly more natural—we've written $T - \lambda$ everywhere else, wouldn't it be just a teensy bit weird to make an exception here and write $\lambda - T$?

Proof. For convenience, replacing λ with $-\lambda$, we instead show that

$$\det(T+\lambda) = \sum_{k=0}^{d} \operatorname{tr}(\textstyle\bigwedge^{d-k} T)\lambda^k. \tag{5.7.2.113}$$

So, let $\mathcal{B} =: \{b_1, \dots, b_d\}$ be a basis of V. Then, for $0 \le k \le d$, by Proposition 5.5.3.24,

$$\textstyle\bigwedge^k \mathcal{B} = \{b_S : S \subseteq \{1, \dots, d\}, |S| = k\} \tag{5.7.2.114}$$

is a basis of $\bigwedge^k V$, where

$$b_S \coloneqq \bigwedge_{i \in S} b_i, \tag{5.7.2.115}$$

where the wedge product is taken in order of increasing i. As this is a basis, we can speak of coordinates, and so let us abbreviate

$$[T]^S{}_T \coloneqq [\textstyle\bigwedge^k T]_{\bigwedge^k \mathcal{B}}{}^S{}_T, \tag{5.7.2.116}$$

where $S, T \subseteq \{1, \dots, d\}$ with $|S| = k = |T|$. That is, $[T]^S{}_T$ is the coefficient of b_S when you write $[\bigwedge^k T](b_T)$ as a linear-combination of the elements of $\bigwedge^k \mathcal{B}$. Thus,

$$\operatorname{tr}(\textstyle\bigwedge^k T) = \displaystyle\sum_{\substack{S \subseteq \{1,\dots,d\} \\ |S|=k}} [T]^S{}_S. \tag{5.7.2.117}$$

Also note that

$$[\textstyle\bigwedge^k T](b_S) \wedge b_{S^c} = \operatorname{sgn}(S)[T]^S{}_S b_1 \wedge \cdots \wedge b_d,{}^a \tag{5.7.2.118}$$

for, upon writing $[\bigwedge^k T](b_S)$ as a linear-combination of elements of $\bigwedge^k \mathcal{B}$, we see that all the b_T-term will vanish when you take the wedge product with b_{S^c} unless b_T and b_{S^c} have no factors in common.[b]

Using this, we see that

$$\begin{aligned}
&[\textstyle\bigwedge^d[T+\lambda]](v_1\wedge\cdots\wedge v_d)\\
&\quad:=[[T+\lambda](v_1)]\wedge\cdots\wedge[[T+\lambda](v_d)]\\
&\quad:=(T(v_1)+\lambda v_1)\wedge\cdots\wedge(T(v_d)+\lambda v_d)\\
&\quad=\sum_{k=0}^{d}\lambda^k\left[\sum_{\substack{S\subseteq\{1,\dots,d\}\\|S|=k-d}}\operatorname{sgn}(S)[\textstyle\bigwedge^k T](b_S)\wedge b_{S^c}\right]\\
&\quad=\sum_{k=0}^{d}\lambda^k\left[\sum_{\substack{S\subseteq\{1,\dots,d\}\\|S|=k-d}}\operatorname{sgn}(S)^2[T]^S{}_S b_1\wedge\cdots\wedge b_d\right]\\
&\quad=\left(\sum_{k=0}^{d}\lambda^k\operatorname{tr}(\textstyle\bigwedge^{d-k}T)\right)b_1\wedge\cdots\wedge b_d,
\end{aligned}$$

and hence

$$\det(T+\lambda)=\sum_{k=0}^{d}\operatorname{tr}(\textstyle\bigwedge^{d-k}T)\lambda^k, \tag{5.7.2.119}$$

as desired. ■

[a] The $\operatorname{sgn}(S)$ (Theorem 5.5.1.4) arises as a result of taking all the factors of b_S and of b_{S^c} and putting them 'in order' to yield $b_1\wedge\cdots\wedge b_d$.

[b] This of course, from the definition (5.7.2.115), is true iff $T=S$.

Theorem 5.7.2.120. Let V be a d-dimensional vector space over a field $\mathbb{F}$ with algebraic closure $\mathbb{A}$ and let $T\colon V\to V$ be linear. Then,

$$p_{\text{char}}(x)=(-1)^d\prod_{\lambda\in\operatorname{Eig}(T^{\mathbb{A}})}(x-\lambda)^{d_\lambda}, \tag{5.7.2.121}$$

where $d_\lambda:=\dim(\operatorname{Eig}^\infty_{\lambda,T^{\mathbb{A}}})$.

R In particular, for $\lambda\in\mathbb{F}$, $\lambda\in\operatorname{Eig}(T)$ iff $p_{\text{char}}(\lambda)=0$.

This is by far the most common ways, and often the most practical way, to compute the eigenvalues of a matrix.[a]

Compute p_{char} as $\det(T - \lambda)$. Set the result equal to 0. Solve for λ. Your solutions are then the eigenvalues of T.

[a] Though for linear-transformations that are not matrices, you'll often just want to start from the definition of eigenvalue.

Proof. This follows immediately from Theorem 5.7.2.26 by replacing T with $T - \lambda$. ■

Corollary 5.7.2.122 — Cayley-Hamilton Theorem Let V be a finite-dimensional vector space over a field and let $T : V \to V$ be linear. Then,

$$p_{\text{char}}(T) = 0. \tag{5.7.2.123}$$

R In fact, it follows from Theorem 4.5.1 (the defining result of the minimal polynomial) that p_{min} divides p_{char}.

Proof. Let $\mathbb{F}$ be the ground field of V and let $\mathbb{A}$ be an algebraic-closure of $\mathbb{F}$. By Proposition 4.5.18, we have that

$$p_{\text{min}}(x) = \prod_{\lambda \in \text{Eig}(T^{\mathbb{A}})} (x - \lambda)^{n_\lambda}, \tag{5.7.2.124}$$

where n_λ is the size of the largest Jordan block with eigenvalue λ appearing in the Jordan canonical form of $T^{\mathbb{A}}$. In particular, $n_\lambda \leq \dim(\text{Eig}^{\infty}_{\lambda, T^{\mathbb{A}}})$. By the definition of the minimal

polynomial, we certainly have that

$$p_{\min}(T) = 0. \tag{5.7.2.125}$$

Then, from the previous result, as $n_\lambda \leq \dim(\mathrm{Eig}_{\lambda,T^{\mathbb{A}}})$, it follows that

$$p_{\mathrm{char}}(T) = 0. \tag{5.7.2.126}$$

■

As you may already be aware, one of the most important applications of the characteristic polynomial is in the computation of eigenvalues (of matrices).[29] Let us return to the matrix of Example 4.5.30 where we more or less just told you what the eigenvalues were.

▪ **Example 5.7.2.127** As in Example 4.5.30, define

$$A := \begin{bmatrix} 5 & 4 & 2 & 1 \\ 0 & 1 & -1 & -1 \\ -1 & -1 & 3 & 0 \\ 1 & 1 & -1 & 2 \end{bmatrix}, \tag{5.7.2.128}$$

so that

$$A - \lambda := \begin{bmatrix} 5-\lambda & 4 & 2 & 1 \\ 0 & 1-\lambda & -1 & -1 \\ -1 & -1 & 3-\lambda & 0 \\ 1 & 1 & -1 & 2-\lambda \end{bmatrix}. \tag{5.7.2.129}$$

[29] If your linear-transformation is not defined by a matrix or a matrix cannot be easily be computed for it, please, for the love of `insert nonexclusive deity reference here`, just use the definition. For example, if I ask you to find the eigenvalues of the derivative operator, don't try to take the determinant of $\frac{\mathrm{d}}{\mathrm{d}x} - \lambda$ or something crazy like that.

Using the cofactor expansion along the first column, we compute

$$\begin{aligned}
\det(A-\lambda) &= (5-\lambda)\cdot\det\left(\begin{bmatrix}1-\lambda & -1 & -1\\ -1 & 3-\lambda & 0\\ 1 & -1 & 2-\lambda\end{bmatrix}\right)\\
&\quad -1\cdot\det\left(\begin{bmatrix}4 & 2 & 1\\ 1-\lambda & -1 & -1\\ 1 & -1 & 2-\lambda\end{bmatrix}\right)\\
&\quad -1\cdot\det\left(\begin{bmatrix}4 & 2 & 1\\ 1-\lambda & -1 & -1\\ -1 & 3-\lambda & 0\end{bmatrix}\right)\\
&= (5-\lambda)\cdot\left(-1\cdot\det\left(\begin{bmatrix}-1 & 3-\lambda\\ 1 & -1\end{bmatrix}\right)+(2-\lambda)\cdot\det\left(\begin{bmatrix}1-\lambda & -1\\ -1 & 3-\lambda\end{bmatrix}\right)\right)\\
&\quad -\left(4\cdot\det\left(\begin{bmatrix}-1 & -1\\ -1 & 2-\lambda\end{bmatrix}\right)-2\cdot\det\left(\begin{bmatrix}1-\lambda & -1\\ 1 & 2-\lambda\end{bmatrix}\right)\right.\\
&\qquad \left.+1\cdot\det\left(\begin{bmatrix}1-\lambda & -1\\ 1 & -1\end{bmatrix}\right)\right)\\
&\quad -\det\left(1\cdot\det\left(\begin{bmatrix}1-\lambda & -1\\ -1 & 3-\lambda\end{bmatrix}\right)+1\cdot\det\left(\begin{bmatrix}4 & 2\\ -1 & 3-\lambda\end{bmatrix}\right)\right)\\
&= (5-\lambda)\cdot(-(1-(3-\lambda))+(2-\lambda)\cdot((1-\lambda)(3-\lambda)-1))\\
&\quad -(4\cdot(-(2-\lambda)-1)-2\cdot((1-\lambda)(2-\lambda)+1)+(-(1-\lambda)+1))\\
&\quad -(((1-\lambda)(3-\lambda)-1)+(4(3-\lambda)+2))\\
&= \lambda^4-11\lambda^3+42\lambda^2-64\lambda+32\\
&= (\lambda-1)(\lambda-2)(\lambda-4)^2.
\end{aligned}$$

Thus, this matrix has three distinct eigenvalues, 1, 2, and 4, with respective multiplicities 1, 1, and 2.

5.8 Bilinear and quadratic forms

We end this chapter with a discussion of what are called *bilinear forms* and *quadratic forms*. Our interest comes from the fact that all metric furnish examples of bilinear forms.

5.8.1 Basic definitions

Definition 5.8.1.1 — Bilinear form Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule. Then, a ***bilinear form*** on V is a bilinear map $(\cdot \mid \cdot)\colon V \times V \to \mathbb{K}$.

R Thus, a bilinear form is just a dual-pair in which both spaces are the same. In this language then, a metric on V is a nonsingular symmetric bilinear form on V.

The term "bilinear form" is common, but often times I will simply say "Let $(\cdot \mid \cdot)\colon V \times V \to \mathbb{K}$ be bilinear. . . ". A lot of the time, the extra word "form" is unnecessary (it's only necessary when for some reason it's not clear what the domain of the pairing is).

Definition 5.8.1.2 — Quadratic form Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule. Then, a ***quadratic form*** on V is a function $Q\colon V \to \mathbb{K}$ of the form $Q(v) = (v \mid v)$ for $(\cdot \mid \cdot)\colon V \times V \to \mathbb{K}$ symmetric and bilinear.

Theorem 5.8.1.3 — Quadratic forms are 'the same' as symmetric bilinear forms. Let V be a $\mathbb{K}$-$\mathbb{K}$-bimodule and let $Q\colon V \times V \to \mathbb{K}$ be a quadratic form on V. Then, if $2 \in \mathbb{K}$ is a unit,

$$(v \mid w) \coloneqq \frac{1}{2}\left(Q(v+w) - Q(v) - Q(w)\right) \tag{5.8.1.4}$$

is the unique symmetric bilinear form on V such that $Q(v) = (v \mid v)$ for all $v \in V$.

R Every symmetric bilinear form $(\cdot \mid \cdot)$ of course determines a quadratic form $Q(v) \coloneqq (v \mid v)$ by definition. This result says that, under the mild hypothesis that $2 \in \mathbb{K}$ is a unit, every quadratic form in turn defines a *unique* symmetric bilinear form.

R For this reason, I will mostly not work with quadratic forms themselves, and shall simply stick to a study of symmetric bilinear forms (and bilinear forms in

general). This only makes a difference if 2 is not a unit anyways, and which is not often an issue. An exception, however, is when it comes to diagonalization: we will see that quadratic forms are always diagonalizable but symmetric bilinear forms are only diagonalizable if 2 is a unit—see Theorem 5.8.3.3.

Proof. We first check that $(\cdot \mid \cdot)$ is in fact bilinear (it is manifestly symmetric). By definition, there is some symmetric bilinear $B\colon V \times V \to \mathbb{K}$ such that $Q(v) = B(v, v)$. Using this, we find

$$\begin{aligned}(v\,,\, w) &:= \frac{1}{2}\left(B(v+w, v+w) - B(v,v) - B(w,w)\right)\\ &= \frac{1}{2}\left(B(v,v) + 2B(v,w) + B(w,w)\right.\\ &\qquad \left. -B(v,v) - B(w,w)\right)\\ &= B(v,w).\end{aligned} \tag{5.8.1.5}$$

This shows that that $(\cdot \mid \cdot)$ is bilinear.

We next check that

$$\begin{aligned}(v \mid v) &:= \frac{1}{2}\left(B(v+v, v+v) - B(v,v) - B(v,v)\right)\\ &= \frac{1}{2}\left(4B(v,v) - 2B(v,v)\right) = B(v,v) = Q(v).\end{aligned} \tag{5.8.1.6}$$

To show uniqueness, low let $\langle \cdot | \cdot \rangle\colon V \times V \to \mathbb{K}$ be symmetric bilinear and such that $\langle v | v \rangle = Q(v)$. Then,

$$\begin{aligned}\langle v | w \rangle &= \frac{1}{2}\left(\langle v+w | v+w \rangle - \langle v | v \rangle - \langle w | w \rangle\right)\\ &= \frac{1}{2}(Q(v+w) - Q(v) - Q(w)) =: (v \mid w).\end{aligned} \tag{5.8.1.7}$$

■

Exercise 5.8.1.8 Give an example of a vector space V over $\mathbb{Z}/2\mathbb{Z}$ and two distinct symmetric bilinear maps

$(\cdot\,|\,\cdot), \langle\cdot|\cdot\rangle : V \times V \to \mathbb{K}$ such that

$$(v\,|\,v) = \langle v|v\rangle \tag{5.8.1.9}$$

for all $v \in V$.

R In other words, find a counter-example to the previous result in characteristic 2.

5.8.2 Bilinear forms and matrices

Bilinear forms are of course bilinear maps, and as such, in index notation will be written as B_{ab}. This suggests that, upon picking a basis, one will obtain a double-indexed array of scalars B_{ij}, $1 \leq i, j \leq \dim(V)$. This is indeed the case, and the other way around, matrices can be used to define bilinear forms. We stress caution, however, as matrices cannot tell the difference between a $\langle 0, 2\rangle$ tensor (a bilinear form) or a $\langle 1, 1\rangle$ tensor (a linear transformation) (not to mention $\langle 2, 0\rangle$ tensors). Nevertheless, matrices remain the most convenient way to define bilinear forms.

Proposition 5.8.2.1 — Bilinear form of a matrix Let $\mathbb{K}$ be a ring and let A be an $m \times m$ matrix with entries that are central in $\mathbb{K}$. Then, $B_A \in \bigotimes_2 \mathbb{K}^n$, the ***bilinear form defined by*** A, defined by

$$v^a [B_A]_{ab} w^b := \sum_{i,j=1}^{n} v^i A_{ij} w^j \tag{5.8.2.2}$$

is bilinear.

Furthermore,

(i). B_A is symmetric iff $A_{ij} = A_{ji}$ for all $1 \leq i, j \leq n$; and
(ii). B_A is nonsingular iff B_A is nondegenerate iff $\det(A) \neq 0$.

R Note how we have staggered our indices on A_{ij} different than normally. This is to suggest that this matrix is supposed to defined a bilinear form, not a linear-transformation.

R We require that the entries of A be central so that $B_A(v\alpha, w) = B_A(v, \alpha w)$.

Proof. We leave this as an exercise.

Exercise 5.8.2.3 Prove the result.

■

The other way around, we can associate a matrix to a given bilinear form given a choice of basis.

Theorem 5.8.2.4 — Coordinates (of a bilinear form). Let V be a $\mathbb{K}$-module, $\mathbb{K}$ a cring, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ be a basis for V, and let $B\colon V \times V \to \mathbb{K}$ be a bilinear form. Then, there is a unique $d \times d$ matrix, $[B]_{\mathcal{B}}$, the ***coordinates*** of B with respect to the basis $\mathcal{B}$ such that

$$v^a B_{ab} w^b = \sum_{i,j=1}^{d} v^i \, [[B]_{\mathcal{B}}]_{ij} \, w^j \tag{5.8.2.5}$$

for all $v, w \in V$.

Furthermore, explicitly,

$$[B]_{\mathcal{B}ij} = B(b_i, b_j). \tag{5.8.2.6}$$

R There are of course analogues for tensors of arbitrary rank. We hesitate to present them because of their limited usefulness. For rank at least 4, the arrays of numbers become essentially impossible to write down on a sheet of paper, and for rank 3 it's still quite difficult. Even in the rank 2 case, there is always the issue that a matrix can't distinguish between $\langle 1, 1\rangle$, $\langle 2, 0\rangle$, and $\langle 0, 2\rangle$ tensors. Still, given its usefulness in this context, we reluctantly present the result for bilinear forms.

R This doesn't seem to work in the noncommutative case as there is no way of guaranteeing that the entries of $[B]_{\mathcal{B}}$ be central (which we need in order for B to be bilinear.

R $[\cdot]_{\mathcal{B}}\colon \bigotimes_2 V \to \mathrm{Matrix}_2(\mathbb{K})$ is an isomorphism and satisfies $[B_A]_{\mathcal{S}} = A$, where $\mathcal{S}$ is the standard basis of $\mathbb{K}^n$. There are the direct analogues of Propositions 3.2.2.16 and 3.2.2.30. We don't bother reproducing what are essentially carbon copies of previous results here.

Proof. We leave this as an exercise.

Exercise 5.8.2.7 Prove the result.

■

5.8.3 Diagonalizable bilinear forms

Definition 5.8.3.1 — Diagonalizable (bilinear form) Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and $B\colon V \times V \to \mathbb{F}$ be bilinear. Then, T is ***diagonalizable*** iff there is a basis $\mathcal{B}$ of V such that $[B]_{\mathcal{B}}$ is a diagonal matrix.

R In this case, $[B]_{\mathcal{B}}$ is the ***diagonalization*** of B with respect to $\mathcal{B}$.

R Warning: Unlike the case of linear-transformations, where the diagonalizations were unique up to permutation of the diagonal elements, this is *not* the case for diagonalizations of bilinear forms. For example, if I replace b with $\alpha \cdot b$ in $\mathcal{B}$, while this would have no effect for the diagonalization of a linear-transformation, this changes the corresponding diagonal element of $[B]_{\mathcal{B}}$ by a factor of α^2—see (5.8.2.6).

R Note that diagonalizable bilinear forms are automatically symmetric (because diagonal matrices are symmetric).

Note also that this did *not* make sense for linear-transformations as there is no notion of what it means for a linear-transformation to be symmetric.[a]

[a] Unless you have extra structure around, like a metric, in which case you can say that the linear-transformation is symmetric iff the associated bilinear form is.

Definition 5.8.3.2 — Diagonalizable (quadratic form) Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and let $Q\colon V \to \mathbb{F}$ be a quadratic form. Then, Q is ***diagonalizable*** iff there is a diagonalizable symmetric bilinear $(\cdot \mid \cdot)\colon V \times V \to \mathbb{F}$ such that $Q(v) = (v \mid v)$.

There is a relatively simple characterization of diagonalizable bilinear forms, analogous to Theorem 4.3.5 for linear-transformations.

Theorem 5.8.3.3. Let V be a finite-dimensional vector space over a field $\mathbb{F}$, let $B\colon V \times V \to \mathbb{F}$ be a bilinear form, and let $Q\colon V \to \mathbb{F}$ be a quadratic form.

(i). If $\mathrm{Char}(\mathbb{F}) \neq 2$, then B is diagonalizable iff it is symmetric.

(ii). Q is diagonalizable.

R (i) most definitely fails if $\mathrm{Char}(\mathbb{F}) = 2$—see the following counter-example.

R Note how different this criterion is from the one for linear-transformations (Theorem 4.3.5).

Proof. We leave this as an exercise.

Exercise 5.8.3.4 Prove the result.

R Hint: See [HJS02, Theorem 6.35].

■

▪ **Example 5.8.3.5 — A symmetric bilinear from that is not diagonalizable** [a] Define $\mathbb{F} := \mathbb{Z}/2\mathbb{Z}$, $V := \mathbb{F}^2$, and let $B_A : V \times V \to \mathbb{F}$ be the bilinear form defined by the matrix

$$A := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{5.8.3.6}$$

B_A is symmetric as $A_{ij} = A_{ji}$.

Exercise 5.8.3.7 Show that B_A is not diagonalizable.

[a] Adapted from [HJS02, Example 6.8.5].

We have an analogue of Proposition 4.3.1.1 which gives the relationship between a matrix that defines a linear-transformation and its diagonalization.

Proposition 5.8.3.8 Let A be an $m \times m$ matrix with entries in a field $\mathbb{F}$, let $B_A : V \times V \to \mathbb{F}$ be the corresponding bilinear map, and let $\mathcal{B}$ be a diagonalizing basis for B_A. Then,

$$[B_A]_{\mathcal{B}} = [id]_{\mathcal{S}\leftarrow\mathcal{B}}{}^{\dagger} [B_A]_{\mathcal{S}} [\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}, \tag{5.8.3.9}$$

where $\mathcal{S}$ is the standard basis of $\mathbb{F}^m$.

R Note that $[B_A]_{\mathcal{S}} = A$ by Theorem 5.8.2.4.

Furthermore, $[B_A]_{\mathcal{B}}$ is the diagonalization of B_A (by definition). Thus, writing $D := [B_A]_{\mathcal{B}}$ and $P := [\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}}$, this equation is sometimes written more concisely (but perhaps less transparent) as

$$D = P^{\dagger} A P. \tag{5.8.3.10}$$

Compare (4.3.1.3).

R One can see how this should be $P^\dagger$ (instead of P or P^{-1}) by writing this in index notation. It should be clearer in index notation that

$$D_{ij} = P_i{}^x A_{xy} P^y{}_j.^a \tag{5.8.3.11}$$

But in terms of matrices, this is just $D = P^\dagger AP$.

Indeed, I would argue that we should really be writing (5.8.3.9) in terms of indices in the first place—matrix multiplication is suggestive of composition, and that's not really what's going on (it's contraction, not composition).

[a] You can figure this out using heuristics: there are only so many ways to combine these indices in such a way that makes sense. Indicentally, this is one case where writing indices on the left might make this even more obvious: $D_{ij} = {}_i P^x A_{xy}{}^y P_j$.

Proof. We leave this as an exercise.

Exercise 5.8.3.12 Prove the result.

■

For linear-transformations, to actually compute the diagonalization, we compute the eigenvalues and eigenvectors. Then, D would be diagonal with eigenvalues along the diagonal and P would be the matrix whose columns were the corresponding eigenvectors of A. We now investigate how to compute the diagonalization and relate it to the original symmetric bilinear form.

Theorem 5.8.3.13. Let $\mathbb{F}$ be a field, let A be a symmetric $m \times m$ matrix with entries in $\mathbb{F}$, and let R: $\text{Matrix}_m(\mathbb{F}) \to \text{Matrix}_m(\mathbb{F})$ be any composition of row operations such that $R(A)$ is upper-triangular. Then, $E_R A E_R^\dagger$ is a diagonalization

of $B_A : \mathbb{F}^m \times \mathbb{F}^m \to \mathbb{F}$ with respect to the basis given by the columns of $E_R^\dagger$, where E_R is the elementary matrix of R.

R In practice, this is used as follows. Take the matrix A and "augment" it with the identity matrix $\mathrm{id}_{m\times m}$ to form an $m \times 2m$ matrix as follows.

$$\left[A \;\middle|\; \mathrm{id}_{m\times m}\right] \tag{5.8.3.14}$$

Now, "row-column-reduce" this until you obtain a diagonal matrix on the left, but, while doing so, only before the *row* operations to the right hand side. Then, what pops out on the right is R.

R Recall that (Theorem 3.2.1.62) E_R is the unique matrix such that $R(X) = E_R X$ for all matrices $X \in \mathrm{Matrix}_m(\mathbb{F})$.

Proof. We leave this as an exercise.

Exercise 5.8.3.15 Prove the result.

■

What follows is an example of how to use this in practice.

■ **Example 5.8.3.16** [a] Take $\mathbb{F} := \mathbb{R}$ and define

$$A := \begin{bmatrix} 1 & -1 & 3 \\ -1 & 2 & 1 \\ 3 & 1 & 1 \end{bmatrix}. \tag{5.8.3.17}$$

Augment this to form

$$\left[\begin{array}{ccc|ccc} 1 & -1 & 3 & 1 & 0 & 0 \\ -1 & 2 & 1 & 0 & 1 & 0 \\ 3 & 1 & 1 & 0 & 0 & 1 \end{array}\right]. \tag{5.8.3.18}$$

Adding the first column to the second, we obtain[b]

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ -1 & 1 & 1 & 0 & 1 & 0 \\ 3 & 4 & 1 & 0 & 0 & 1 \end{array}\right]. \tag{5.8.3.19}$$

Adding the first row to the second, we obtain[c]

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 1 & 1 & 0 \\ 3 & 4 & 1 & 0 & 0 & 1 \end{array}\right]. \tag{5.8.3.20}$$

We continue similarly:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 4 & 1 & 1 & 0 \\ 3 & 4 & -8 & 0 & 0 & 1 \end{array}\right] \tag{5.8.3.21}$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 4 & 1 & 1 & 0 \\ 0 & 4 & -8 & -3 & 0 & 1 \end{array}\right] \tag{5.8.3.22}$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 4 & -24 & -3 & 0 & 1 \end{array}\right] \tag{5.8.3.23}$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & -24 & -7 & -4 & 1 \end{array}\right] \tag{5.8.3.24}$$

According to this, we should have that

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -24 \end{bmatrix} = P^{\dagger} A P, \tag{5.8.3.25}$$

where

$$P := \begin{bmatrix} 1 & 1 & -7 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}, \tag{5.8.3.26}$$

and you can verify that this is indeed the case by a computation.

[a] Adapted from [HJS02, Example 6.8.6].
[b] Note how we did *not* do anything to the right-hand side.
[c] Note how we *did* do the same thing to the right-hand side this time.

5.8.4 Sylvester's Law of Inertia

We mentioned before that diagonalizations of bilinear forms are not necessarily unique, as, upon scaling a basis element by α, the corresponding diagonal element gets scaled by α^2. *Sylvester's Law of Inertia* tells us to what extent we can obtain uniqueness over the real numbers. As the set of real numbers that are squares are precisely the nonnegative real numbers, one would expect that we can always choose a basis in which the diagonal elements are either 1, −1, or 0.[30]

Theorem 5.8.4.1 — Sylvester's Law of Inertia. Let V be a finite-dimensional real vector space and let $B\colon V \times V \to \mathbb{R}$ be symmetric bilinear. Then, there is a basis $\mathcal{B}$ of V such that $[B]_{\mathcal{B}}$ is a diagonal matrix whose diagonal entries are all +1, −1, or 0.

Furthermore, the number of diagonal entries which are +1, −1, and 0 are all independent of the choice of $\mathcal{B}$.

R The number of +1s on the diagonal is the ***positive index of inertia*** m_+ and the number of −1s on the diagonal is the ***negative index of inertia*** m_-. The number of 0s on the diagonal, m_0, is equal to the

[30] If the entry on the diagonal was previously $a \neq 0$, scale the corresponding basis element by $\frac{1}{\sqrt{|a|}}$.

dimension of the kernel of the map $V \to V^\dagger$, $v^a \mapsto B_{ab}v^b$. $\langle n_0, n_+, n_- \rangle$ is the ***signature*** of B.[a]

R Thus, there is a basis $\mathcal{B} =: \{b_1, \ldots, b_d\}$ such that $B(b_i, b_j) = 0$ if $i \neq j$ and $B(b_i, b_i) = \pm 1$ otherwise. Such a basis is sometimes said to be an *orthonormal* basis for B.

R Essentially the same thing is true over $\mathbb{C}$, except now there will only be $+1$ and 0 on the diagonal. This essentially follows from the fact that we can now scale the diagonal elements by -1, as this is a square ($-1 = \mathrm{i}^2$) in $\mathbb{C}$.

[a] Some authors take $n_- - n_+$ to be the ***signature***.

Proof. We leave this as an exercise.

Exercise 5.8.4.2 Prove the result.

R Hint: See [HJS02, Theorem 6.38].

■

5.9 Summary

The subject of study of this chapter was multilinear maps, the motivation for which came from differentiation (where the higher derivatives are multilinear maps in the tangent vectors). This in turn motivated us to introduce two concepts: the dual-space and the tensor product.

The dual-space of V is defined to be $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, \mathbb{K})$, the set of all linear maps from V to $\mathbb{K}$ (Definition 5.2.1.1)

The tensor product of two modules $V \times W$ was defined so that bilinear maps $V \times W \to U$ are 'the same as' $V \otimes W \to U$.

Together, these two constructions allowed us to reduce the study of multilinear maps to the study of linear maps (between tensor products of V and V^*). Be sure to take a look at Subsection 5.4.5, which

contains a more detailed summary of what we did with tensors in index notation.

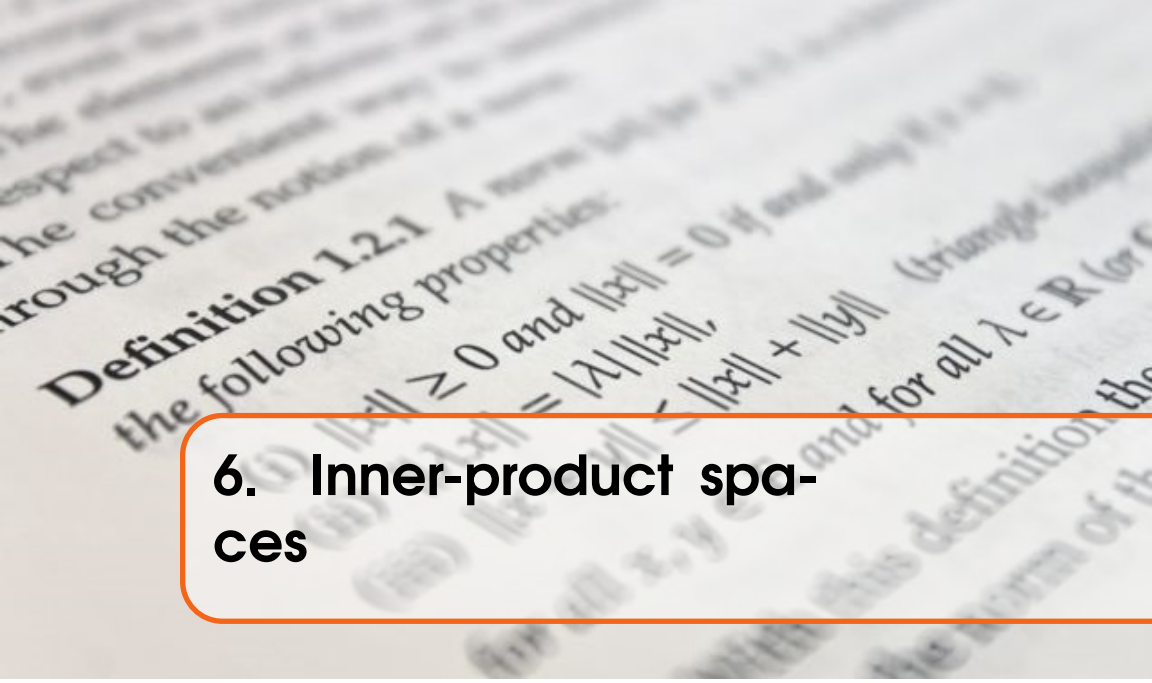
We then turned to a study of the determinant (which necessitated a discussion of antisymmetric tensors and extension of scalars). The determinant wound up being the unique scalar $\det(T)$ such that $\bigwedge^d T = \det(T)$, where d is the dimension of the underlying vector space. While we were at it, we were able to define the trace as $\operatorname{tr}(T) \coloneqq T^a{}_a$. Some facts worth remembering about the determinant:

(i). The definition itself, essentially $\bigwedge^d T = \det(T)$ (Theorem 5.7.2.6).
(ii). $\det(T)$ is the product of the eigenvalues of T in an algebraic closure counted with multiplicity (Theorem 5.7.2.26).
(iii). $\operatorname{tr}(T)$ is the sum of the eigenvalues of T in an algebraic closure counted with multiplicity (Theorem 5.7.1.3).
(iv). For matrices, the determinant is uniquely defined by how it changes upon performing row operations (Theorem 5.7.2.37).
(v). The cofactor expansion can be used to explicitly compute determinants of matrices (Corollary 5.7.2.80).
(vi). The absolute value of the determinant tells you how T scales the volume (Theorem 5.7.2.101).
(vii). The sign of the determinant tells you whether T changes the orientation (Theorem 5.7.2.108).
(viii). The characteristic polynomial of T is defined to be $\det(T - \lambda)$, and has the important property that its roots are exactly the eigenvalues of T (Theorem 5.7.2.120). In practice, this is how eigenvalues of matrices are usually computed.

Finally, we discussed bilinear and quadratic forms. "Bilinear form" is just a fancy name for a map $V \times V \to \mathbb{K}$, and a quadratic form $Q\colon V \to \mathbb{K}$ is a function of the form $Q(v) = (v \mid v)$ for a bilinear form $(\cdot \mid \cdot)\colon V \times V \to \mathbb{K}$. Except for $\operatorname{Char}(\mathbb{F}) = 2$, these are in one-to-one correspondence with one another (Theorem 5.8.1.3).

Our main concern here was diagonalization, and it turns out that one can always diagonalize quadratic forms, and hence one can always diagonalize bilinear forms if $\operatorname{Char}(\mathbb{F}) \neq 2$ (Theorem 5.8.3.3).

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12



6. Inner-product spaces

6.1 Motivation

We began these notes motivating the definition of a $\mathbb{K}$-module as an abstraction of the set of column vectors $\mathbb{R}^d$. This was just one possible abstraction, however. $\mathbb{R}^d$ is many things: It can be thought of as an $\mathbb{R}$-module, yes, but it can also be thought of as a topological space, a topological $\mathbb{R}$-module, a normed vector space, just a set, etc.. What we will be concerned with in this chapter, however, is the structure that $\mathbb{R}^d$ has as an *inner-product space*.

An *inner-product* is going to be an abstraction of the notion of the dot product on $\mathbb{R}^d$, in which case an *inner-product space* will be a vector space together with an inner-product. $\mathbb{R}^d$ will then have the canonical structure of an inner-product space with inner-product given by the usual dot product.

The intuition as to what extra information an inner-product gives us comes from the classical result for the dot product in $\mathbb{R}^d$:

$$v \cdot w = \|v\|\|w\| \cos(\theta), \tag{6.1.1}$$

where $\theta \in (-\pi, \pi]$ is the angle from v to w in the unique plane containing $\{0, v, w\}$ (unless one of v, w is the zero vector, in which case by convention we can take $\theta = 0$). From this, we see that the

dot product gives us information about length of vectors and angles between them. Of particular importance is the case of $v \cdot w = 0$, which roughly corresponds to v and w being perpendicular.[1]

So, if our objective then is to generalize and abstract the properties of the dot product, we had better investigate some of its properties. Given $v, w \in \mathbb{C}^d$, you'll recall that the dot product of v and w is defined by

$$v \cdot w \coloneqq \sum_{k=1}^{d} v_k^* w_k, \tag{6.1.2}$$

where v_k^* is the complex conjugate of v_k. This of course is a function $\mathbb{C}^d \times \mathbb{C}^d \to \mathbb{C}$. Given the subject of the previous chapter, it is now natural to ask "Is this bilinear?". Unfortunately, the answer is *no*, albeit for a somewhat silly reason. The dot product is bilinear *except* for the fact that

$$(\alpha v) \cdot w = {}^2\alpha^* v \cdot w. \tag{6.1.3}$$

That is, it isn't linear in the first argument, but rather it is *conjugate*-linear. Thus, $\mathbb{C}^d \times \mathbb{C}^d \to \mathbb{C}$ is not bilinear, but it is what is called *sesquilinear*.

Besides that, one crucial property to note is

$$v \cdot v \coloneqq \sum_{k=1}^{d} v_k^* v_k = \sum_{k=1}^{d} |v_k|^2 =: \|v\|^2. \tag{6.1.4}$$

In particular, $v \cdot v \geq 0$ with $v \cdot v = 0$ iff $v = 0$. These conditions together are what is referred to as *nonnegative definite*.

One thing you might have noticed is that, these properties we are referring to aren't particularly amenable to vast generalization. Certainly not compared to when we came up with the definition of a $\mathbb{K}$-module. At the very least, "nonnegative definite" requires a notion of order and "sesquilinear" requires a notion of 'conjugation'. Indeed, we will not be able to generalize the theory of inner-product spaces to

[1] Only "roughly" because there isn't really a classical notion of what it means for the zero vector to be perpendicular to something.

anywhere near the level of generality we did with $\mathbb{K}$-modules. There is a theory for inner-product spaces over $\mathbb{R}$ or $\mathbb{C}$, but that's about it.[3]

Thus, our idea for the definition of an inner-product is a "sesquilinear nonnegative definite map $V \times V \to \mathbb{C}$". Before we make this definition, however, let us try to 'fix' the issue of being conjugate-linear instead of bilinear.[4]

6.2 Conjugate space

In the previous section, we noted how that classical dot product is not linear, but rather *conjugate*-linear in the first argument. In this section, we introduce the *conjugate space*, which is a tool that will allow us to replace conjugate-linear maps with 'actual' linear maps.

Definition 6.2.1 — Conjugate-linear-transformation Let V and W be complex-vector spaces, and let $T : V \to W$ be a function. Then, T is a ***conjugate-linear-transformation*** iff

(i). $T : V \to W$ is a group homomorphism; and
(ii). $T(\alpha \cdot v) = \alpha^* \cdot T(v)$ for all $\alpha \in \mathbb{C}$ and $v \in V$.

R Of course, this is exactly the same as the definition of a linear-transformation (Definition 1.1.32) except for the fact that we have "$\alpha^* \cdot T(v)$" instead of just "$\alpha \cdot T(v)$".

Definition 6.2.2 — Conjugate space Let V be a complex vector space. Then, the ***conjugate space*** of V, $\bar{V}$, is the complex vector space defined by

[3] *Maybe* it would be possible to mimic the theory for a general real closed field and its algebraic closure, but, as I am aware of no applications of this, we will make no such attempt.

[4] There's really no getting around this. If we take our canonical example of the dot product defined in (6.1.2) and try to get rid of the complex conjugate, we wind up with something that is not nonnegative (for example, $\mathrm{i} \cdot im = -1$).

(I).

$$\bar{V} := \{\bar{v} : v \in V\}; \tag{6.2.3}$$

(II).

$$\bar{v} + \bar{w} := \overline{v + w}; \tag{6.2.4}$$

and

(III).

$$\alpha \cdot \bar{v} := \overline{\alpha^* v}. \tag{6.2.5}$$

R Thus, $\bar{V}$ has essentially the same underlying set of vectors and addition as V (though we write $\bar{v}$ for the elements of $\bar{V}$ to clarify that we are thinking of them as elements of $\bar{V}$ and not as elements of V), but with the scaling modified by a complex conjugate.

R Note that there is a canonical conjugate-linear isomorphism $V \to \bar{V}$, $v \mapsto \bar{v}$.[a] Intuitively, this is thought of as taking the complex conjugate of the components of the vector.

In particular, if $S \subseteq V$, we have that

$$\bar{S} = \{\bar{v} : v \in S\} \subseteq \bar{V}. \tag{6.2.6}$$

[a] A *conjugate-linear isomorphism* is effectively just an invertible map that is conjugate-linear.

The conjugate space allows us to replace conjugate-linear maps with linear ones in the following way.

Theorem 6.2.7. Let V and W be complex vector spaces, and let $T : V \to W$ be a function. Then, the following are equivalent.

(i). $T : V \to W$ is conjugate-linear.

(ii). $T\colon \bar{V} \to W$ is linear.
(iii). $T\colon V \to \bar{W}$ is linear.
(iv). $T\colon \bar{V} \to \bar{W}$ is conjugate-linear.

R The other three maps are obtained from T by precomposing or postcomposing with the canonical maps $\bar{V} \to V$ and $W \to \bar{W}$.

By abuse of notation, we denote all of these simply by "T"—in practice, they will be distinguished only by their domains and codomains.[a]

R The last map, sometimes denoted $\bar{T}\colon \bar{V} \to \bar{W}$, is the ***conjugate*** of T. This is justified by Proposition 6.2.14, which says that, in coordinates, $\bar{T}$ amounts to just taking the complex conjugate of all the entires. (It is also justified by the fact that $V \mapsto \bar{V}$, $T \mapsto \bar{T}$ then defines a functor, but we won't care about this.)

R There are analogous equivalences for $T\colon V \to W$ being linear. We refrain from stating them explicitly to avoid being overly verbose. Though do note in particular that $T\colon V \to W$ is linear iff $T\colon \bar{V} \to \bar{W}$ is linear.

R Thus, we can think of T as a linear map if we replace V with $\bar{V}$ or W with $\bar{W}$. By convention, we will tend to replace V with $\bar{V}$.

R In the definition, write $\bar{v}$ for elements of $\bar{V}$. In this context, however, we will almost always write $T(v) \coloneqq T(\bar{v})$. This is justified by the fact that we may always think of T as having domain V but conjugate-linear instead of linear. (You can imagine that writing "$\bar{v}$" all the time becomes quite tedious.)

[a] An exception to this is the last, which will sometimes be denoted $\bar{T}\colon \bar{V} \to \bar{W}$—see the following remark.

Proof. We leave this as an exercise.

Exercise 6.2.8 Prove the result.

■

Before returning to inner-product spaces themselves, we first check that this notion of conjugate agrees with the ordinary one upon choose coordinates.

Proposition 6.2.9 — Conjugate space in coordinates Let V be a complex vector space, let $\mathcal{B}$ be a basis of V, and let $v \in V$. Then,

$$[\bar{v}]_{\bar{\mathcal{B}}} = \overline{[v]_{\mathcal{B}}}. \tag{6.2.10}$$

R In words, the coordinates of the conjugate of v are given by the complex conjugate of the coordinates of v.

Proof. Write

$$v = \sum_{b \in \mathcal{B}} v^b \cdot b \tag{6.2.11}$$

for unique $v^b \in \mathcal{B}$. Applying the map $V \to \bar{V}$, $v \mapsto \bar{v}$, we obtain

$$\bar{v} = \sum_{b \in \mathcal{B}} \overline{v^b} \cdot \bar{b}, \tag{6.2.12}$$

and hence

$$[\bar{v}]_{\bar{\mathcal{B}}} = \overline{[v]_{\mathcal{B}}}, \tag{6.2.13}$$

as desired. ■

We of course have an analogous result for linear-transformations.

Proposition 6.2.14 — Conjugate linear-transformation in coordinates Let V and W be finite-dimensional complex vector spaces, let $\mathcal{B}$ and $\mathcal{C}$ be bases for V and W respectively, and let $T : V \to W$ be a linear-transformation. Then,

$$[\bar{T}]_{\bar{\mathcal{C}}\leftarrow\bar{\mathcal{B}}} = \overline{[T]_{\mathcal{C}\leftarrow\mathcal{B}}}. \tag{6.2.15}$$

R In words, the matrix of $\bar{T}$ is obtained from the matrix of T by taking the complex conjugate component-wise.

Proof. We simply apply the definition of the coordinates of a linear-transformation (Theorem 3.2.2.1) and show that $\overline{[T]_{\mathcal{C}\leftarrow\mathcal{B}}}$ satisfies the defining equation of $[\bar{T}]_{\bar{\mathcal{C}}\leftarrow\bar{\mathcal{B}}}$. So, let $v \in V$. Then, using the previous result,

$$\begin{aligned}\overline{[T]_{\mathcal{C}\leftarrow\mathcal{B}}}[\bar{v}]_{\bar{\mathcal{B}}} &= \overline{[T]_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}}} = \overline{[T]_{\mathcal{C}\leftarrow\mathcal{B}}}[v]_{\mathcal{B}} \\ &= \overline{[T(v)]_{\mathcal{C}}} = [\overline{T(v)}]_{\bar{\mathcal{C}}} = [\bar{T}(\bar{v})]_{\bar{\mathcal{C}}},\end{aligned} \tag{6.2.16}$$

and hence, by definition, we have that

$$[\bar{T}]_{\bar{\mathcal{C}}\leftarrow\bar{\mathcal{B}}} = \overline{[T]_{\mathcal{C}\leftarrow\mathcal{B}}}, \tag{6.2.17}$$

as desired. ∎

Having dealt with this, we can return to the 'official' definition of an inner-product.

6.3 Basic definitions

6.3.1 Inner-products

Definition 6.3.1.1 — Inner-product Let V be a complex vector space. Then, an ***inner-product*** on V is a function $\langle\cdot|\cdot\rangle : \bar{V} \times V \to V$ such that

(i). $\langle \cdot | \cdot \rangle$ is bilinear;
(ii). $\langle v|w\rangle^* = \langle w|v\rangle$;
(iii). $\langle v|v\rangle \geq 0$; and
(iv). $\langle v|v\rangle = 0$ iff $v = 0$.

R (ii) is referred to as ***conjugate symmetry***, (i) and (ii) together are referred to as ***sesquilinearity***,[a] (iii) is referred to as ***nonnegativity***, and (iv) is referred to as ***definiteness***.

R Explicitly, (i) is equivalent to

$$\langle v|\alpha_1 \cdot w_1 + \alpha_2 \cdot w_2\rangle = \alpha_1\langle v|w_1\rangle + \alpha_2\langle v|w_2\rangle$$

and

$$\langle \alpha_1 \cdot v_1 + \alpha_2 \cdot v_2|w\rangle = \alpha_1^*\langle v_1|w\rangle + \alpha_2^*\langle v_2|w\rangle.$$

R Warning: Many authors take $\langle \cdot | \cdot \rangle$ to be conjugate-linear in the *second* argument, whereas we have taken it to be conjugate-linear in the first. The convention I use comes from physics. Quite honestly, I had used it so much before I ever saw anyone use the mathematicians' convention that now conjugate-linearity in anything but the first argument seems to me to be an utter perversion of the highest order. This time, however, admittedly my rational explanation as to why one should prefer one convention over the other is rather limited.

R (iii) and (iv) together are more commonly referred to as ***positive-definite***, though really "nonnegative" is more appropriate as the condition involves "≥" not ">".

R An inner-product is thus a pairing $\bar{V} \times V \to \mathbb{C}$ in the sense of Definition 5.2.2.1. There, we tended to write $(\cdot\,|\,\cdot)$ for the pairings. Here, we choose to write $\langle \cdot | \cdot \rangle$ to stress the fact that we will often be thinking of $\langle \cdot | \cdot \rangle$ as a function on $V \times V$ that is conjugate-linear in the first argument (whereas of course pairings on

Definition 6.3.1.2 — Inner-product space An ***inner-product space*** is

is linear in the second argument and conjugate-linear in the first.

(I). a complex vector space V; together with
(II). an inner-product $\langle \cdot | \cdot \rangle : \bar{V} \times V \to \mathbb{C}$.

R One can treat inner-product spaces over $\mathbb{R}$ as well, and most of the theory (but not) remains just as valid. For simplicity, "inner-product space" for us will mean what others might refer to as a "complex inner-product space". When appropriate, we will try to remember to point out places where the real theory differs.

R Warning: One would naively guess that the right notion of morphism in this case are those linear maps $T : V \to W$ that satisfy

$$\langle T(v_1) | T(v_2) \rangle = \langle v_1 | v_2 \rangle \tag{6.3.1.3}$$

for all $v_1, v_2 \in V$. No doubt, such maps are very important,[a] but this condition is a bit too strong to be the 'right' notion of morphism for inner-product spaces.

Instead, it is better to just consider the *continuous*[b] linear maps between inner-product spaces—see Subsection 6.4.3.

[a] They're called *unitary maps*—see Definition 6.6.4.9.

[b] Though we technically haven't told you what "continuous" means in this context.

▪ **Example 6.3.1.4 —** $\mathbb{C}^d$ $\mathbb{C}^d$ is an inner-product space with inner-product given by the ***dot product***

$$\langle v | w \rangle := v \cdot w := \sum_{k=1}^{d} v_k^* w_k . \tag{6.3.1.5}$$

An extension of $\mathbb{C}^d$ to countably-infinite dimensions, known as $\ell^2(\mathbb{N})$, is one of the most important, if not the most important, infinite-dimensional inner-product spaces.

▪ **Example 6.3.1.6 — ℓ^2** Define

$$\ell^2(\mathbb{N}) := \left\{ a \in \mathbb{C}^{\mathbb{N}} : \sum_{m\in\mathbb{N}} |a_m|^2 < \infty \right\}, \tag{6.3.1.7}$$

and define $\langle\cdot|\cdot\rangle : \overline{\ell^2(\mathbb{N})} \times \ell^2(\mathbb{N}) \to \mathbb{C}$ by

$$\langle a|b\rangle := \sum_{m\in\mathbb{N}} a_m^* b_m. \tag{6.3.1.8}$$

Exercise 6.3.1.9 Show that $|\langle a|b\rangle| < \infty$ for $a, b \in \ell^2(\mathbb{N})$.

R Hint: You might try waiting until after having learned the Cauchy-Schwarz Inequality (Theorem 6.3.2.1).

Exercise 6.3.1.10 Check that $\langle\cdot|\cdot\rangle : \overline{\ell^2(\mathbb{N})} \times \ell^2(\mathbb{N}) \to \mathbb{C}$ satisfies the axioms of an inner-product.

R You should note that this is essentially nothing more than a generalization of the dot-product to countably-infinite dimensions. The only thing to watch out for is that you can't define the inner-product of all sequences—you have to restrict to those sequences for which the sum will converge.

R In fact, for any $p \geq 1$,[a] we can define

$$\ell^p(\mathbb{N}) := \left\{ a \in \mathbb{C}^{\mathbb{N}} : \sum_{m\in\mathbb{N}} |a_m|^p < \infty \right\}. \tag{6.3.1.11}$$

And in fact, we always have a norm

$$\|a\|_p := \left(\sum_{m\in\mathbb{N}} |a_m|^p \right)^{1/p}. \tag{6.3.1.12}$$

The reason we care about $p = 2$ is because this is the only norm given by an inner-product—see Exercise 6.3.2.21.

R Actually, there is nothing particularly special about $\mathbb{N}$, and this can be generalized to any set S.[b] In fact, this can be generalized even further to what is ordinarily written as $\mathrm{L}^p(X)$, where X is a measure space.[c]

R The reason ℓ^2 is particularly special is because, given an orthonormal basis $\mathcal{B}$ and $v \in V$, the coordinates of v with respect to $\mathcal{B}$ is an element of $\ell^2(\mathcal{B})$—see Proposition 6.5.2.1.

R Note that $\mathbb{C}^\infty \subseteq \ell^2(\mathbb{N})$, and hence $\mathbb{C}^\infty$ may be regarded as an inner-product space with the same inner-product. As it turns out, however, $\ell^2(\mathbb{N})$ is much better behaved—it is what is called a *Hilbert space*—see Definition 6.4.3.5.

[a] Actually, this definition makes sense for any $p > 0$, but $\|\cdot\|_p$ we define below won't be a norm unless $p \geq 1$. Furthermore, there is an $\ell^\infty(\mathbb{N})$, but this definition has to be given separately (it's not quite of the same form).

[b] Yes, you can talk about convergence of sums over any set, and if someone tells you otherwise, they don't know what they're talking about—see Notation 6.4.2.1.

[c] In case you're wondering about the change in notation, I personally use ℓ^p for the actual set of functions, whereas I reserve L^p for *equivalence classes* of functions. You're not expected to know any of this—I'm just telling you so that you are aware it's a thing.

■ **Example 6.3.1.13 —** $C^\infty([-1,1])$ $C^\infty([-1,1])$ is an inner-product space with inner-product given by

$$\langle f \,|\, g \rangle := \int_{-1}^{1} \mathrm{d}x \, f(x)^* g(x). \tag{6.3.1.14}$$

R Just about the only thing special about $[-1,1]$ is that it is compact, so that C^∞ functions are bounded on $[-1,1]$, so that this integral is finite. If we tried to do the same trick with $C^\infty(\mathbb{R})$, we'd have to restrict f, g so as to ensure that the integral converged.

R Unless otherwise stated, function spaces like this should be assumed to be equipped with the analogous inner-product. So, for example, $\mathrm{Mor}_{\mathbf{Top}}([-\pi, \pi], \mathbb{C})$ is by default equipped with the inner-product

$$\langle f | g \rangle := \int_{-\pi}^{\pi} \mathrm{d}x \, f(x)^* g(x). \tag{6.3.1.15}$$

R You should note the similarity between this and the dot product (defined in (6.3.1.5)). The integral $\int_{-1}^{1} \mathrm{d}x$ plays the role of the sum $\sum_{k=1}^{d}$, and v_k^* and w_k are replaced respectively by $f(x)^*$ and $g(x)$. Thus, though this perspective is not always useful, we can think of f and g as 'column vectors' with components are indexed by a 'continuous variable' $x \in [-1, 1]$, instead of by the usual 'discrete variable' $k \in \{1, \ldots, d\}$.j

▪ **Example 6.3.1.16** $\mathbb{C}[x]$ is an inner-product space with inner-product defined by

$$\langle p | q \rangle := \int_{-\infty}^{\infty} \mathrm{d}x \, p(x)^* q(x) \mathrm{e}^{-x^2/2}. \tag{6.3.1.17}$$

R This inner-product (and variants of it, with a different "weighting function" in place of $\mathrm{e}^{-x^2/2}$) are relevant to what is called *Sturm-Liouville Theory*. For example, this theory will immediately give you that a collection of polynomials called the *Hermite polynomials* is orthogonal (Definition 6.5.1.1) with respect to this inner-product.[a]

R We do *not* consider $\mathbb{C}[x]$ to be equipped with this inner-product by default.

[a] It gives orthogonality for other important collections of polynomials, but the "weighting function" will be different in general.

In the context if inner-product spaces, we will sometimes make use of alternative notation called *bra-ket* notation, its main use being that it makes certain formula more transparent.

Notation 6.3.1.18 — Bra-ket notation Let V be an inner-product space and let $v \in V$.

(i). We shall sometimes write $|v\rangle := v \in V$ for vectors in V. When using this notation, $|v\rangle$ is referred to as a ***ket***.

(ii). Similarly, for $v \in V$, we shall sometimes write $\langle v| \in V^\dagger$ for the linear-functional $\langle v| : V \to \mathbb{C}$ defined by $[\langle v|](w) := \langle v|w\rangle$. When using this notation, $\langle v|$ is referred to as a ***bra***.

Using kets to denote elements of V, the definition of $\langle v|$ can be written

$$[\langle v|](|w\rangle) := \langle v|w\rangle, \tag{6.3.1.19}$$

which demonstrates where the notation comes from.

R "Bra-ket" is pronounced the same as "bracket" (/bɹækɛt/), for obvious reasons. "Ket" itself then has the obvious pronunciation (/kɛt/). "Bra" on the other hand in this context is pronounced as /bɹæ/, that is, as the first half of the word "bra-ket" because, well, because it's the first half of the word "bra-ket". Please don't pronounce this as /bɹɑ/—that means something different.[a]

[a] The script I'm using to denote the pronunciation here is the International Phonetic Alphabet—feel free to Google that if you care enough.

6.3.2 The norm of an inner-product

An inner-product is going to permit us to define what is called a *norm* on the vector space (Proposition 6.3.2.9). However, if we want to actually show that this *is* a norm, we must first investigate an equality that is important in its own right: the *Cauchy-Schwarz Inequality*.

Theorem 6.3.2.1 — Cauchy-Schwarz Inequality. Let V be an inner-product space and let $v, w \in V$. Then,

$$|\langle v|w\rangle| \leq \|v\|\|w\|. \tag{6.3.2.2}$$

Furthermore, we have inequality iff one of v, w is a scalar multiple of the other.

R $\|v\| := \sqrt{\langle v|v\rangle}$ and similarly for w—see Proposition 6.3.2.9.

R I've also seen this referred to as the ***Cauchy-Bunyakowsky-Schwarz Inequality***.

Proof. If $w = 0$, the result is trivial, so suppose $w \neq 0$. Then define

$$|u\rangle := \left[1 - \frac{1}{\|w\|^2}|w\rangle\langle w|\right]|v\rangle := |v\rangle - \frac{\langle w|v\rangle}{\|w\|^2}|w\rangle.^a \tag{6.3.2.3}$$

Exercise 6.3.2.4 Show that

$$\|v\|^2 = \left\|\frac{\langle w|v\rangle}{\|w\|^2}w\right\|^2 + \|u\|^2. \tag{6.3.2.5}$$

R Later, we will be able to see this immediately from the Pythagorean Theorem (Theorem 6.5.1.11) (after checking that u and $\frac{\langle w|v\rangle}{\|w\|^2}w$ are orthogonal).

It follows that

$$\|v\|^2 = \frac{|\langle w|v\rangle|}{\|w\|^2} + \|u\|^2 \geq \frac{|\langle w|v\rangle|}{\|w\|^2}, \tag{6.3.2.6}$$

whence we have $|\langle w|v\rangle| \leq \|v\|\|w\|$, as desired.

Certainly if one of v, w is a scalar multiple of the other, then we have equality. To prove the converse, suppose that $|\langle v|w\rangle| = \|v\|\|w\|$. If $v = 0$, then $v = 0 \cdot w$, so suppose $v \neq 0$. The above then holds, and from (6.3.2.6) we see that equality implies that $\|u\|^2 = 0$, and hence $u = 0$. From the definition of u, it then follows that

$$v = \frac{\langle w|v\rangle}{\|w\|^2} w, \tag{6.3.2.7}$$

as desired. ■

[a] Later, we will recognize the second term here as the projection of v onto the subspace spanned by w, in which case we will recognize u as the projection of v onto $\{w\}^\perp$.

The axioms of an inner-product, nonnegative definiteness in particular, allow one to define an associated norm.

Definition 6.3.2.8 — (Semi)norm Let V be a complex vector space. Then, a ***seminorm*** on V is a function $\|\cdot\|: V \to \mathbb{R}_0^+$ such that

(i). (Homogeneity) $\|\alpha v\| = \|\alpha\|\|v\|$ for $\alpha \in \mathbb{R}$ and $v \in V$;
(ii). (Triangle Inequality) $\|v_1 + v_2\| \leq \|v_1\| + \|v_2\|$.

$\|\cdot\|$ is a ***norm*** if furthermore (Definiteness) $\|x\| = 0$ implies $x = 0$.

R The term "triangle inequality" comes from the geometric interpretation "The length of a size of a triangle is at most the sum of the lengths of the other two.".

Proposition 6.3.2.9 — Norm of an inner-product Let V be a complex vector space and let $\langle\cdot|\cdot\rangle: V \times V \to \mathbb{C}$ be an inner-product on V. Then, the ***norm*** $\|\cdot\|$ of $\langle\cdot|\cdot\rangle$, defined by,

$$\|v\| := \sqrt{\langle v|v\rangle} \tag{6.3.2.10}$$

is a norm on V.

R Note that this definition requires nonnegativity to even make sense (otherwise, we can't take the square-root).

R Obviously the norm depends on the inner-product, but we do not indicate such dependence in the notation because... well, imagine how obnoxious that would look.

Proof. We leave this as an exercise.

Exercise 6.3.2.11 Prove the result.

■

Which norms come from inner-products?

Thus, an inner-product determines a norm. It is then natural to ask if the converse is true. Of course, not every norm will come from an inner-product, but there is a nice characterization of those norms which do (Theorem 6.3.2.16). There is also the question of, in the case that the norm does come from an inner-product, is that inner-product unique? The answer to this question is in the affirmative.

Theorem 6.3.2.12 — Polarization Identity. Let V be an inner-product space and let $v, w \in V$. Then,

$$\langle v|w\rangle = \frac{1}{4}\left(\|v+w\|^2 - \|v-w\|^2 - \mathrm{i}\|v+\mathrm{i}w\|^2 + \mathrm{i}\|v-\mathrm{i}w\|^2\right). \tag{6.3.2.13}$$

R You should note that "polarization" itself is a relatively general trick. For example, see (6.6.4.39)—this is a similar sort of identity to write the expression $\langle v|T(w)\rangle$ as a linear-combination of expressions of the form $\langle v|T(v)\rangle$.

R Warning: It might not be immediately obvious what this becomes over the reals. The answer is that you just throw away the terms that involve i. Thus, for a real inner-product space,

$$\langle v|w\rangle = \frac{1}{4}\left(\|v+w\|^2 - \|v-w\|^2\right). \quad (6.3.2.14)$$

R The significance of this is not so much the exact formula itself, but rather that the inner-product is determined by the norm. Thus, for example, if you know that a linear-transformation "preserves" the norm, then you know automatically from the Polarization Identity that it also "preserves" the inner-product.

In particular, don't bother memorizing. Just understand when it can be used, and then you can look it up if need be.

Proof. We simply compute.

$$\begin{aligned}
&\|v+w\|^2 - \|v-w\|^2 - \mathrm{i}\|v+\mathrm{i}w\|^2 + \mathrm{i}\|v-\mathrm{i}w\|^2 \\
&\quad = \langle v+w|v+w\rangle - \langle v-w|v-w\rangle \\
&\qquad - \mathrm{i}\langle v+\mathrm{i}w|v+\mathrm{i}w\rangle + \mathrm{i}\langle v-\mathrm{i}w|v-\mathrm{i}w\rangle \\
&\quad = \|v\|^2 + \langle v|w\rangle + \langle w|v\rangle + \|w\|^2 \\
&\qquad - \|v\|^2 + \langle v|w\rangle + \langle w|v\rangle - \|w\|^2 \\
&\qquad - \mathrm{i}\|v\|^2 + \langle v|w\rangle - \langle w|v\rangle + \mathrm{i}\|w\|^2 \\
&\qquad + \mathrm{i}\|v\|^2 + \langle v|w\rangle - \langle w|v\rangle - \mathrm{i}\|w\|^2 \\
&\quad = 4\langle v|w\rangle,
\end{aligned} \quad (6.3.2.15)$$

as desired. ∎

We now address the question of existence.

Theorem 6.3.2.16 — Parallelogram Law. Let V be a complex vector space and let $\|\cdot\|: V \to \mathbb{R}_0^+$ be a norm on V. Then, $\|v\| = \sqrt{\langle v|v\rangle}$ for a unique inner-product $\langle\cdot|\cdot\rangle: \bar{V} \times V \to \mathbb{C}$ iff

$$\|v+w\|^2 + \|v-w\|^2 = 2(\|v\|^2 + \|w\|^2). \quad (6.3.2.17)$$

R (6.3.2.17) itself is the ***Parallelogram Identity*** or the ***Parallelogram Equality***.

R Imagine two vectors linearly-independent $v, w \in \mathbb{R}^2$. The four points $\{0, v, w, v+w\}$ are the vertices of a parallelogram in the plane. $v+w$ and $v-w$ are the diagonals of this parallelogram. Thus, the ***Parallelogram Law*** states that the sum of the squares of the diagonals is equal to the sum of the squares of the sides.

R In particular, this equality of the norm holds in inner-product spaces.

Proof. ($\Rightarrow$) Suppose that $\|v\| = \sqrt{\langle v|v\rangle}$ for a unique inner-product $\langle\cdot|\cdot\rangle \bar{V} \times V \to \mathbb{C}$. Then,

$$\begin{aligned}
&\|v+w\|^2 + \|v-w\|^2 \\
&\quad = \langle v+w|v+w\rangle + \|v-w\|^2 \\
&\quad = \|v\|^2 + \langle w|v\rangle + \langle v|w\rangle + \|w\|^2 \\
&\qquad + \|v\|^2 - \langle w|v\rangle - \langle v|w\rangle + \|w\|^2 \\
&\quad = 2(\|v\|^2 + \|w\|^2),
\end{aligned} \quad (6.3.2.18)$$

as desired.

($\Leftarrow$) Suppose that

$$\|v+w\|^2 + \|v-w\|^2 = 2(\|v\|^2 + \|w\|^2). \quad (6.3.2.19)$$

Define $\langle\cdot|\cdot\rangle\colon \bar{V}\times V\to\mathbb{C}$ by

$$\langle v|w\rangle := \tfrac{1}{4}\left(\|v+w\|^2-\|v-w\|^2-\mathrm{i}\|v+\mathrm{i}w\|^2+\mathrm{i}\|v-\mathrm{i}w\|^2\right).$$

Plugging in $w=v$, we see that the second term vanishes, the third and fourth terms cancel, and the first term becomes $\frac{1}{4}\|v+v\|^2=\|v\|^2$. Thus, it remains to show only that $\langle\cdot|\cdot\rangle$ is an inner-product

Nonnegative definiteness is manifest from $\langle v|v\rangle=\|v\|^2$. Upon swapping $v\leftrightarrow w$, the first and second terms remain unchanged, whereas the third and fourth terms swap. The net result is that this swap changing the imaginary part by a sign and the real part not at all, that is, $\langle w|v\rangle=\langle v|w\rangle^*$. It only remains to check that $\langle v|w\rangle$ is linear as a function of w.

For avoid fractions, we look at $4\langle v|w_1+w_2\rangle$. For additional simplification, we look at only the real and imaginary parts one at a time. We now compute, using (6.3.2.19).

$$\begin{aligned}4\Re[\langle v|w_1+w_2\rangle] &= \|v+(w_1+w_2)\|^2-\|v-(w_1+w_2)\|^2\\ &= \left(2\|v+w_1\|^2+2\|w_2\|^2-\|(v+w_1)-w_2\|^2\right)\\ &\quad+\left(\|(v-w_2)+w_1\|^2-2\|v-w_2\|^2-2\|w_1\|^2\right)\\ &= 2\left(\|v+w_1\|^2-\|v-w_2\|^2+\|w_2\|^2-\|w_1\|^2\right).\end{aligned}$$

As the left-hand side is $w_1\leftrightarrow w_2$ symmetric, we must similarly have

$$\begin{aligned}&4\Re[\langle v|w_1+w_2\rangle]\\ &\quad= 2\left(\|v+w_2\|^2-\|v-w_1\|^2+\|w_1\|^2-2\|w_2\|^2\right).\end{aligned}$$

Adding this two equalities yields

$$\begin{aligned}&8\Re[\langle v|w_1+w_2\rangle]\\ &\quad= 2\left(\|v+w_1\|^2+\|v-w_1\|^2\right)\\ &\qquad+2\left(\|v+w_2\|^2-\|v-w_2\|^2\right),\end{aligned}\tag{6.3.2.20}$$

as desired. The imaginary part is similar and we omit the computation.

As $w \mapsto \langle v|w\rangle$ preserves addition, it preserves scaling by integers, and hence scaling by rationals.[a] As $w \mapsto \langle v|w\rangle$ is continuous,[b] it must in turn preserve scaling for all real numbers. Finally, as $\langle v|\mathrm{i}w\rangle = \mathrm{i}\langle v|w\rangle$, it follows that $w \mapsto \langle v|w\rangle$ preserves scaling by all complex numbers, and we are done.

Uniqueness follows from the Polarization Identity (the inner-product, if it existed, is determined by the norm). ■

[a] We've seen this trick before—if $f(x)$ preserves scaling by integers, then look at $f(m \cdot \frac{n}{m}x)$ to see that it preserves scaling by rationals as well.

[b] It is a bounded linear map by Cauchy-Schwarz.

Exercise 6.3.2.21 Recall Example 6.3.1.6 the definition of $\ell^p(\mathbb{N})$ and $\|\cdot\|_p$:

$$\ell^p(\mathbb{N}) := \left\{ a \in \mathbb{C}^{\mathbb{N}} : \sum_{m\in\mathbb{N}} |a_m|^p < \infty \right\} \tag{6.3.2.22}$$

and, for $a \in \ell^p(\mathbb{N})$,

$$\|a\|_p := \left(\sum_{m\in\mathbb{N}} |a_m|^p \right)^{1/p}. \tag{6.3.2.23}$$

Show that $\|\cdot\|_p$ comes from an inner-product iff $p = 2$.

R Note that $\|\cdot\|_p$ is indeed a norm for all $p \geq 1$, but don't bother checking this.

6.4 Topological issues

6.4.1 Introduction

There is one serious problem that we're going to need to address in the theory of inner-product spaces. Without extra hypothesis, shit *breaks* in infinite-dimensions. Certainly we've seen things break

before in infinite-dimensions, for example, linear operators need not have any eigenvalues in infinite-dimensions, even over algebraically closed fields. However, most things that broke before weren't so immediately close to the foundations. On the other hand, all but the most trivial of results about inner-product spaces require extra hypotheses to hold in infinite-dimensions. Another big difference is that a lot of the breaking we saw before really can't be fixed—even in the nicest of infinite-dimensional spaces, operators aren't going to have eigenvalues; there's just no getting around it. The things that are going to break here, however, are relatively easily fixed, and so I'm very tempted to put in the little extra effort to fix them.

The catch is that this technically requires material that is not a prerequisite for the course. I'm going to try to do the best I can to get the best of both worlds and write an exposition that will continue to be helpful to you when you need to know how things work in infinite-dimensions, but yet won't lose you if you haven't seen the prerequisites before. For example, in order for a statement in finite-dimensions to remain valid in infinite-dimensions, one commonly must say "closed subspace" instead of just "subspace" (it turns out that every subspace is closed in finite-dimensions). Thus, in case you don't know what "closed" means, you can ignore the word, pretend it's a finite-dimensional space, and everything will be hunky-dory. I will do the best I can to let you know other things that can be ignored as they come up if you're only interested in finite-dimensions.[5]

If you only care about the finite-dimensional case, you can safely skip the rest of this section. Before you do so however, you will probably find it useful to notes that, under the assumption everything involved is finite-dimensional,

(i). whenever you see the term "Hilbert space", instead pretend I said "finite-dimensional inner-product space";

[5]I won't use anything not covered in my analysis notes [Gle17], and so that is one source I can guarantee will answer any questions you might have regarding the prerequisite material. (The reason I don't give specific theorem numbers is because [Gle17] is still in 'beta', and the numbers will likely change in future versions.)

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

(ii). you can ignore any references to anything having to do with topology;[6]
(iii). you can ignore any references to anything having to do with continuity;[7]
(iv). whenever you see "$\mathbf{TopVect}_{\mathbb{C}}$" or "**TopVect**",[8] instead pretend I said just $\mathbf{Vect}_{\mathbb{C}}$;[9]
(v). you can assume that any sums whose terms are linearly-independent are finite;[10]
(vi). you can ignore instances of the word "complete";[11] and
(vii). whenever you see the phrase "closed subspace", instead pretend I said just "subspace";[12] and
(viii). whenever you see "Cls(Span(−))", instead pretend I wrote just "Span(−)".[13]

Note that we prove all of these justifications below in Subsection 6.4.5.

6.4.2 Conventions on sums

You'll recall that way back in Subsection 2.1.1 we established a convention that all sums are implicitly finite, even if the indexing set is not finite.[14] We are going to abolish (or rather, replace) this convention, but first, it is important to understand that, in a sense, it wasn't really a convention at all—see Proposition 6.4.2.3.

[6]This is justified by the fact that all finite-dimensional inner-product spaces are Hilbert spaces.

[7]This is justified by the fact that all linear maps between finite-dimensional inner product spaces are continuous.

[8]The latter will be used as short-hand because in this chapter we are essentially always working over $\mathbb{C}$.

[9]This is justified by the fact that all linear maps between finite-dimensional inner-product spaces are continuous.

[10]This is justified by the fact that linearly-independent subsets of finite-dimensional vector spaces are finite.

[11]This is justified by the fact that all finite-dimensional inner-product spaces are complete.

[12]This is justified by the fact that all subspaces of finite-dimensional inner-product spaces are closed.

[13]This is justified by the fact that all subspaces of finite-dimensional inner-product spaces are closed.

[14]In other words, it was implicit that all terms were 0 except finitely many.

To understand Proposition 6.4.2.3, we first need to recall the usual definition of a sum, when we are not implicitly assuming that only finitely many terms are nonzero.

Notation 6.4.2.1 Let V be a commutative T_0 topological group and let $S \subseteq V$. Then,

$$\sum_{v \in S} v \tag{6.4.2.2}$$

is the limit of the net $\mathscr{F} \ni F \mapsto \sum_{v \in F} v$, where $\mathscr{F}$ is the collection of all finite subsets of S ordered by inclusion.

R We require T_0 so that the space is T_2 so that limits are unique so that the notation is unambiguous.

R If you are only interested in the finite-dimensional case, you can ignore all of this, and safely assume that all sums are in fact finite.

R I haven't checked it carefully so don't quote me on it, but I believe our previous convention was actually just a special case of this: with our previous convention, we were implicitly equipping V with the discrete topology.

Proposition 6.4.2.3 Let V be a topological commutative group and let $S \subseteq V$. Then, if V has the discrete topology,

$$\sum_{v \in S} v \tag{6.4.2.4}$$

converges iff $\{v \in S : v \neq 0\}$ is finite.

Proof. Suppose that V has the discrete topology.

($\Rightarrow$) Suppose that

$$\sum_{v \in S} v \tag{6.4.2.5}$$

converges. As V has the discrete topology, that means that the corresponding net must be eventually constant. Thus, there is some finite set $F_0 \subseteq S$ such that, if $F \subseteq S$ is a finite set containing F_0,

$$\sum_{v \in F_0} v = \sum_{v \in F} v. \tag{6.4.2.6}$$

It follows that

$$\sum_{v \in F \setminus F_0} v = 0. \tag{6.4.2.7}$$

For $v_0 \in S \setminus F_0$, taking $F := F_0 \cup \{v_0\}$ in this equation, we see that $v_0 = 0$. Thus, $\{v \in S : v \neq 0\} = F_0$ is finite.

($\Leftarrow$) Immediate. ■

So, on one hand, we can just abolish the previously established convention in Subsection 2.1.1. However, I find the following conceptually clearer.

The objects of study are not actually $\mathbb{K}$-modules, but in fact *topological* $\mathbb{K}$-modules. Secretly, up to this point, everything has been a discrete $\mathbb{K}$-module, and the previous result explains why what was referred to as a convention before can really be thought of as the statement that everything previously was discrete. Now, however, we investigate topological $\mathbb{K}$-modules whose topology is not discrete.

The significance of this is that all definitions we met before remain (superficially) unchanged for topological modules.[a] We recover the notions we've been working with to this point by equipping a module with the discrete topology. We obtain the new notions we care about now by simply considering topological modules whose topology comes from an inner-product.

[a] The dual-space is a minor exception to this—see Definition 6.4.3.15.

We thus hereby replace the previously used convention Convention 2.1.1.4 with the following.

Convention 6.4.2.8 Whenever a sum of elements in a topological $\mathbb{K}$-module appears, it should be assumed that it converges unless otherwise stated.

In particular, note that "linear-combination" (Definition 2.1.1.5) now allows for infinitely-many terms. Furthermore, if we ever say something like "all linear-combinations" or "arbitrary linear-combinations", it should be understood that we only mean to include convergent linear-combinations.

As an example of how our definitions superficially don't change at all, but can be different from what we're used to if the topology is not discrete, consider the definition of a basis (Definition 2.2.1). We still say that $\mathcal{B} \subseteq V$ is a basis iff for every $v \in V$ there are unique $v^b \in \mathbb{C}$ such that

$$v = \sum_{b \in \mathcal{B}} v^b \cdot b. \tag{6.4.2.9}$$

This is word-for-word the same definition as before. *However*, we are now no longer using the convention that it is implicit in this equality that all but finitely many $v^b = 0$, and so in principle this sum can (and will) contain infinitely-many nonzero terms. Making the definition for topological $\mathbb{K}$-modules is a strict generalization in the sense that we recover the 'old' definition if the topological module is discrete, in which case, by the above result, this sum is secretly finite, which agrees with our previously used convention.

You should also take note that *many authors do not use this convention*. Instead, they'll make up new definitions like "topological basis". I find it cleaner to think of there just being one concept (that of a basis), and the context in which it is used is that of topological modules. You then obtain their "algebraic basis"[15] by using the discrete topology and you obtain their "topological basis" by using the inner-product topology. Similar comments apply to other definitions as well.

On the other hand:

> While definitions superficially remain unchanged, the *propositions, theorems, etc. do not*.

This is because we are now applying the same definitions in a more general context (not just for discrete modules), and one cannot expect results that one proved for discrete modules to hold for any topological module.

So, in a nutshell, all definitions are the same as they were before,[16] except that instead of assuming all sums are finite, we just assume that they converge.[17]

6.4.3 Hilbert spaces

Before doing anything further, let's first make sure (as best we can) that everyone is on the same page. If you're reading this subsection, it's assumed that you know enough about general topology to know

[15] Also known as a "Hamel basis".

[16] Again, the dual-space is a small exception—see Definition 6.4.3.15.

[17] This sounds simple enough, but be warned, this changes things quite a bit.

what the intended topology on an inner-product space is. In case not, we remind you.

Proposition 6.4.3.1 Let V be an inner-product space. Then, there is a unique topology on V that has the property that a net $\lambda \mapsto v_\lambda \in V$ converges to $v_\infty \in V$ iff

$$\lambda \mapsto \|v_\lambda - v_\infty\| \tag{6.4.3.2}$$

converges to 0 in $\mathbb{R}$.

R This defines a canonical uniformity and so we have a notion of Cauchyness: $\lambda \mapsto v_\lambda \in V$ is Cauchy iff

$$\langle \lambda, \mu \rangle \mapsto \|v_\lambda - v_\mu\| \tag{6.4.3.3}$$

converges to 0 in $\mathbb{R}$.

Of course, V will then be complete iff every Cauchy net converges.

R If you have interest in the infinite-dimensional case and don't know what nets are, go and learn what nets are. Strictly speaking, you don't need them, but use of sequences instead of nets is really just a crutch that will hinder you in the long run.[a]

[a] Not every mathematician will agree with me on this. But I also can't say I've ever met a mathematician that understands nets well try to argue that they are unimportant (if you are one, I would be curious to hear your thoughts)—only ones that feel uncomfortable with them, e.g. "Look how far I've gotten without using nets.". Very roughly speaking, this is sort of like saying "Look at all the linear algebra I've been able to do with just matrices.". Okay, sure, you *can* do linear algebra (in some sense) without talk of vector spaces or linear-transformations, but dear god what self-respecting mathematician would commit such a perversion? (Spoiler alert: none.) The point is, just because you can get away with it, doesn't mean it's a good idea.

Proof. This follows from Kelley's Convergence Theorem ([Gle17]). ∎

Similarly, we remind you what it means to be continuous.

Proposition 6.4.3.4 — Continuous function Let V and W be inner-product spaces, let $f : V \to W$ be a function between topological spaces, and let $x_0 \in X$. Then, f is ***continuous*** at x_0 iff $\lim_{x \to x_0} f(x) = f(x_0)$.

R f is ***continuous*** iff f is continuous at x for all $x \in X$.

R Said more explicitly, f is continuous at x_0 iff whenever $\lambda \mapsto x_\lambda$ converges to x_0, it follows that $\lambda \mapsto f(x_\lambda)$ converges to $f(x_0)$.

R Actually, in this context, there is a very important equivalent characterization of continuity (at least when f is linear) called *boundedness*—see Theorem 6.4.3.11.

R With one minor caveat, this actually holds true in the more general setting of *topological spaces*.

Proof. See [Gle17, Chapter 3]. ■

In the previous subsection we didn't really do anything new—we just clarified some things. In particular, we mentioned that we're going to need to impose some extra hypotheses in infinite-dimensions, but haven't yet told you what those hypotheses are. It's about time we do that.

Definition 6.4.3.5 — Hilbert space A ***Hilbert space*** is a complete inner-product space.

R The condition of being complete is an exceptionally natural one in this case. In a sense, this allows us to take *arbitrary* linear-combinations of vectors, not just finite ones.[a] Thus, if you're interested in a topological vector space in which you can take "arbitrary linear-combinations", you're going to want to work in a complete space.

R See Example 6.6.3.12 for an example of an inner-product space that is not a Hilbert space.

[a] Okay, so we don't need completeness to make sense of infinite sums per se, but we do need it to guarantee that the infinite sums which 'should' make sense do make sense.

▪ **Example 6.4.3.6** Of the examples we introduced immediately after the definition of an inner-product space (Definition 6.3.1.2), only $\mathbb{C}^d$ and ℓ^2 were Hilbert spaces.

Exercise 6.4.3.7 Show that $\mathbb{C}^d$ and $\ell^2(S)$ are Hilbert spaces (S any set).

On the other hand, we will see Example 6.6.3.12 and Exercise 6.6.3.19 that $C^\infty([-1,1])$ and $\mathbb{C}[x]$ with inner-products as defined in Example 6.3.1.13 and Example 6.3.1.16 are *not* Hilbert spaces.

As always, having introduced a new type of mathematical object, we should tell you what the relevant morphisms are. In fact, we should have done this before, but as the category makes reference to topology, we waited to present it in a section that is only intended to be read by those who care about infinite-dimensions.

▪ **Example 6.4.3.8 — The category of topological $\mathbb{K}$-modules** Let $\mathbb{K}$ be a topological ring. Then, the category of topological $\mathbb{K}$-modules is the concrete category **Top$\mathbb{K}$-Mod**

(i). whose collection of objects Obj(**Top$\mathbb{K}$-Mod**) is the collection of all topological $\mathbb{K}$-modules; and
(ii). with morphism set $\mathrm{Mor}_{\mathbf{Top}\mathbb{K}\text{-}\mathbf{Mod}}(V,W)$ precisely the set of all continuous linear-transformations from V to W.

R As in the nontopological case, we write $\mathbf{TopVect}_{\mathbb{F}} := \mathbf{Top}\mathbb{F}\text{-}\mathbf{Mod}$ if $\mathbb{F}$ is a division ring.

R In this chapter, as we are working essentially exclusively with $\mathbb{C}$, we will frequently write **TopVect** := $\mathbf{TopVect}_{\mathbb{C}}$.

We of course regard all inner-product spaces as topological vector spaces over $\mathbb{C}$, and so, according to this, by 'default', maps between inner-product are continuous and linear.

Just as we were interested in if we could make the morphism sets of $\mathbb{K}$-modules into $\mathbb{K}$-modules (Subsection 1.1.1), it is of interest to know if we can make morphism sets of topological $\mathbb{K}$-modules into topological $\mathbb{K}$-modules. Of course, from our discussion in Subsection 1.1.1, we know that to even get the structure of a module we need to work with bimodules instead of modules (or take $\mathbb{K}$ to be commutative). This is answered by the following result.

Proposition 6.4.3.9

(i). Let V be a topological R-S-bimodule and let W be a topological R-T bimodule. Then, $\mathrm{Mor}_{\mathbf{Top}R\text{-}\mathbf{Mod}}(V, W)$ is a topological S-T-bimodule when equipped with the topology of pointwise convergence.

(ii). Let V be a topological R-S-bimodule and let W be a topological T-S-bimodule. Then, $\mathrm{Mor}_{\mathbf{TopMod}\text{-}S}(V, W)$ is a topological T-R-bimodule when equipped with the topology of pointwise convergence.

R Recall that (Theorem 1.1.6) an R-module V is 'the same as' a commutative group V together with a ring homomorphism $R \to \mathrm{End}_{\mathbf{Grp}}(V)$. If we want an analogue of this result for topological R-modules, we need to equip $\mathrm{End}_{\mathbf{Grp}}(V)$ with the topology of pointwise convergence, which is why this is a natural topology to use in this context.

R Unless otherwise stated, it should be assume that morphism sets of topological bimodules are equipped with the topology of pointwise convergence.

Especially in the case $V = W$ is a Hilbert space, there is a plethora of other important topologies one

can use, though, despite their importance, we sadly will not be making use of them.

R In this context, this topology is often called the ***strong operator topology***.

Proof. We leave this as an exercise.

Exercise 6.4.3.10 Prove the result.

■

We know plenty about linear maps by now. What we don't know too much about yet is what it means to be continuous in this context. Fortunately, for linear-transformations between inner-product spaces, there is a relatively easy criterion.

Theorem 6.4.3.11 — Continuous iff bounded. Let V and W be inner-product spaces and let $T\colon V \to W$ be linear. Then, T is continuous iff there is some $M \geq 0$ such that $\|T(v)\| \leq M\|v\|$ for all $v \in V$.

R A linear-transformation $T\colon V \to W$ is ***bounded*** iff there is some $M \geq 0$ such that $\|T(v)\| \leq M\|v\|$ for all $v \in V$.[a] Using this language, this becomes the statement

> T is continuous iff it is bounded.

R In fact, this same statement holds verbatim for normed vector spaces—the only reason we don't state it in this context is because we haven't introduce normed vector spaces. Furthermore, it generalizes to what are called *semimetric spaces* (or *pseudometric spaces*), though in that context the statement has to be rewritten.

[a] This term technically conflicts with the other usage of the term, namely, that the image is a bounded set. For example, $\mathbb{R} \ni x \mapsto 3x \in \mathbb{R}$ is bounded

in this sense of the term (you can take $M = 3$) but not bounded in the usual sense (because it "goes to ∞"). In practice, however, this causes no confusion.

Proof. See [Gle17, Chapter 4]. ■

This suggests the following definition.

Definition 6.4.3.12 — Operator norm Let V and W be inner-product spaces and let $T\colon V \to W$ be bounded. Then, the ***norm*** of T, $\|T\|$, is defined by

$$\|T\| := \inf\{M \geq 0 : \|T(v)\| \leq M\|v\|\}. \tag{6.4.3.13}$$

R In particular, we have

$$\|T(v)\| \leq \|T\|\|v\| \tag{6.4.3.14}$$

for all $v \in V$. *Furthermore*, $\|T\|$ is the 'best' (i.e. smallest) constant for which this inequality is always true.

We mentioned previously that, unlike everything else, our definition of dual-space changes. The only change is that we want to consider the *continuous* linear-functionals.

Definition 6.4.3.15 — Dual-space Let V be a topological $\mathbb{K}$-$\mathbb{K}$-bimodule. Then, the ***dual-space*** of V is the topological $\mathbb{K}$-$\mathbb{K}$-bimodule

$$V^\dagger := \mathrm{Mor}_{\mathbf{Top}\mathbb{K}\text{-}\mathbf{Mod}}(V, \mathbb{K}), \tag{6.4.3.16}$$

equipped with the topology of pointwise convergence.

R Unless you already feel comfortable with it, I wouldn't worry too much about the topology on $V^\dagger$ itself. The most important thing to take note of is that $V^\dagger$ is the space of *continuous* linear-functionals.

R In this context, the topology of pointwise convergence is often referred to as the *weak-* topology*.

I realize that this is terribly awkward as I just told you that (Proposition 6.4.3.9) the topology of pointwise convergence on morphism sets is often called the *strong* operator topology, so, you know, not weak. Did I mention that mathematicians are terrible when it comes to terminology? Yes. Mathematicians are terrible when it comes to terminology. That said, it's not as if they don't have their reasons for using this terminology. Despite these admittedly good reasons, I don't know if that justifies using the term "strong" and "weak" in two different contexts that wind up meaning the same thing in a special case common to both contexts.

R If for some awkward reason one wants to talk about the space of *all* (not necessary continuous) linear maps $V \to \mathbb{K}$ as well, they might refer to the space of continuous linear maps $V \to \mathbb{K}$ as the *topological dual-space* or just *topological dual*, in which case the space of all linear maps would be referred to as the *algebraic dual-space* or just *algebraic dual*.

"Sub-Hilbert spaces"

We said before that all the definitions we gave before are taken to be the same as they were before (now without the extra assumption of implicit finiteness of sums). And while this is true, so that "subspace" does mean the same as it did before, in this context, we now also have a notion of a *sub-Hilbert space*.[18]

Definition 6.4.3.17 — Sub-Hilbert space Let V be a Hilbert space. Then, a ***sub-Hilbert space*** of V is a subset $W \subseteq V$ such that W is a Hilbert space.

[18] This term is nonstandard. We'll see why in a moment.

R We didn't introduce an analogous concept for inner-product spaces because it would coincide exactly with the previous notion of subspace.

As with subspaces, we have a convenient characterization used to check when a subset is indeed a sub-Hilbert space.

Proposition 6.4.3.18 Let V be a Hilbert space and let $W \subseteq V$. Then, W is a sub-Hilbert space iff

(i). W is a subspace; and
(ii). W is closed.

R This explains why no one ever uses the term "sub-Hilbert space"—we can (and will) just say "closed subspace" instead.

Proof. We leave this as an exercise.

Exercise 6.4.3.19 Prove the result.

■

Given a subset $S \subseteq V$ of a vector space, we proceeded to define $\text{Span}(S)$ as the smallest subspace that contains S. There is of course a corresponding notion for sub-Hilbert spaces.

Theorem 6.4.3.20 — Topological span. Let V be a Hilbert space and let $S \subseteq V$. Then, $\text{Cls}(\text{Span}(S))$ is the unique sub-Hilbert space of V, the ***topological span*** of S, such that

(i). $S \subseteq \text{Cls}(\text{Span}(S))$; and
(ii). if $W \subseteq V$ is another sub-Hilbert space containing S, it follows that $\text{Cls}(\text{Span}(S)) \subseteq W$.

Furthermore, explicitly, $\text{Cls}(\text{Span}(S))$ is the sum of all linear-combinations of elements of S.

R Thus,

$$\mathrm{Cls}(\mathrm{Span}(S)) = \left\{ \sum_{s \in S} \alpha_s \cdot s : \alpha_s \in \mathbb{C} \right\}. \quad (6.4.3.21)$$

Again, note that per our convention (Convention 6.4.2.8), (i) it is implicit that this sum converges and (ii) there is no requirement that the sum be finite. Thus, the difference between $\mathrm{Span}(S)$ and $\mathrm{Cls}(\mathrm{Span}(S))$ is that the former consists of just the finite linear-combinations and the latter consists of all linear-combinations.

Proof. We leave this as an exercise.

Exercise 6.4.3.22 Prove the result.

■

I would argue that we should have been working with complete topological $\mathbb{K}$-modules all along.[19] Then, the appropriate notion of "subspace" would include completeness: in the discrete topology, this is vacuous, and so we would recover the notion we first learned in Chapter 1; but in this context we would recover the notion of a sub-Hilbert space. This way, we would not have to speak of two distinct concepts (subspace and sub-Hilbert space), but just one, from which we could recover the two old concepts as special cases. In turn, there would only be one definition of Span.

The problem with doing this is that I would have to speak of "completeness" all the way back in Chapter 1. Contrast this with the definition of linear-independence, basis, etc. where I don't have to use any fancy words students might not know—it is very easy to phrase the definition in such a way so that (i) it gives the right answer both in the "purely algebraic" case and in the "inner-product case" and (ii) students can understand it with no extra prerequisites. So, for now

[19] I don't mean this literally for obvious pedagogical reasons. I mean, conceptually, for a 'unifying' picture, you can think of everything as a complete topological $\mathbb{K}$-module.

anyways, I'm going to leave the exposition as is and simply tell you that I think it is conceptually cleaner to think of there as being just one definition of subspaces that works in all cases: a subset that is also a *complete* $\mathbb{K}$-module.

6.4.4 Miscellaneous

In this subsection, we collection miscellaneous results that (i) will be used at least once in our exposition, (ii) are not part of inner-product space theory per se, (iii) you would likely know if you took a course in analysis previously, and (iv) don't have any particularly good place to be stated.

Theorem 6.4.4.1 — Hölder's Inequality. Let X be a topological measure space, let $1 \leq p, q \leq \infty$ be Hölder conjugates, and let $f, g \in \mathrm{Bor}(X)$. Then,

$$\|\cdot\|[fg]_1 \leq \|\cdot\|[f]_p \|\cdot\|[g]_q. \tag{6.4.4.2}$$

R A "topological measure space" is a σ-compact topological space equipped with a regular Borel measure.

R Note that the case $p = 2 = q$ is the Cauchy-Schwarz Inequality for $\mathrm{L}^2(X)$.

Proof. See [Gle17, Chapter 5]. ∎

Theorem 6.4.4.3 — Minkowski's Inequality. Let $\langle X_1, \mathrm{m}_1 \rangle$ and $\langle X_2, \mathrm{m}_2 \rangle$ be topological measure spaces, let $f \in \mathrm{Bor}(X_1 \times X_2)$, and let $1 \leq p \leq \infty$. Then,

$$\left\| \int_{X_2} \mathrm{d}\,\mathrm{m}_2(x_2)\, f(\cdot, x_2) \right\|_p \leq \int_{X_2} \mathrm{d}\,\mathrm{m}_2(x_2)\, \| f(\cdot, x_2) \|_p,$$

where $\|\cdot\|_p$ is the L^p-norm on X_1.

R Explicitly, this reads (for $p < \infty$)

$$\left[\int_{X_1} \mathrm{d}\,\mathrm{m}_1(x_1)\left|\int_{X_2} \mathrm{d}\,\mathrm{m}_2(x_2)\, f(x_1, x_2)\right|^p\right]^{1/p} \leq \int \mathrm{d}_{X_2}\,\mathrm{d}\,\mathrm{m}_2(x_2)\left[\int_{X_1} \mathrm{d}\,\mathrm{m}_1(x_1)\,|f(x_1, x_2)|^p\right]^{1/p}.$$

R I remember this roughly as "You can bring the exponents 'in a level' if you switch the order of integration."

Proof. See [Gle17, Chapter 5]. ∎

6.4.5 The justifications

We now prove all the results we referenced above at the end of Subsection 6.4.1 that we used as justifications for you being able to make certain simplifying assumptions if all you care about is finite-dimensions.

Proposition 6.4.5.1 Let V be a finite-dimensional inner-product space. Then, V is a Hilbert space.

R In other words, V is complete.

Proof. We leave this as an exercise.

Exercise 6.4.5.2 Prove the result.

∎

Proposition 6.4.5.3 Let V be a finite-dimensional inner-product space, and let W be a T_0 complex topological vector space, and let $T : V \to W$ be linear. Then, T is continuous.

R Don't worry about the "T_0"—all inner-product spaces are T_0, and in fact, you will probably have to go out of your way to construct something that is not T_0.

Proof. We leave this as an exercise.

Exercise 6.4.5.4 Prove the result.

■

Proposition 6.4.5.5 Let V be a finite-dimensional inner-product space and let $W \subseteq V$ be a subspace. Then, W is closed.

Proof. We leave this as an exercise.

Exercise 6.4.5.6 Prove the result.

■

Anyways, let's return to the study of inner-product spaces themselves.

6.5 Orthogonality

6.5.1 Basic definitions

At the very beginning of this chapter, we noted that the statement that $v \cdot w = 0$ is essentially the statement that v and w are perpendicular. "Perpendicular" really is a statement about angles, which a priori don't make sense, and so we instead we use a different term: *orthogonal*.

Definition 6.5.1.1 — Orthogonal Let V be an inner-product space and let $v, w \in V$. Then, v and w are ***orthogonal*** iff $\langle v|w\rangle = 0$.

R A subset $S \subseteq V$ is ***orthogonal*** iff any two distinct elements of S are orthogonal.

R As said before, intuitively, orthogonal vectors are thought of as being perpendicular.

Just as we had a notion of what it means for subspaces to be linearly-independent (Definition 4.4.1.12), we likewise have a notion of what it means for subspaces to be orthogonal.

Definition 6.5.1.2 — Orthogonal (subspaces) Let V be an inner-product spaces and let $\mathscr{W}$ be a collection of subspaces of V. Then, $\mathscr{W}$ is ***orthogonal*** iff for every $v_W \in W$ for $W \in \mathscr{W}$, the set

$$\{v_W : W \in \mathscr{W}\} \tag{6.5.1.3}$$

is orthogonal.

R That is, a collection of subspaces is orthogonal iff any set of elements from distinct subspaces from this collection is orthogonal.

Exercise 6.5.1.4 Let V be an inner-product space and let $S \subseteq V$ be orthogonal. Show that if $0 \notin S$, then S is linear-independent.

Definition 6.5.1.5 — Normalized Let V be a normed vector space and let $v \in V$. Then, v is ***normalized*** iff $\|v\| = 1$.

R If $v \in V$ is nonzero, then $\frac{v}{\|v\|}$ is normalized and is referred to as the ***normalization*** of v.

R Note that, if V is an inner-product space and $S \subseteq V$ is orthogonal, as long as $0 \notin S$, we can easily replace S with an ortho*normal*[a] set by replacing every element of S with its normalization.

R In case it's not obvious, a "normed vector space" is a complex vector space equipped with a norm.

[a] See the following definition.

Definition 6.5.1.6 — Orthonormal Let V be an inner-product space and let $S \subseteq V$. Then, S is ***orthonormal*** iff S is orthogonal and every element of S is normalized.

R If we have an set $\{e_i : i \in \mathcal{I}\}$ indexed by another set $\mathcal{I}$, then the condition that this set be orthonormal is equivalent to the statement that

$$\langle e_i | e_j \rangle = \delta_{ij}. \tag{6.5.1.7}$$

Exercise 6.5.1.8 Let V be an inner-product space and let $S \subseteq V$ be orthonormal.

(i). Show that S is linearly-independent.
(ii). Why is this not true if you replace "orthonormal" with "orthogonal"?

Exercise 6.5.1.9 Show that

$$\left\{ \frac{1}{\sqrt{2\pi}} e^{inx} : n \in \mathbb{Z} \right\}$$

is orthonormal in $C^\infty([-\pi, \pi])$.

R In fact, it's an orthonormal *basis* in the space of periodic functions—see Example 6.5.2.51.

Exercise 6.5.1.10 Let V be an inner-product space, let $\{e_1, \ldots, e_d\} \subseteq V$ be an orthonormal basis of V, and let $\{v_1, \ldots, v_d\} \subseteq V$ be such that

$$\|v_k - e_k\| < \frac{1}{\sqrt{d}}$$

for $1 \leq k \leq d$. Show that $\{v_1, \ldots, v_d\}$ is a basis of V.[a]

[a] Adapted from [Axl15].

The notion of orthogonality allows us to state one of the most well-known theorems of all time.

Theorem 6.5.1.11 — Pythagorean Theorem. Let V be an inner-product space and let $S \subseteq V$ be orthogonal. Then,

$$\left\| \sum_{v \in S} v \right\|^2 = \sum_{v \in S} \|v\|^2. \tag{6.5.1.12}$$

R If $S =: \{v, w\}$ just as two elements, then this reduces to the statement that

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2. \tag{6.5.1.13}$$

Replacing w with $-w$, this reads

$$\|v - w\|^2 = \|v\|^2 + \|w\|^2. \tag{6.5.1.14}$$

Now, thinking of 0, v, and w as the vertices of a right triangle, $v - w$ is the hypotenuse, and using this language this is just the statement that the length of the hypotenuse square is the sum of the length of the "legs" squared. Hence, the ***Pythagorean Theorem***.

R In fact, the converse of the case of two vectors is true for *real* inner-product space: If V is a real inner-product space, then v and w are orthogonal iff $\|v + w\|^2 = \|v\|^2 + \|w\|^2$.

Proof. We leave this as an exercise.

Exercise 6.5.1.15 Prove the result.

■

6.5.2 Orthonormal bases

When working with Hilbert spaces, we are almost always going to want to have our bases be orthonormal. One of the most significant facts about working with an orthonormal basis is that it makes coordinates with respect to that basis essentially trivial to compute.

Proposition 6.5.2.1 Let V be an inner-product space, let $\mathcal{B}$ be an orthonormal basis of V, and let $v \in V$. Then,

$$|v\rangle = \sum_{b\in\mathcal{B}} |b\rangle \langle b|v\rangle. \tag{6.5.2.2}$$

R By the Pythagorean Theorem (Theorem 6.5.1.11), we have that

$$\|v\|^2 = \sum_{b\in\mathcal{B}} |\langle b|v\rangle|^2. \tag{6.5.2.3}$$

In particular:

> The coordinates of v with respect to $\mathcal{B}$ is an element of $\ell^2(\mathcal{B})$: $\langle \langle b|v\rangle : b \in \mathcal{B}\rangle \in \ell^2(\mathcal{B})$.

R Of course, from the definition (Definition 3.1.1), the coefficients here are the coefficients of v with respect to the basis $\mathcal{B}$. That is,

$$v^b = \langle b|v\rangle, \tag{6.5.2.4}$$

where v^b is the b-coordinate of v with respect to the basis $\mathcal{B}$.

R In non-bra-ket notation, this same equation reads

$$v = \sum_{b\in\mathcal{B}} \langle b|v\rangle b. \tag{6.5.2.5}$$

We present this as an example of translation here, but will refrain from doing so in the future. I will

use whichever notation I find more transparent and you can then write down the other version if you like. Usually this is quite trivial (e.g. remove the ⟨s, |s, and ⟩s). In this case, I find bra-ket notation more illuminating. The following remark elaborates on one reason why.

R This can be remembered as

$$\sum_{b\in\mathcal{B}} |b\rangle\langle b| = 1.^a \tag{6.5.2.6}$$

Recall that (Proposition 6.4.3.9) by default we equip $\mathrm{End}_{\mathbf{TopVect}_{\mathbb{C}}}(V)$ with the topology of pointwise convergence, and so what this really means is that, for every $v \in V$, $\sum_{b\in\mathcal{B}} |b\rangle\langle b|v\rangle$ converges to v. This, however, is just the conclusion of the result (6.5.2.2).

R We will generalize this later in Proposition 6.6.5.18. Proposition 6.6.5.18 gives an expression for computing projections onto closed subspaces, and it turns out that this result is the special case of that one when projecting onto V itself.

R In fact, this is actually equivalent to $\mathcal{B}$ being an orthonormal basis—see Theorem 6.5.2.8.

[a] Where of course "1" here really means "id_V".

Proof. We leave this as an exercise.

Exercise 6.5.2.7 Prove the result.

■

This is one reason why orthonormal bases are so convenient, and so it is of interest to know whether every inner-product spaces has an orthonormal basis. The answer is "No." for inner-product spaces in general, but "Yes." for Hilbert spaces. To see this, we first give several equivalent characterizations of orthonormal bases in a Hilbert space.

Theorem 6.5.2.8 — Characterization of orthonormal bases. Let V be a Hilbert space and let $\mathcal{B} \subseteq V$ be orthonormal. Then, the following are equivalent.

(i). $\mathcal{B}$ is an orthonormal basis.
(ii). $\text{Cls}(\text{Span}(\mathcal{B})) = V$.
(iii).

$$|v\rangle = \sum_{b\in\mathcal{B}} |b\rangle \langle b|v\rangle \tag{6.5.2.9}$$

for all $v \in V$.
(iv).

$$\|v\|^2 = \sum_{b\in\mathcal{B}} |\langle b|v\rangle|^2 \tag{6.5.2.10}$$

for all $v \in V$.
(v). $\mathcal{B}^\perp = 0$.
(vi). $\mathcal{B}$ is a maximal orthonormal subset of V.

R As $\text{Cls}(\text{Span}(\mathcal{B}))$ is the topological span of $\mathcal{B}$ (Theorem 6.4.3.20) and $\mathcal{B}$ is automatically linearly-independent (Exercise 6.5.1.4), the equivalence of (ii) can be roughly thought of as the statement that "An orthonormal set is a basis iff it is linearly-independent and spanning.".

R Note that (iii) is essentially just Proposition 6.5.2.1.

R ***Bessel's Inequality*** states that, for a Hilbert space V, $S \subseteq V$ orthonormal, and $v \in V$,

$$\|v\|^2 \geq \sum_{s\in S} |\langle s|v\rangle|^2. \tag{6.5.2.11}$$

Thus, according to (iv), an orthonormal subset is a basis iff we always have equality in Bessel's Inequality.

For what it's worth, I would not bother remembering Bessel's Inequality itself. Instead, just remember (iv)—Bessel's Inequality then follows easily because you can always extend an orthonormal set to a basis (Proposition 6.5.2.29).

R As $\langle\cdot|\cdot\rangle\colon \bar{V}\times V\to\mathbb{C}$ is a dual pair, given $S\subseteq V$, recall that (Definition 5.2.2.17) $S^\perp$ is defined by

$$S^\perp := \{v\in\bar{V} : \langle v|b\rangle = 0\}. \tag{6.5.2.12}$$

Hence, explicitly, (v) is the statement that $\langle v|b\rangle$ for all $b\in\mathcal{B}$ implies $v=0$.

R Compare (vi) with Proposition 2.2.8.[a] There is only the analogue of maximal linearly-independent here as orthonormal sets are automatically linearly-independent (Exercise 6.5.1.4).

[a] This is the result that says that being a basis is the same as being maximal linearly-independent is the same as being minimal spanning.

Proof. We leave this as an exercise.

Exercise 6.5.2.13 Prove the result.

■

Theorem 6.5.2.14 — Hilbert spaces have orthonormal bases. Let V be an inner-product space. Then, if V is a Hilbert space, it has an orthonormal basis.

R Warning: The converse is false—see Example 6.5.2.22. You might be tempted to pick an orthonormal basis $\mathcal{B}$ and define a map $V\to\ell^2(\mathcal{B})$ via $v\mapsto\langle\langle b|v\rangle : b\in\mathcal{B}\rangle$; however, this map may not have an inverse, as, if V is not complete, there is no guarantee that

$$\ell^2(\mathcal{B})\ni a\mapsto\sum_{b\in\mathcal{B}} a^b\cdot b \tag{6.5.2.15}$$

makes sense (it's possible this sum doesn't converge in V).

R Warning: This fails if your inner-product space is not complete—see Example 6.5.2.27.

Proof. We leave this as an exercise.

Exercise 6.5.2.16 Prove the result.

R Hint: Use Zorn's Lemma (Theorem A.3.5.9) together with the previous result.

■

▪ **Example 6.5.2.17 — Legendre polynomials** Define $V := \mathbb{C}[x]$ equipped with the inner-product $\langle \cdot | \cdot \rangle \colon \bar{V} \times V \to \mathbb{C}$ defined by

$$\langle f | g \rangle := \int_{-1}^{1} \mathrm{d}x \, f(x)^* g(x). \tag{6.5.2.18}$$

For $m \in \mathbb{N}$, the degree m ***Legendre polynomial*** is given by[a]

$$\frac{1}{2^m m!} \frac{\mathrm{d}^m}{\mathrm{d}x^m} [(x^2 - 1)^m]. \tag{6.5.2.19}$$

Exercise 6.5.2.20 Show that the set of Legendre polynomials constitutes an orthonormal basis for V.

R The degree m Legendre polynomial is an eigenvector with eigenvalue $m(m+1)$ of the linear operator $T \colon V \to V$ defined by

$$[T(f)](x) := -\frac{\mathrm{d}}{\mathrm{d}x} \left[(1 - x^2) \frac{\mathrm{d}}{\mathrm{d}x} f(x) \right]. \tag{6.5.2.21}$$

Once we know more theory, we will be able to immediately deduce the that the Legendre polynomials are orthonormal with no extra computation—see Exercise 6.7.2.14. In fact, using even more theory, one can immediately deduce that this forms an orthonormal *basis*.

[a] This is ***Rodrigues' formula*** for Legendre polynomials.

▪ **Example 6.5.2.22 — An incomplete inner-product space that has an orthonormal basis**

$$\{e_m : m \in \mathbb{N}\} \tag{6.5.2.23}$$

is an orthonormal basis for $\mathbb{C}^\infty$, which is not complete. For example,

$$m \mapsto \sum_{k=0}^{m} \tfrac{1}{m+1} e_k \tag{6.5.2.24}$$

is Cauchy in $\mathbb{C}^\infty$ but does not converge.

Exercise 6.5.2.25 Verify that (6.5.2.23) is indeed an orthonormal basis of $\mathbb{C}^\infty$.

Exercise 6.5.2.26 Verify that (6.5.2.24) is indeed a Cauchy sequence which does not converge in $\mathbb{C}^\infty$.

▪ **Example 6.5.2.27 — An inner-product space with no basis**

Exercise 6.5.2.28 Find an example of an inner-product space with no basis.

R Hint: See http://math.gmu.edu/~tlim/NoOrthonormalBasis.pdf.

Proposition 6.5.2.29 Let V be a Hilbert space and let $S \subseteq V$. Then, if S is orthonormal, then there is a superset of S that is an orthonormal basis.

R Compare Proposition 2.2.17. Note that there can only be an analogue of the linearly-independent state-

ment as orthonormal sets are automatically linearly-independent.

Proof. We leave this as an exercise.

Exercise 6.5.2.30 Prove the result.

■

You'll recall that (see immediately before Theorem 2.2.25) when studying bases before, we noted that they were important for at least three reasons. One reason was that they allowed us to define dimension, and another reason is that they allowed us to define coordinates of linear-transformations. The third reason they are important is that they provide a convenient way to *define* linear-transformations (Theorem 2.2.25): if you tell me where every basis element maps to, then you have defined a linear-transformation. In the context of inner-product spaces, there is no need to change or generalize the definitions of dimension or coordinates. However, we do have an analogue of Theorem 2.2.25 for orthonormal bases.

Theorem 6.5.2.31 — Linear-transformations and orthonormal basis of domain. Let V and W be inner-product spaces, let $\mathcal{B}$ be an orthonormal basis for V, and for every $b \in \mathcal{B}$ let $w_b \in W$ be some vector in W. Then, there exists a unique continuous linear-transformation $T : V \to W$ such that $T(b) = w_b$ for all $b \in \mathcal{B}$ iff (i) $\sum_{b\in\mathcal{B}} v^b \cdot w_b$ converges for all $\langle v^b : b \in \mathcal{B}\rangle \in \ell^2(\mathcal{B})$ and (ii) $\sup\{\|w_b\| : b \in \mathcal{B}\} < \infty$.

Furthermore, in this case,

$$\|T\| = \sup\{\|w_b\| : b \in \mathcal{B}\}. \tag{6.5.2.32}$$

R Just as in Theorem 2.2.25, this result says that we can define a continuous-linear transformation between inner-product spaces by specifying what it does to an orthonormal basis. The catch is that the values we

chose now can't be totally arbitrary—we now have to worry about convergence.

R Intuitively, we need (i) in order that any such linear-transformation exists at all, and we need (ii) to guarantee that this linear-transformation is continuous.

Note that we cannot deduce the existence of T from Theorem 2.2.25 because, as explained immediately before Subsection 6.4.3, the results before were essentially proved for discrete vector spaces, and here V and W will almost never be discrete.

R Warning: Only one of these two conditions is not enough. To see that it is not enough that $\sum_{b\in\mathcal{B}} v^b \cdot w_b$ converges for all $\langle v^b : b \in \mathcal{B}\rangle \in \ell^2(\mathcal{B})$, see Example 6.5.2.46. To see that it is not enough that $\sup\{\|w_b\| : b \in \mathcal{B}\}$ be finite, see Example 6.5.2.48.

Proof. ($\Rightarrow$) Suppose that T is continuous. Let $\langle v^b : b \in \mathcal{B}\rangle \in \ell^2(\mathcal{B})$ and define

$$v := \sum_{b\in\mathcal{B}} v^b \cdot b \in V. \tag{6.5.2.33}$$

As T is continuous, it preserves limits, and so we have that

$$T(v) = \sum_{b\in\mathcal{B}} v^b \cdot T(b) = \sum_{b\in\mathcal{B}} v^b \cdot w_b, \tag{6.5.2.34}$$

and in particular, the sum here converges.

Furthermore, by Theorem 6.4.3.11 T is bounded, and so

$$\|T(w_b)\| = \|T(b)\| \leq \|T\|\|b\| = \|T\|, \tag{6.5.2.35}$$

and hence

$$\sup\{\|w_b\| : b \in \mathcal{B}\} \leq \|T\| < \infty. \tag{6.5.2.36}$$

($\Leftarrow$) Suppose that (i) $\sum_{b\in\mathcal{B}} v^b \cdot w_b$ converges for all $\langle v^b : b \in \mathcal{B}\rangle \in \ell^2(\mathcal{B})$ and that (ii) $\sup\{\|w_b\| : b \in \mathcal{B}\} < \infty$. Let $v \in V$

and write

$$v = \sum_{b \in \mathcal{B}} v^b \cdot b \tag{6.5.2.37}$$

for unique $v^b \in \mathbb{C}$. Note that $\langle v^b : b \in \mathcal{B} \rangle \in \ell^2(\mathcal{B})$ by the remark in Proposition 6.5.2.1.

By (i), we may thus define $T : V \to W$ by

$$T(v) := \sum_{b \in \mathcal{B}} v^b \cdot w_b. \tag{6.5.2.38}$$

Exercise 6.5.2.39 Check that T is a linear-transformation.

It remains to check that T is continuous. To do so, using Theorem 6.4.3.11, we instead show that T is bounded. Write

$$w_b = \sum_{c \in \mathcal{B}} w^c{}_b \cdot c \tag{6.5.2.40}$$

for unique $w^c{}_b \in \mathbb{C}$. Note that

$$\|w_b\|^2 = \sum_{c \in \mathcal{B}} |w^c{}_b|^2. \tag{6.5.2.41}$$

Now, look at

$$\begin{aligned}
\|T(v)\|^2 &= \left\| \sum_{b\in\mathcal{B}} v^b \cdot \left(\sum_{c\in\mathcal{B}} w^c{}_b \cdot c \right) \right\| \\
&= \left\| \sum_{c\in C} \left(\sum_{b\in\mathcal{B}} w^c{}_b \cdot v^b \right) \cdot c \right\| \\
&= \sum_{c\in C} \left| \sum_{b\in\mathcal{B}} w^c{}_b \cdot v^b \right|^2 \\
&\leq^a \sum_{b\in\mathcal{B}} \sum_{c\in C} \left| w^c{}_b v^b \right|^2 \\
&= \sum_{b\in\mathcal{B}} \|w_b\|^2 \left| v^b \right|^2 \\
&\leq C^2 \sum_{b\in\mathcal{B}} \left| v^b \right|^2 \\
&= C^2 \|v\|^2,
\end{aligned} \tag{6.5.2.42}$$

where we have written

$$\begin{aligned}
C^2 &:= \sup\{\|w_b\|^2 : b \in \mathcal{B}\} \\
&= (\sup\{\|w_b\| : b \in \mathcal{B}\})^2 < \infty.
\end{aligned} \tag{6.5.2.43}$$

It follows that

$$\|T(v)\| \leq C\|v\|, \tag{6.5.2.44}$$

and so by definition (Theorem 6.4.3.11), T is bounded.

For the "Furthermore. . . " part of the result, assume that these equivalent statements are true. From (6.5.2.35), $\|T\| \geq C$. On the other hand, from (6.5.2.44), we have $\|T\| \leq C$. Hence,

$$\|T\| = C := \sup\{\|w_b\| : b \in \mathcal{B}\}. \tag{6.5.2.45}$$

■

[a] By Minkowski's Inequality (Theorem 6.4.4.3).

▪ **Example 6.5.2.46**

Exercise 6.5.2.47 Find $\{w_m : m \in \mathbb{N}\} \subseteq \ell^2(\mathbb{N})$ such that (i) $\sum_{m\in\mathbb{N}} v^m \cdot w_m \in \ell^2(\mathbb{N})$ converges for all $\langle v^m : m \in \mathbb{N}\rangle \in \ell^2(\mathbb{N})$ but (ii)

$$\ell^2(\mathbb{N}) \ni \langle v^m : m \in \mathbb{N}\rangle \mapsto \sum_{m\in\mathbb{N}} v^m \cdot w_m \in \mathbb{C}$$

does *not* define a continuous linear-transformation.

R Hint: See mathoverflow.

▪ **Example 6.5.2.48** For $m \in \mathbb{N}$, define $w_m := e_0 := \langle 1, 0, 0, \ldots\rangle$. Then, certainly $\sup\{\|w_m\| : m \in \mathbb{N}\} = 1 < \infty$. On the other hand, $\langle 1, 1/2, 1/3, \ldots\rangle \in \ell^2(\mathbb{N})$, but

$$\sum_{m\in\mathbb{N}} \tfrac{1}{m+1} w_m = \left(\sum_{m\in\mathbb{N}} \frac{1}{m+1}\right) e_0 \tag{6.5.2.49}$$

doesn't even converge, and so

$$T(v) := \sum_{m\in\mathbb{N}} v^m \cdot e_m \tag{6.5.2.50}$$

doesn't even define a linear-transformation $\ell^2(\mathbb{N}) \to \ell^2(\mathbb{N})$.

Let us end with a particularly important example related to Fourier analysis.

▪ **Example 6.5.2.51 — Fourier series** Define

$$V := \left\{ f \in C^\infty([-\pi, \pi]) : f^{(k)}(\pi) = f^{(k)}(-\pi) \text{ for all } k \in \mathbb{N}. \right\}$$

to be the inner-product space of 2π-periodic functions.[a]

It follows that

$$\left\{ \tfrac{1}{\sqrt{2\pi}} e^{inx} : n \in \mathbb{Z} \right\} \tag{6.5.2.52}$$

is an orthonormal basis for V (in fact, you already checked in Exercise 6.5.1.9 that it's orthonormal). To condense notation, let us write

$$e_n(x) \coloneqq \frac{1}{\sqrt{2\pi}} e^{inx}. \tag{6.5.2.53}$$

As this is an orthonormal *basis*, given $f \in V$, we can write

$$f(x) = \frac{1}{\sqrt{2\pi}} \sum_{n\in\mathbb{Z}} \langle e_n | f \rangle e^{\in nx}. \tag{6.5.2.54}$$

From the definition of the inner-product,

$$\langle e_n | f \rangle \coloneqq \frac{1}{\sqrt{2\pi}} \int_{-\pi}^{\pi} dx\, e^{-inx} f(x). \tag{6.5.2.55}$$

If you've studied Fourier series before, you probably recognize this.

The point to take home is that you needn't memorize the formulae for Fourier series. Instead:

> The Fourier coefficients can be computed using using the fact that the coordinates with respect to an orthonormal basis are given by $\langle b|v\rangle$ (Proposition 6.5.2.1) together with the fact that
>
> $$\left\{ \tfrac{1}{\sqrt{2\pi}} e^{inx} : n \in \mathbb{Z} \right\} \tag{6.5.2.56}$$
>
> is an orthonormal basis for the space of periodic functions.

[a] Incidentally, this is not usually the space used in this context (because it's not a Hilbert space). It's much more common to work with the space called $L^2(S^1)$. We avoid this so that you can follow this example without first being familiar with L^2.

6.6 The projection onto a closed convex subset and its corollaries

Let V be an inner-product space, let $T\colon V \to V$ be linear, and let $y_0 \in V$. We know by now that the equation $T(x) = y_0$ may or may not have a solution (it has a solution iff T is surjective). However, an inner-product gives us, among other things, a notion of distance, and so we can ask the question "If we can't find an $x \in V$ such that $T(x) = y_0$, is it then possible to just find an $x \in V$ such that $T(x)$ is as close to y_0 as possible.". The answer to this question is, under sufficient hypotheses (which are always satisfied in finite-dimensions), "Yes.".

6.6.1 The result

We begin with one of the most important results in the foundations of the theory.[20]

Definition 6.6.1.1 — Convex Let $\mathbb{K}$ be a preordered ring, let V be a $\mathbb{K}$-module, and let $C \subseteq V$. Then, V is ***convex*** iff for every $v, w \in V$,

$$\{(1-t)v + tw : t \in [0,1]\} \subseteq C. \tag{6.6.1.2}$$

R Don't get frightened by this "preordered ring" business—we're only going to be using this in the case $\mathbb{K} = \mathbb{C}$ anyways. We just need an order so that the statement "$0 \leq t \leq 1$" makes sense.

R The set appearing in (6.6.1.2) should be thought of as the line segment from v to w. Thus, a set is convex iff it contains the line segment connecting any two of its points.

R Thus, note in particular that subspaces are always convex.

[20] I can't say I've seen it used directly so much, but it has a couple corollaries which are themselves fundamental to the theory.

Theorem 6.6.1.3. Let V be a Hilbert space, let $C \subseteq V$ be nonempty closed convex, and let $v \in V$.. Then, there exists a unique $v_0 \in C$ such that

$$\|v - c_0\| \leq \|v - c\| \tag{6.6.1.4}$$

for all $c \in C$.

R In words, C has a unique element closest to v_0.

R This result (together with the one regarding the existence of orthonormal bases Theorem 6.5.2.14) explains in large part why the hypothesis of "completeness" is so ubiquitous in the subject—it's because these two results are used (either explicitly or implicitly) so much.

Proof. We leave this as an exercise.

Exercise 6.6.1.5 Prove the result.

R Hint: See [B C90, Theorem I.2.5].

■

6.6.2 The orthogonal complement decomposition

In case C is a closed subspace, in which case we write W in place of C suggestively, this unique element in W closest to v will be called the *projection* of v onto W. There's just one itsy-bitsy problem with this—we've already defined projections (Proposition 4.4.1.49)! If we want this element to be called the projection, we had better check that these two notions coincide. In order for the other notion we met back in Chapter 4 to make sense, however, we first require a direct-sum decomposition of V.

Corollary 6.6.2.1 Let V be a Hilbert space and let $W \subseteq V$ be a closed subspace. Then,

$$V = W \oplus W^{\perp}. \tag{6.6.2.2}$$

R In particular,

$$v = \mathrm{proj}_W(v) + \mathrm{proj}_{W^{\perp}}(v) \tag{6.6.2.3}$$

for all $v \in V$.

R Warning: This may fail if either V is not a Hilbert space or W is not closed—see Exercise 6.6.2.8 and Example 6.6.2.9.

Proof. We apply Corollary 4.4.1.28, which says that it suffices to show that (i) $V = W + W^{\perp}$ and (ii) $W \cap W^{\perp} = 0$.

We first check that $W \cap W^{\perp} = 0$ because it is quick. Let $v \in W \cap W^{\perp}$. Then, $\langle v|v\rangle = 0$, and hence $\|v\|^2 = 0$, and hence $v = 0$.

We now check that $V = W + W^{\perp}$. Let $v \in V$. As W is closed and convex, by the previous result, there is a unique $w_0 \in W$ such that

$$\|v - w_0\| \leq \|v - w\| \tag{6.6.2.4}$$

for all $w \in W$. We of course have that $v = w_0 + (v - w_0)$, and so it suffices to show that $v - w_0 \in W^{\perp}$. To do this, it suffices to show that $v - w_0$ is orthogonal to $w - w_0$ for all $w \in W$, then it is orthogonal to $(w + w_0) - w_0 = w$ for all $w \in W$. Thus, without loss of generality, we may assume that $w_0 \in W$. We then wish to show that $v \in W^{\perp}$.

We proceed by contradiction: suppose that there is some $w \in W$ with $\langle v|w\rangle \neq 0$. Replacing w with $\mathrm{i}w$ if necessary, we may assume without loss of generality that $\Re[\langle v|w\rangle] \neq 0$. Similarly, replacing w with $-w$ if necessary, we may assume

without loss of generality that $\Re[\langle v|w\rangle] > 0$. Then, for every $\varepsilon > 0$,

$$\|v - \varepsilon w\|^2 = \|v\|^2 - 2\varepsilon\Re[\langle v|w\rangle] + \varepsilon^2\|w\|^2. \quad (6.6.2.5)$$

As $\Re[\langle v|w\rangle] > 0$, we can choose ε sufficiently small so that[a]

$$-2\varepsilon\Re[\langle v|w\rangle] + \varepsilon^2\|w\|^2 < 0. \quad (6.6.2.6)$$

But then $\|v - \varepsilon w\|^2 < \|v\|^2$: a contradiction of the fact that $0 \in W$ was the element of W closest to v. Thus, it must indeed be the case that $v \in W^\perp$, as desired.

$$|\langle v - w_0|w\rangle| \leq \|v - v_0\|\|w\| \leq \|v - w\|\|w\| \quad (6.6.2.7)$$

■

[a] The intuition is that the second term goes to 0 faster, and so eventually it will be dominated by the term with $-2\varepsilon\Re[\langle v|w\rangle]$.

Exercise 6.6.2.8 — $V \neq W \oplus W^\perp$, W closed Can you find an example of an inner-product space V with a closed subspace $W \subseteq V$ such that $V \neq W \oplus W^\perp$?

■ **Example 6.6.2.9 — $V \neq W \oplus W^\perp$, V a Hilbert space** Take $V := \ell^2(\mathbb{N})$ and $W := \mathbb{C}^\infty$. We claim that $W^\perp = 0$. To see this, let $a \in W^\perp$. As $e_m \in \mathbb{C}^\infty$ for all $m \in \mathbb{N}$, we must have that $\langle a|e_m\rangle = 0$ for all $m \in \mathbb{N}$. However, $\langle a|e_m\rangle = a_m$, and so this condition implies that $a = 0$, as desired.

Thus, given a direct-sum decomposition $V = W \oplus W^\perp$, we now have projections proj_W and $\text{proj}_{W^\perp}$ with respect to this decomposition. As mentioned before, $\text{proj}_W(v)$ coincides with the element in W closest to v.

Theorem 6.6.2.10 — Characterizations of proj_W. Let V be a Hilbert space, let $W \subseteq V$ be a closed subspace, and let $v \in V$.

(i). $\text{proj}_W(v) \in W$ is the unique element of W such that

$$\left\|v - \text{proj}_W(v)\right\| \leq \|v - w\| \tag{6.6.2.11}$$

for all $w \in V$.

(ii). $\text{proj}_W(v) \in W$ is the unique element of W such that $v - \text{proj}_W(v) \in W^\perp$.

Proof. (i) We leave this as an exercise.

Exercise 6.6.2.12 Prove the result.

(ii) We first check that $v - \text{proj}_W(v) \in W^\perp$. Using $V = W \oplus W^\perp$, we may write $v - \text{proj}_W(v) = x + y$ for unique $x \in W$ and $y \in W^\perp$. We wish to show that $x = 0$. We proceed by contradiction: suppose that $x \neq 0$. If this is true, then $\text{proj}_W(v) + x \in W$ is closer to v than $\text{proj}_W(v)$, for

$$\left\|v - \text{proj}_W(v)\right\|^2 = \|x\|^2 + \|y\|^2 > \|y\|^2, \tag{6.6.2.13}$$

but

$$\left\|v - (\text{proj}_W(v) + x)\right\|^2 = \|y\|^2, \tag{6.6.2.14}$$

a contradiction. Thus, $x = 0$, as desired.

To see uniqueness, let $u \in W$ be another element such that $v - u \in W^\perp$. Then, $v = u + (v - u)$, $u \in W$, and $v - u \in W^\perp$, and so we must have $u = \text{proj}_W(v)$ and $v - u = \text{proj}_{W^\perp}(v)$. ■

We plan to return to both orthogonal-complements and projections later to discuss some of their properties (Propositions 6.6.5.1 and 6.6.5.10), but as some of these properties of interest involves the discussion of the *adjoint*, we first discuss this very important concept.

6.6.3 The adjoint

The adjoint of a linear operator (Theorem 6.6.3.29) is really just the transpose (Definition 5.2.2.8) with respect to the nonsingular dual-pair

$\bar{V} \times V \to \mathbb{C}$. To use this then, we must first check that dual-pair defined by an inner-product is nonsingular. Unfortunately, that's just not true (Example 6.6.3.12); *however*, it is true if the inner-product space is a Hilbert space, and that is the statement of the *Riesz Representation Theorem*.

The Riesz Representation Theorem

Perhaps the most important theorem of all the 'basic' results of Hilbert space theory is what is known as the *Riesz Representation Theorem*, and it characterizes the dual-space. An inner-product space V is by definition a dual-pair $\bar{V} \times V \to \mathbb{C}$, and we know that (Definition 5.2.2.2) for any dual-pair, we obtain corresponding maps $V \to \bar{V}^\dagger$ and $\bar{V} \to V^\dagger$, given by $v \mapsto \langle \cdot | v \rangle$ and $\bar{v} \mapsto \langle v | \cdot \rangle$ respectively.[21] The Riesz Representation Theorem states that these are isomorphisms.

Theorem 6.6.3.1 — Riesz Representation Theorem. Let V be a Hilbert space. Then,

$$V \ni v \mapsto \langle \cdot | v \rangle \in \bar{V}^\dagger \text{ and } \bar{V} \in \bar{v} \mapsto \langle v | \cdot \rangle \in V^\dagger \quad (6.6.3.2)$$

are norm-preserving isomorphisms.

R "Norm-preserving" here means that $\|v\| = \|\langle \cdot | v \rangle\|$ and $\|\bar{v}\| = \|\langle v | \cdot \rangle\|$. A more common adjective for this would be *unitary*, but as we haven't defined unitary operators yet (Definition 6.6.4.9), we stick with "norm-preserving" here.

R In brief, $V^\dagger \cong \bar{V}$. In particular, as the elements of $\bar{V}$ are the same as the elements of V,[a] every $v \in V$ defines a linear-functional. In bra-ket notation, the map that sends a vector to its corresponding linear-functional is given by

$$|v\rangle \mapsto \langle v| \,. \quad (6.6.3.3)$$

[21] Note that the bar is needed here so that the map is *linear* instead of *conjugate*-linear.

R Alternatively, if you prefer, you can think of this as the statement that $V^\dagger \cong V$, with the caveat that the isomorphism is *conjugate*-linear.

In practice, I think it's best to think of V being canonically isomorphic to its dual, relegating the fact that this isomorphism is conjugate-linear to the back of your mind.

R In other words, $\langle\cdot|\cdot\rangle\colon \bar{V} \times V \to \mathbb{C}$ is a nonsingular dual-pair.

R Warning: Recall that (Definition 6.4.3.15) $V^\dagger$ is the space of *continuous* linear-functionals on V (and likewise for $\bar{V}^\dagger$).

R Thus, up to a complex-conjugation,[b] $\langle\cdot|\cdot\rangle$ is a metric. Let us then suggestively write $g_{\bar{a}b}$ in index notation to denote the $\langle 0, 2\rangle$ tensor defined on V, the bar on the a indicating to us that it is *conjugate*-linear in that argument and not linear.[c] It is defined in terms of $\langle\cdot|\cdot\rangle$ by

$$\langle v|w\rangle =: g_{\bar{a}b} v^{\bar{a}} w^b. \tag{6.6.3.4}$$

As before, we have an inverse $g^{a\bar{b}}$ that,[d] by definition, satisfies

$$g^{a\bar{x}} g_{\bar{x}b} = \delta^a{}_b \text{ and } g_{\bar{a}x} g^{x\bar{b}} = \delta_{\bar{a}}{}^{\bar{b}}. \tag{6.6.3.5}$$

We can thus $g_{\bar{a}b}$ and $g^{\bar{a}b}$ to raise and lower indices similarly as before: for $v^a \in V$ and $w_{\bar{a}} \in \bar{V}^\dagger$, we write

$$v_{\bar{a}} := g_{\bar{a}x} v^x \text{ and } w^a := g^{a\bar{x}} w_{\bar{x}}; \tag{6.6.3.6}$$

and for $v^{\bar{a}} \in \bar{V}$ and $w_a \in V^\dagger$, we write

$$v_a := v^{\bar{x}} g_{\bar{x}a} \text{ and } w^{\bar{a}} := w_x g^{x\bar{a}}. \tag{6.6.3.7}$$

Thus, you can raise and lower indices like normal, except when you do you add / remove a bar.

Having introduced this, (6.6.3.4) can be rewritten as

$$v_x w^x = \langle v|w\rangle = v^{\bar{x}} w_{\bar{x}}. \tag{6.6.3.8}$$

Incidentally, going from v^a to $v_{\bar{a}}$ in index notation corresponds to going from $|v\rangle$ to $\langle v|$ in bra-ket notation.

For what it's worth, index notation is rarely used in this context as the complex-conjugation makes it easy to make mistakes. For example,

$$\langle \mathrm{i}\, v|w\rangle = -\mathrm{i}\langle v|w\rangle, \tag{6.6.3.9}$$

but naively using the index notation as in (6.6.3.8), this becomes

$$\mathrm{i}\, v_x w^x = -\mathrm{i}\, v_x w^x, \tag{6.6.3.10}$$

which is obviously incorrect.

Thus, we will almost certainly refrain from using index notation in the context of Hilbert spaces, but it is a good check of understanding to see if all this makes sense.

R Furthermore, there is essentially only one map here in that one is obtained from the other by taking the complex conjugate.

R Warning: There are other results that are also referred to as the "Riesz Representation Theorem".

---

[a] The only difference is the scalar multiplication in these two spaces differ by a complex conjugate.

[b] By this I mean that $\langle\cdot|\cdot\rangle$ is *conjugate*-symmetric, whereas metrics are supposed to be symmetric.

[c] More common notation uses a dot (because reasons?): $g_{\dot{a}b}$.

[d] In fact, the Riesz Representation Theorem is the statement that such an inverse exists.

Proof. We show that $V \to \bar{V}^\dagger$ is an isomorphism. The other one is similar. It is automatically injective as these are vector spaces (Proposition 5.2.2.6), and so it suffices to prove surjectivity. So, let $\phi\colon \bar{V} \to \mathbb{C}$ be linear and continuous. Instead, we may consider $\phi\colon V \to \mathbb{C}$ as conjugate-linear and continuous.

By virtue of Theorem 6.5.2.14, V has an orthonormal basis $\mathcal{B}$. Define

$$v_0 \coloneqq \sum_{b\in\mathcal{B}} \phi(b)\cdot b. \tag{6.6.3.11}$$

■

■ **Example 6.6.3.12 — An inner-product space that is not a Hilbert space** We saw in Example 6.3.1.13 that $C^\infty([-1,1])$ is an inner-product space with inner-product given by

$$\langle f\,|\,g\rangle \coloneqq \int_{-1}^{1} \mathrm{d}x\, f(x)^* g(x). \tag{6.6.3.13}$$

We claim that this inner-product space is not a Hilbert space.

Define $\phi\colon C^\infty([-1,1]) \to \mathbb{C}$ by

$$\phi(f) \coloneqq \int_{0}^{1} \mathrm{d}x\, f(x). \tag{6.6.3.14}$$

Exercise 6.6.3.15 Show that ϕ is a continuous linear-functional on $C^\infty([-1,1])$.

R That it is linear is more or less obvious. The difficulty is in proving that it is *continuous*.

Exercise 6.6.3.16 Show that there is no $g \in C^\infty([-1,1])$ such that

$$\int_{-1}^{1} \mathrm{d}x\, g(x)^* f(x) =: \langle g \,|\, f\rangle = \phi(f) := \int_0^1 \mathrm{d}x\, f(x). \tag{6.6.3.17}$$

for all $f \in C^\infty([-1,1])$.

R Hint: Intuitively, if this were true, then we should have

$$g(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{if } x < 0. \end{cases} \tag{6.6.3.18}$$

Thus, try to show that any g that has this property would be discontinuous (and so not in $C^\infty([-1,1])$.

We have thus exhibited a continuous linear-functional on V that is not of the form $\langle g\,|\cdot\rangle$. Thus, V cannot be a Hilbert space (or else it would exhibit a counter-example to the Riesz Representation Theorem).

Exercise 6.6.3.19 Show that $\mathbb{C}[x]$ with inner-product as in Example 6.3.1.16 defined by

$$\langle p \,|\, q\rangle := \int_{\mathbb{R}} \mathrm{d}x\, p(x)^* q(x) \mathrm{e}^{-x^2/2}. \tag{6.6.3.20}$$

is not a Hilbert space.

The adjoint itself

Definition 6.6.3.21 — Adjoint Let V and W be inner-product spaces and let $T: V \to W$ be a continuous linear-transformation. Then, a continuous linear-transformation $T^*: W \to V$ is the ***adjoint*** of T iff

$$\langle T^*(w)|v\rangle = \langle w|T(v)\rangle \tag{6.6.3.22}$$

for all $v \in V$ and $w \in W$.

R The term ***Hermitian conjugate*** is sometimes used synonymously with "adjoint".

R Note that if such an operator does exist, this property uniquely defines it: if $\langle T^*(w)|v\rangle = \langle S(w)|v\rangle$ for all $v \in V$, then in particular $\langle T^*(w) - S(w)|v\rangle = 0$ for $v = T^*(w) - S(w)$, which forces $T^*(w) = S(w)$.

R Taking the complex conjugate of this equation yields

$$\langle T(v)|w\rangle = \langle v|T^*(w)\rangle, \tag{6.6.3.23}$$

so that $T = [T^*]^*$.

R Warning: Adjoints need not exist between general inner-product spaces (Example 6.6.3.32)—one must assume the inner-product spaces are Hilbert space.

▪ **Example 6.6.3.24 — Adjoint of the derivative** Define

$$V := \{f \in C^\infty([-1,1]) : f(\pm 1) = 0\} \tag{6.6.3.25}$$

and $D: V \to C^\infty([-1,1])$ by $D(f) := f'$. We wish to compute the adjoint of D.

So, let $f \in V$ and $g \in C^\infty([-1,1])$. Then,

$$\begin{aligned}\langle g | D(f)\rangle &:= \int_{-1}^{1} \mathrm{d}x\, g(x)^* f'(x) \\ &=^{a} -\int_{-1}^{1} g'(x)^* f(x) =: \langle -D(g) | f\rangle,\end{aligned} \tag{6.6.3.26}$$

and hence $D^* = -D$. In the language of Definition 6.6.4.1, D is *anti-self-adjoint*.

R Incidentally, this problem illustrates what I think is a useful way to think about integration by parts. Integration by parts says that you can move a derivative inside an integral from one term to another at the cost of (i) a minus sign and (ii) some extra terms. A lot of the time in practice those extra terms vanish (as here), in which case integration by parts just reduces to "Moving the derivative from one term to the other introduces a minus sign.".

[a] The "boundary terms" vanish as $f(\pm 1) = 0$. Indeed, I defined V the way I did so that this computation works out.

▪ **Example 6.6.3.27 — Shift operators** Consider the left-shift and right-shift operators $L, R\colon \ell^2(\mathbb{N}) \to \ell^2(\mathbb{N})$ from Example 1.1.48. We wish to compute the adjoints of L and R.[a]

So, let $a, b \in \ell^2(\mathbb{N})$. Then,

$$\begin{aligned}\langle a | L(b)\rangle &:= \sum_{m\in\mathbb{N}} a_m^* [L(b)]_m := \sum_{m\in\mathbb{N}} a_m^* b_{m+1} \\ &=^{b} \sum_{n\in\mathbb{Z}^+} a_{n-1}^* a_n =: \sum_{n\in\mathbb{N}} [R(a)]_n^* b_n \\ &=: \langle R(a) | b\rangle.\end{aligned} \tag{6.6.3.28}$$

Thus, $L^* = R$, and so $R^* = [L^*]^* = L$.

[a] Spoiler alert: $L^* = R$ and $R^* = L$.
[b] Reindex and instead use $n := m + 1$.

Theorem 6.6.3.29 — Operators between Hilbert spaces have adjoints. Let V and W be Hilbert spaces, and let $T: V \to W$ be a continuous linear-transformation. Then, T has an adjoint.

R As $\bar{V} \times V \to \mathbb{C}$ and $\bar{W} \times W \to \mathbb{C}$ are nonsingular dual-pairs, the transpose of T is a linear map $T^\dagger: \bar{W} \to \bar{V}$. The adjoint is essentially the same but regarded as a map $W \to V$, that is,

$$\overline{T^\dagger} = T^* = \bar{T}^\dagger. \tag{6.6.3.30}$$

R Warning: Linear-transformations between inner-product spaces that are not Hilbert spaces need not have an adjoint—see the following example.

R Warning: Do not confuse *adjoint* with *adjugate* (Definition 5.7.2.90)—they are totally unrelated.

R If we ever do write T^*, unless otherwise stated, it should be implicit that we are assuming that T^* actually exists.

Proof. We leave this as an exercise.

Exercise 6.6.3.31 Prove the result.

R Hint: Use the Riesz Representation Theorem (Theorem 6.6.3.1).

■

▪ **Example 6.6.3.32 — A linear operator with no adjoint**

Exercise 6.6.3.33 Find an example of a linear operator that does not have an adjoint.

All of the basic properties of the adjoint are the same as those of the transpose (Proposition 5.2.2.12), except that now we have

$$[\alpha \cdot T]^* = \alpha^* \cdot T, \tag{6.6.3.34}$$

a simple consequence of the fact that $T = \overline{T^\dagger}$.

As with the transpose, you can give a concrete description of a matrix linear-transformation, and furthermore, that description coincides with the 'classical' notion for matrices.

Proposition 6.6.3.35 — Adjoint of a matrix Let V and W be finite-dimensional inner-product spaces, let $\mathcal{B} =: \{b_1, \ldots, b_d\}$ and $C =: \{c_1, \ldots, c_e\}$ be orthonormal bases for V and W respectively, and let $T : V \to W$ be linear. Then,

$$[T^*]_{\mathcal{B}^* \leftarrow \mathcal{B}^*} = [T]_{C \leftarrow \mathcal{B}}{}^*, \tag{6.6.3.36}$$

where we have defined

$$[A^*]^i{}_j := \bar{A}_{\bar{j}}{}^{\bar{i}} \tag{6.6.3.37}$$

for A an $e \times d$ matrix.

R A^* is the ***adjoint*** of A.

R Warning: Note that $\mathcal{B}$ and C are *orthonormal* bases. It need not hold for general bases—see Exercise 6.6.3.42.

R As with $A^\dagger$, the only thing that really matters are $\bar{A}$ itself and the order of the indices—the staggering and bars on the indices is only to be suggestive of how things would be written in abstract index notation. In particular, we could have written this as $[A^*]_{ij} := \bar{A}_{ji}$, though this is probably not the best practice.

R Thus, $A^* = \overline{A^\dagger} = \bar{A}^\dagger$. That is, to compute A^*, you take the complex conjugate of every entry and then take the transpose (or the other way around—the order doesn't matter here). For example,

$$\begin{bmatrix} 1+2\mathrm{i} & 3+4\mathrm{i} \\ 5+6\mathrm{i} & 7+8\mathrm{i} \end{bmatrix}^* = \begin{bmatrix} 1-2\mathrm{i} & 5-6\mathrm{i} \\ 3-4\mathrm{i} & 7-8\mathrm{i} \end{bmatrix}. \quad (6.6.3.38)$$

On the other hand,

$$\begin{bmatrix} 1+2\mathrm{i} & 3+4\mathrm{i} \\ 5+6\mathrm{i} & 7+8\mathrm{i} \end{bmatrix}^\dagger = \begin{bmatrix} 1+2\mathrm{i} & 5+6\mathrm{i} \\ 3+4\mathrm{i} & 7+8\mathrm{i} \end{bmatrix} \quad (6.6.3.39)$$

and

$$\overline{\begin{bmatrix} 1+2\mathrm{i} & 3+4\mathrm{i} \\ 5+6\mathrm{i} & 7+8\mathrm{i} \end{bmatrix}} = \begin{bmatrix} 1-2\mathrm{i} & 3-4\mathrm{i} \\ 5-6\mathrm{i} & 7-8\mathrm{i} \end{bmatrix}. \quad (6.6.3.40)$$

R We thus have three things we can do with matrices: take the transpose, take the complex conjugate, and take the adjoint, with the adjoint being the combination of the transpose and complex conjugate. These are denote respectively by $A^\dagger$, $\bar{A}$, and A^*.

Thinking of complex numbers themselves as 1×1 matrices, this means we have notions of $z^\dagger$, $\bar{z}$, and z^* for $z \in \mathbb{C}$. $z^\dagger = z$, so that's dumb, and $\bar{z} = z^*$. We have a tendency to write z^* for the complex conjugate instead of $\bar{z}$ because in general A^* is more useful than $\bar{A}$.

Proof. We leave this as an exercise.

Exercise 6.6.3.41 Prove the result.

■

Exercise 6.6.3.42 — $[T^*]_{\mathcal{B}} \neq [T]_{\mathcal{B}}{}^*$ Find an example of a finite-dimensional inner-product space V, a linear-

transformation $T: V \to V$, and a basis $\mathcal{B}$ of V such that

$$[T^*]_{\mathcal{B}} \neq [T]_{\mathcal{B}}{}^*.$$

6.6.4 Self-adjoint, nonnegative, unitary, and normal

The adjoint in many ways the analogue of complex conjugation for operators. In fact, it is a strict generalization if you regard complex numbers as defining linear-transformations (consider them as 1×1 matrices defining linear-transformations from $\mathbb{C}$ to itself). With this interpretation, we may introduce what you might say is the operator-theoretic analogue of being real: the notion of *self-adjoint*.

Definition 6.6.4.1 — (Anti-)Self-adjoint Let V and W be inner-product spaces and let $T: V \to W$ be a continuous linear-transformation.

(i). T is ***self-adjoint*** iff $T^* = T$.
(ii). T is ***anti-self-adjoint*** iff $T^* = -T$.

R Some use the term ***Hermitian*** synonymously with "self-adjoint" (just as "Hermitian conjugate" is used synonymously with "adjoint"). Likewise for ***anti-Hermitian*** and "anti-self-adjoint".

R If ever we use the adjective "self-adjoint" to describe a function between inner-product spaces, it should be understood that this is also meant to imply that function is linear and continuous. Similar conventions apply to "unitary", "normal", etc..

R Warning: There is a tendency to make the mistake that the composition of two self-adjoint operators must be self-adjoint. However, this is *not* the case—see Exercise 6.6.4.35. To see why this probably fails, try to prove it quickly: $[S \circ T]^* = T^* \circ S^* = T \circ S$, but there is no reason in general this need be the same as $S \circ T$.

R Incidentally, nearly everything we discuss regarding nonnegative, self-adjoint, unitary, and normal operators generalizes to the context of what are called *C^*-algebras*.

Just as we can decompose a complex number into its real and imaginary parts, we can do the same for operators.

Proposition 6.6.4.2 — Real and imaginary parts Let V be an inner-product space and let $T\colon V \to V$ be a continuous linear operator with adjoint $T^*\colon V \to V$. Then, there exist unique self-adjoint operators $\Re[T], \Im[T]\colon V \to V$, the ***real part*** and the ***imaginary part*** respectively, such that

$$T = \Re[T] + \mathrm{i}\,\Im[T]. \tag{6.6.4.3}$$

Furthermore,

(i). explicitly,

$$\Re[T] = \frac{T + T^*}{2} \text{ and } \Im[T] = \frac{T - T^*}{2\mathrm{i}}; \tag{6.6.4.4}$$

and

(ii). $\Re[T]$ and $\Im[T]$ commute iff T is normal.

R If it helps you to remember these formulae (or the trick for obtaining them), recall that $\mathrm{e}^{\mathrm{i}x} = \cos(x) + \mathrm{i}\sin(x)$ and think what the expressions are for $\cos(x)$ and $\sin(x)$ in terms of $\mathrm{e}^{\mathrm{i}x}$ and $\mathrm{e}^{-\mathrm{i}x}$.

Proof.

Exercise 6.6.4.5 Check that $\Re[T]$ and $\Im[T]$ are self-adjoint.

Exercise 6.6.4.6 Check that $T = \Re[T] + \mathrm{i}\,\Im[T]$.

To see uniqueness, write $T = R + \mathrm{i}I$ for $R, I : V \to V$ self-adjoint. We thus have that $\Re[T] - R = \mathrm{i}(I - \Im[T])$. Taking the adjoint of this yields $\Re[T] - R = -\mathrm{i}(I - \Im[T]) = -(\Re[T] - R)$, whence it follow that $\Re[T] = R$. Similarly, $\Im[T] = I$.

Exercise 6.6.4.7 Show that $\Re[T]$ and $\Im[T]$ commute if T is normal.

For the converse, suppose that $\Re[T]$ and $\Im[T]$ commute. Then, expanding the equation $\Re[T]\Im[T] = \Im[T]\Re[T]$ yields

$$\frac{T^2 - TT^* + T^*T - [T^*]^2}{4\mathrm{i}} = \frac{T^2 + TT^* - T^*T - [T^*]^2}{4\mathrm{i}},$$

whence it follows that

$$-TT^* + T^*T = TT^* - T^*T, \tag{6.6.4.8}$$

and hence, after rearranging, $T^*T = TT^*$. ■

In a similar way as self-adjoint is an analogue of being real, there is an analogue of being a complex number of absolute value 1.

Definition 6.6.4.9 — Unitary Let V and W be inner-product spaces and let $T : V \to W$ be a continuous linear-transformation. Then, T is ***unitary*** iff

$$\langle T(v_1) | T(v_2) \rangle = \langle v_1 | v_2 \rangle \tag{6.6.4.10}$$

for all $v_1, v_2 \in V$.

R If V and W are real inner-product spaces, it is more common for people to say ***orthogonal*** instead of "unitary".

R For what it's worth, you don't need to assume that it is continuous or linear—these will follow from the fact it preserves the inner-product.

Thus, a linear-transformation is unitary iff it "preserves" the inner-product. However, by the Polarization Identity (Theorem 6.3.2.12), this is equivalent to the superficially weaker condition that it only "preserve" the *norm*.

Proposition 6.6.4.11 Let V and W be inner-product spaces and let $T\colon V \to W$ be a continuous linear-transformation. Then, T is unitary iff

$$\|T(v)\| = \|v\| \tag{6.6.4.12}$$

for all $v \in V$.

Proof. ($\Rightarrow$) Suppose that T is unitary. Then,

$$\|T(v)\|^2 := \langle T(v)|T(v)\rangle = \langle v|v\rangle =: \|v\|^2. \tag{6.6.4.13}$$

($\Leftarrow$) Suppose that

$$\|T(v)\| = \|v\| \tag{6.6.4.14}$$

for all $v \in V$. It then follows that

$$\langle T(v)|T(w)\rangle = \langle v|w\rangle \tag{6.6.4.15}$$

for all $v, w \in V$ by the Polarization Identity (Theorem 6.3.2.12). ■

While this condition might be a natural one, it's not immediately clear how this is analogous to being a complex number of absolute value 1. The following result clarifies this.

Proposition 6.6.4.16 Let V and W be inner-product spaces and let $T\colon V \to W$ be a continuous linear-transformation. Then, T is unitary iff $T^*T = \mathrm{id}_V$ and $TT^* = \mathrm{id}_W$.

R In other words,

T is unitary iff $T^{-1} = T^*$.

R Note that $z \in \mathbb{C}$ has absolute value 1 iff $z^* z = |z| = 1$, hence the analogy.

Proof. We leave this as an exercise.

Exercise 6.6.4.17 Prove the result.

■

Combining these characterizations into a single result for convenience gives us the following.

Theorem 6.6.4.18 — Characterization of unitary linear-transformations. Let V and W be inner-product spaces and let $T : V \to W$ be a continuous linear-transformation with adjoint $T^* : W \to V$. Then, the following are equivalent.

(i). $\langle T(v_1) | T(v_2) \rangle = \langle v_1 | v_2 \rangle$ for all $v_1, v_2 \in V$.
(ii). $\|T(v)\| = \|v\|$ for all $v \in V$.
(iii). $T^* T = \mathrm{id}_V$ and $T T^* = \mathrm{id}_W$.
(iv). $T^{-1} = T^*$.

R Note that (i) was taken as our definition of unitary (Definition 6.6.4.9).

Proof. This follows from Definition 6.6.4.9 and Propositions 6.6.4.11 and 6.6.4.16. ■

There is a nice characterization of those matrices which define unitary operators.

Proposition 6.6.4.19 Let A be an $m \times m$ matrix with complex entries. Then, A is unitary iff its columns form an orthonormal basis for $\mathbb{C}^m$.

R In the real case, this reads "A is orthogonal iff its columns form an orthonormal basis for $\mathbb{R}^m$". Thus, the term "orthogonal" in this case is a poor one. Really, these should be called ortho*normal* matrices.

R The self-adjoint analogue of this result simply says that A is self-adjoint iff $A^* = A$—as this is more or less immediate from the definition (together with Proposition 6.6.3.35), we didn't bother stating it explicitly.

Proof. We leave this as an exercise.

Exercise 6.6.4.20 Prove the result.

■

And again, we have an analogue of nonnegative real numbers.

Definition 6.6.4.21 — Nonnegative Let V be an inner-product space and let $T: V \to V$ be a continuous linear-transformation.

(i). T is ***nonnegative*** iff $T = S^*S$ for some continuous linear-transformation S.
(ii). T is ***nonpositive*** iff $T = -S^*S$ for some continuous linear-transformation S.

R Note that there is no requirement that S have codomain W.

R Just as "positive definite" was more common than "nonnegative definite", so to the term "positive linear-transformation" is more common than "nonnegative linear-transformation" (though less appropriate).

R Of course, this is motivated by the fact that the non-negative real numbers are precisely those numbers which can be written in the form $|z|^2 = z^* z$ for some $z \in \mathbb{C}$.

R In case you're wondering "But why not SS^*?", the answer is that this is equivalent—see the following result.

There are a couple of equivalent ways to state this.

Proposition 6.6.4.22 Let V be a Hilbert space and let $T : V \to V$ be a continuous linear-transformation. Then, the following are equivalent.

(i). T is nonnegative.
(ii). There is a linear-transformation S such that $T = SS^*$.
(iii). There is a self-adjoint operator S such that $T = S^2$.
(iv). There is a nonnegative operator S such that $T = S^2$.

R Additionally, we will see in Proposition 6.6.4.50 that these statements are also equivalent to the statement that $\langle v | T(v) \rangle \geq 0$ for all $v \in V$.

R In particular, if T is nonnegative, then there is unique nonnegative operator $\sqrt{T}$, the ***square-root***, such that $T = \sqrt{T}^2$.[a]

[a] Just as in the real numbers, the condition $S^2 = T$ does not uniquely determine S—one must further require that S be nonnegative, in which case we have $S = \sqrt{T}$.

Proof. We leave this as an exercise.

Exercise 6.6.4.23 Prove the result.

■

This allows us to make the following definition.

Definition 6.6.4.24 — Absolute value Let V and W be Hilbert spaces and let $T: V \to W$ be a continuous linear-transformation. Then, the ***absolute value***, $|T|$, is defined by

$$|T| := \sqrt{T^*T}. \tag{6.6.4.25}$$

R Warning: We need not have $|T| = |T^*|$—see the following exercise. In fact, squaring the equation $|T| = |T^*|$, we see that $|T| = |T^*|$ iff T is normal.

Exercise 6.6.4.26 Let $R: \ell^2(\mathbb{N}) \to \ell^2(\mathbb{N})$ be the right-shift operator. Compute $|R|$.

Proposition 6.6.4.27 Let V be a Hilbert space, let $T: V \to V$ be a continuous linear-transformation, and let $v \in V$. Then,

$$\|T(v)\| = \||T|(v)\|. \tag{6.6.4.28}$$

R That is, the norm of $T(v)$ is equal to the norm of $|T|(v)$.

R In particular, $\mathrm{Ker}(T) = \mathrm{Ker}(|T|)$.

Proof.

$$\begin{aligned} \||T|(v)\|^2 &= \langle |T|(v)||T|(v)\rangle = \langle v||T|^2(v)\rangle \\ &= \langle v|[T^*T](v)\rangle = \langle T(v)|T(v)\rangle \\ &= \|T(v)\|^2. \end{aligned} \tag{6.6.4.29}$$

■

Just as we can write a general operator in the form $A + \mathrm{i}\,B$ for A and B self-adjoint, we can write a self-adjoint operator in the form $A - B$ for A and B nonnegative.

Proposition 6.6.4.30 Let V be a Hilbert space and let $T\colon V \to V$ be self-adjoint. Then, there are unique nonnegative operators $T_\pm\colon V \to V$ such that

(i). $T = T_+ - T_-$; and
(ii). $T_+T_- = 0 = T_-T_+$.

Furthermore, $|T| = T_+ + T_-$.

R T_+ and T_- are respectively the ***nonnegative*** and ***non-positive*** parts of T, though they are more commonly referred to as the "positive" and "negative" parts respectively.

R In particular, this, together with Proposition 6.6.4.2, implies that every operator can be written as a finite linear-combination of nonnegative operators.

R To help your intuition for this, consider the following. Let X be any set and let $f\colon X \to \mathbb{R}$. Then, $f = f_+ - f_-$ and $f_+f_- = 0 = f_-f_+$, $f_+, f_- \geq 0$, where

$$f_+(x) \coloneqq \begin{cases} f(x) & \text{if } f(x) \geq 0 \\ 0 & \text{otherwise} \end{cases} \tag{6.6.4.31}$$

and

$$f_-(x) \coloneqq \begin{cases} -f(x) & \text{if } f(x) \leq 0 \\ 0 & \text{otherwise.} \end{cases} \tag{6.6.4.32}$$

Proof. We leave this as an exercise.

Exercise 6.6.4.33 Prove the result.

R Hint: See [B C90, Proposition VIII.3.4].

■

In general, operators are 'too noncommutative' in order to accurately draw any analogies at all between them and the complex numbers. However, there is a class of operators for which, roughly speaking, can be thought of as an analogue of a complex number, in a similar way that self-adjoint is analogous to being real and unitary is analogous to having absolute value 1. This class is known as the class of *normal operators*.

Definition 6.6.4.34 — Normal Let V be an inner-product space and let $T : V \to V$ be continuous and linear. Then, T is ***normal*** iff $T^*T = TT^*$.

R That is, T is normal iff it commutes with its adjoint.

R Note how we require the domain and codomain to coincide here. If the codomain were instead T, T^*T would be an operator on V and TT^* would be an operator on W, and so it wouldn't make sense to say that $T^*T = TT^*$.

R Note that self-adjoint and unitary operators are all normal.

Exercise 6.6.4.35 Give an example of S and T nonnegative such that $S \circ T$ is not normal.

R In particular, the composite of two nonnegative (resp. self-adjoint, normal) operators need not be nonnegative (resp. self-adjoint, normal). On the other hand, the composition of two unitary operators is unitary—see the following exercise.

Exercise 6.6.4.36 Show that the composition of two unitary linear-transformations is unitary.

The function $\langle v|T(v)\rangle$

It turns out that the function $v \mapsto \langle v|T(v)\rangle$ can tell us quite a bit about T. The first thing we observe is that, if this function vanishes, then T vanishes.

Proposition 6.6.4.37 Let V be an inner-product space and let $T\colon V \to V$ be linear. Then, if

$$\langle v|T(v)\rangle = 0 \tag{6.6.4.38}$$

for all $v \in V$, then $T = 0$.

R For real inner-product spaces, you must additionally assume that T is self-adjoint in order for this to hold.

Proof. To show that $T = 0$, it suffices to show that $\langle v|T(w)\rangle = 0$ for all $v, w \in V$. However, this follows from a 'Polarization Identity':

$$\begin{aligned}\langle v|T(w)\rangle = \tfrac{1}{4}\big(&\langle v+w|T(v+w)\rangle - \langle v-w|T(v-w)\rangle \\ &-\mathrm{i}\langle v+\mathrm{i}w|T(v+\mathrm{i}w)\rangle + \mathrm{i}\langle v-\mathrm{i}w|T(v-\mathrm{i}w)\rangle\big).\end{aligned} \tag{6.6.4.39}$$

■

This has an important corollary that serves another characterization of normal operators.

Proposition 6.6.4.40 Let V be an inner-product space and let $T\colon V \to V$ be continuous an linear. Then, T is normal iff

$$\|T(v)\| = \|T^*(v)\| \tag{6.6.4.41}$$

for all $v \in V$.

Proof. ($\Rightarrow$) Suppose that T is normal. Let $v \in V$. Then,

$$\begin{aligned} \|T(v)\|^2 &= \langle T(v)|T(v)\rangle = \langle v|T * (T(v))\rangle \\ &= \langle v|T(T^*(v))\rangle = \langle T^*(v)|T^*(v)\rangle \\ &= \|T^*(v)\|^2, \end{aligned} \tag{6.6.4.42}$$

and hence $\|T(v)\| = \|T^*(v)\|$.

($\Leftarrow$) Suppose that $\|T(v)\| = \|T^*(v)\|$ for all $v \in V$. Then, $\langle T(v)|T(v)\rangle = \langle T^*(v)|T^*(v)\rangle$, and hence $\langle v|T^*(T(v))\rangle = \langle v|T(T^*(v))\rangle$, and hence

$$\langle v|[T^* \circ T - T \circ T^*](v)\rangle = 0 \tag{6.6.4.43}$$

for all $v \in V$. It then follows from the previous result that $T^*T - TT^* = 0$, that is, T is normal. ■

This in turn has another useful corollary about normal operators.

Corollary 6.6.4.44 Let V be an inner-product space and let $T: V \to V$ be continuous and linear. Then, if T is normal, then

$$\mathrm{Ker}(T^*) = \mathrm{Ker}(T). \tag{6.6.4.45}$$

Proof. From the previous result, $v \in \mathrm{Ker}(T)$ iff $T(v) = 0$ iff $\|T(v)\| = 0$ iff $\|T^*(v)\| = 0$ iff $T^*(v) = 0$ iff $0 \in \mathrm{Ker}(T^*)$. ■

Exercise 6.6.4.46 Does $\mathrm{Ker}(T) = \mathrm{Ker}(T^*)$ imply T is normal?

We just observed that $\langle v|T(v)\rangle = 0$ for all $v \in V$ implies $T = 0$ and proved a couple of corollaries. We now investigate how this function can be used to characterize self-adjoint operators.

Proposition 6.6.4.47 Let V be an inner-product space and let $T: V \to V$ be continuous and linear. Then, T is self-adjoint iff

$$\langle v|T(v)\rangle \in \mathbb{R} \tag{6.6.4.48}$$

for all $v \in V$.

Proof. We leave this as an exercise.

Exercise 6.6.4.49 Prove the result.

■

There is an exact analogue for nonnegative operators.

Proposition 6.6.4.50 Let V be an inner-product space and let $T: V \to V$ be continuous and linear. Then, T is nonnegative iff

$$\langle v|T(v)\rangle \geq 0 \tag{6.6.4.51}$$

for all $v \in V$.

Proof. ($\Rightarrow$) Suppose that T is nonnegative. Then, by definition, $T = S^*S$ for some continuous linear-transformation S. Then, for $v \in V$,

$$\begin{aligned}\langle v|T(v)\rangle &= \langle v|S^*(S(v))\rangle = \langle S(v)|S(v)\rangle \\ &= \|S(v)\|^2 \geq 0.\end{aligned} \tag{6.6.4.52}$$

($\Leftarrow$) We leave this as an exercise.

Exercise 6.6.4.53 Prove the result.

■

Exercise 6.6.4.54 Define

$$V := \left\{ f \in C^\infty([-1,1]) : f^{(k)}(1) = f^{(k)}(-1) \text{ for all } k \in \mathbb{N}. \right\}$$

and $T\colon V \to V$ by

$$T(f) := f''. \tag{6.6.4.55}$$

Show that $-T$ is nonnegative.

Though be warned: the analogous statement for unitary operators fails.

▪ **Example 6.6.4.56 — $|\langle v|T(v)\rangle| \neq \|v\|^2$ for T unitary** Consider the right-shift operator $R\colon \ell^2(\mathbb{N}) \to \ell^2(\mathbb{N})$. This is unitary by Proposition 6.6.4.11. On the other hand, consider the vector $v := \langle 1, 0, 0, \ldots\rangle \in \ell^2(\mathbb{N})$. As $R(v) = \langle 0, 1, 0, \ldots\rangle$, it follows that $\langle v|R(v)\rangle = 0$.

The function $v \mapsto \langle v|T(v)\rangle$ has one more significant role to play in the Min-Max Theorem (Theorem 6.7.2.16), though we must postpone this until we know that all eigenvalues of self-adjoint operators are real (Corollary 6.7.2.9).

6.6.5 Orthogonal-complements and projections

In and near Theorem 6.6.2.10, we discuss the direct-sum decomposition $V = W \oplus W^\perp$ and how the projections $\mathrm{proj}_W(v)$ and $\mathrm{proj}_{W^\perp}(v)$ with respect to this direct-sum decomposition coincides with the elements of W and $W^\perp$ respectively closest to v. We wanted to investigate additional properties of both $W^\perp$ and proj_W back then, but an important property of the projection is that it is *self-adjoint*, and so we waited until discussion of the adjoint to state them.

A return to orthogonal-complements

You'll recall that (Definition 5.2.2.17) we have already defined the notion of orthogonal complement in the context of dual-pairs. And sure enough, as an inner-product $\bar{V} \times V \to \mathbb{C}$ itself defines a dual-paring, we obtain a notion of orthogonal complement for inner-product

spaces. However, while the definition is the same, as with everything else, previously we were implicitly assuming that everything was discrete, and as now we are no longer making this assumption, we run the risk of some results no longer holding. Unfortunately, it turns out that this is the case, and so we redo the correct analogues of results we saw before. (Furthermore, orthogonal complements play a much more important role in the theory of inner-product spaces, and so it's worth reviewing anyways.)

First of all, given a dual-pair $W \times V \to \mathbb{K}$, we could speak of the orthogonal complement of subsets of W (which themselves were subsets of V) and vice-versa. For an inner-product space however, as $W = \bar{V}$, in this case we may regard subsets of $W = \bar{V}$ as subsets of V, and so we only need to consider the one case (orthogonal complements of subsets of V) in this context.

Proposition 6.6.5.1 — Properties of the orthogonal complement Let V be a Hilbert space and let $S \subseteq V$.

(i). $S^\perp$ is a closed subspace of V.
(ii). If $S \subseteq T$, then $T^\perp \subseteq S^\perp$.
(iii). $[S^\perp]^\perp = \mathrm{Cls}(\mathrm{Span}(S))$.[a]
(iv). $S \cap S^\perp = 0$ if S is nonempty.
(v). $0^\perp = V$.
(vi). $V^\perp = 0$.
(vii). For $U \subseteq V$ a subspace,

$$\dim(V) = \dim(U) + \dim(U^\perp). \tag{6.6.5.2}$$

R You'll note that some of these are true just as they were before (except for (i), (iii) and (iv)). The reason for the repetition is just so that this is an exact analogue of Proposition 5.2.2.21. (Though there is no analogue of (iv) in Proposition 5.2.2.21 because $S \cap S^\perp$ doesn't make sense in that context.)

R The most important thing to take note of here is (iii).[b] Do not forget that closure!

R Note that some of the properties in Proposition 5.2.2.21 required nonsingularity or nondegeneracy. We get that for free here because of the Riesz Representation Theorem (Theorem 6.6.3.1).

[a] When generalizing to locally-convex spaces, this is still essentially true, but the closure is taken to be the weak/weak-* closure (which happens to agree with the norm closure on convex subsets).

[b] The only other one that has changed is (i) which is harder to get wrong.

Proof. We leave this as an exercise.

Exercise 6.6.5.3 Prove the result.

■

The important result relating transposes and orthogonal complements (Proposition 5.2.2.32) also changes slightly to account for the closures.

Proposition 6.6.5.4 Let V and W be Hilbert spaces and let $T : V \to W$ be a continuous linear-transformation. Then,

$$\mathrm{Ker}(T^*) = \mathrm{Im}(T)^\perp \tag{6.6.5.5}$$

$$\mathrm{Ker}(T) = \mathrm{Im}(T^*)^\perp \tag{6.6.5.6}$$

R You'll notice that this is stated slightly differently than in Proposition 5.2.2.32. It's stated the way it is in Proposition 5.2.2.32 because I find this way the most intuitive—the result gives descriptions of $\mathrm{Ker}(T^\dagger)$ and $\mathrm{Im}(T^\dagger)$. Unfortunately, however, this way of stating the result is *not* correct in this context.

(6.6.5.5) is the same as it was before, though (6.6.5.6) is different. To see why, take the $^\perp$ of (6.6.5.6). Using Proposition 6.6.5.1(iii), this yields

$$\mathrm{Ker}(T)^\perp = \mathrm{Cls}(\mathrm{Im}(T^*)). \tag{6.6.5.7}$$

Contrast this with $\mathrm{Im}(T^\dagger) = \mathrm{Ker}(T)^\perp$ as in Proposition 5.2.2.32. Thus, if we wanted to write it in an

analogous way, we would have to include a closure. Instead, the $^{\perp}$s in (6.6.5.5) and (6.6.5.6) are placed so that everything that appears is closed, and hence no closures are needed.[a]

R Do take note of this. It is quite important.

[a] Kernels are always closed and $S^{\perp}$ is always closed (Proposition 6.6.5.1(i)).

Proof. We leave this as an exercise.

Exercise 6.6.5.8 Prove the result.

■

Exercise 6.6.5.9 Let V be a Hilbert space, let $W \subseteq V$ be a closed subspace, and let $T : V \to V$ be continuous and linear. Show that W is T-invariant iff $W^{\perp}$ is T^*-invariant.

A return to projections

And now for projections.

Proposition 6.6.5.10 — Properties of proj_W Let V be a Hilbert space and let $W \subseteq V$ be a closed subspace.

(i). $\text{proj}_W : V \to V$ is continuous and linear.
(ii). $\left\|\text{proj}_W\right\| = 1$ iff $W \neq 0$.
(iii). $\text{Im}(\text{proj}_W) = W$.
(iv). $\text{Ker}(\text{proj}_W) = W^{\perp}$.
(v). $\text{proj}_W + \text{proj}_{W^{\perp}} = \text{id}_V$.
(vi). $\text{proj}_W^2 = \text{proj}_W$.
(vii). $\text{proj}_W^* = \text{proj}_W$.

R The last two are important in that they actually "abstractly characterize" which continuous linear-transformations are projection operators—see Theorem 6.6.5.13.

R In particular, (iii) says that you can write the projection onto $W^\perp$ in terms of the projection onto W (and vice versa): $\text{proj}_{W^\perp}(v) = v - \text{proj}_W(v)$.

R The last two also imply that proj_W is nonnegative by Proposition 6.6.4.22.

Proof. We leave this as an exercise.

Exercise 6.6.5.11 Prove the result.

■

As mentioned in the remark of the previous result, the two properties $P^2 = P$ and $P^* = P$ are important, and so we give the class of operators which satisfy these properties a name.

Definition 6.6.5.12 — Orthogonal projection Let V be a Hilbert space and let $P\colon V \to V$ be continuous and linear. Then, P is an ***orthogonal projection*** iff $P^2 = P$ and $P^* = P$.

R Recall that (Proposition 4.4.1.49) given at direct-sum decomposition $V = U \oplus W$, we have a notion of projection proj_U onto U (and similarly for W). Of note is that this projection *depends on the decomposition itself, not just* U. It turns out that the "orthogonal" in "orthogonal projection" refers to the fact that these projections are those with respect to decompositions of the form $V = W \oplus W^\perp$ for $W \subseteq V$ a closed subspace. Indeed, all projections satisfy $P^2 = P$—the condition $P^* = P$, which only makes sense if we have an inner-product, guarantees that the *orthogonal* projections are projections with respect to decompositions of this form—see the following result.

Theorem 6.6.5.13 — Closed subspaces ↔ projections. Let V be a Hilbert space and let $P: V \to V$ be an orthogonal projection. Then, there is a unique closed subspace $W \subseteq V$ such that $P = \mathrm{proj}_W$.

Furthermore, explicitly, $W = \mathrm{Im}(P)$.

R This establishes a one-to-one correspondence between closed subspaces and orthogonal projections: given a closed subspace $W \subseteq V$, we obtain the orthogonal projection proj_W; and given an orthogonal projection $P: V \to V$, we obtain the closed subspace[a] $\mathrm{Im}(P)$.

[a] That it is a subspace is immediate. That it is closed is not.

Proof. Step 1: Find W.
Define $W := \mathrm{Im}(P)$.

Step 2: Show that $P|_W = \mathrm{id}_W$.
Let $w \in W$. Write $w = P(v)$ for some $v \in V$. Then, $P(w) = P^2(v) = P(v) = w$.

Step 3: Show that $\mathrm{Ker}(P) = W^\perp$.
From Proposition 6.6.5.4, we have that

$$\mathrm{Ker}(P) = \mathrm{Ker}(P^*) = \mathrm{Im}(P)^\perp = W^\perp. \tag{6.6.5.14}$$

Step 4: Finish the proof.
Let $v \in V$. By Corollary 6.6.2.1, we have that

$$v = \mathrm{proj}_W(v) + \mathrm{proj}_{W^\perp}(v). \tag{6.6.5.15}$$

Applying P to this equation, we obtain

$$P(v) = P(\mathrm{proj}_W(v)) + P(\mathrm{proj}_{W^\perp}(v)). \tag{6.6.5.16}$$

However, the second term vanishes as $\mathrm{Ker}(P) = W^{\perp}$, and the first term simplifies to just $\mathrm{proj}_W(v)$ as $P|_W = \mathrm{id}_W$. This yields,

$$P(v) = \mathrm{proj}_W(v), \tag{6.6.5.17}$$

as desired.

To see uniqueness, note that if we had $\mathrm{proj}_U = P = \mathrm{proj}_W$ for some subspace $U \subseteq V$, then we would have $U = \mathrm{Im}(\mathrm{proj}_U) = \mathrm{Im}(\mathrm{proj}_W) = W$. ■

All of this so far has practically been the definition of "exhilarating", but all that exhilaration won't amount to much if we can't compute the damn thing. The following result states in practice how you will compute projections onto closed subspaces.

Proposition 6.6.5.18 Let V be a Hilbert space, let $W \subseteq V$ be a closed subspace, and let $\mathcal{B}$ be an orthonormal basis of W. Then,

$$\mathrm{proj}_W = \sum_{b \in \mathcal{B}} |b\rangle\langle b| \,. \tag{6.6.5.19}$$

R This is equivalent to the statement that

$$\mathrm{proj}_W(v) = \sum_{b \in \mathcal{B}} \langle b|v\rangle b \tag{6.6.5.20}$$

for all $v \in V$.

R We've seen this notation used before in a remark of Proposition 6.5.2.1 where we saw that

$$\mathrm{id}_V = \sum_{b \in \mathcal{B}} |b\rangle\langle b|, \tag{6.6.5.21}$$

where $\mathcal{B}$ is an orthonormal basis of V. We now see that Proposition 6.5.2.1 is a special case of this result for $W = V$.

Proof. We leave this as an exercise.

Exercise 6.6.5.22 Prove the result.

■

Given a linearly-independent set $S \subseteq V$, one might be interested to know if one can 'turn S into' an orthonormal set, in the sense that the span S and the orthonormal set agree. The answer is "Yes." and it is the previous result that allows us to do this.

Proposition 6.6.5.23 — Gram-Schmidt Algorithm Let V be a Hilbert space, let $S \subseteq V$ be linearly-independent, equip S with some well-founded relation $\preceq$, for $v \in S$ let $\check{v}$ be the normalization[a] of

$$v - \mathrm{proj}_{W_v}(v), \tag{6.6.5.24}$$

where

$$W_v := \mathrm{Cls}(\mathrm{Span}(\{w \in S : w \preceq v, w \neq v\})), \tag{6.6.5.25}$$

and define $\check{S} := \{\check{v} : v \in S\}$. Then, $\check{S}$ is orthonormal and for every $v \in S$

$$\begin{aligned} &\mathrm{Cls}(\mathrm{Span}(\{w \in S : w \preceq v, w \neq v\})) \\ &\quad = \mathrm{Cls}(\mathrm{Span}(\{\check{w} \in \check{S} : w \preceq v, w \neq v\})). \end{aligned} \tag{6.6.5.26}$$

R In practice, S will usually be a finite set $S = \{v_1, \ldots, v_m\}$ in which case the well-founded relation is the one coming from the usual order on $\{1, \ldots, m\}$.

[a] Note that by linear-independence of S, the displayed vector is never 0, and so we can indeed normalize it.

Proof. We leave this as an exercise.

Exercise 6.6.5.27 Prove the result.

■

This in turn allows us to give the *QR factorization* of a matrix.

Proposition 6.6.5.28 — QR Factorization Let A be an $m \times n$ matrix with complex entries. Then, if the columns of A are linearly-independent, then there is a unitary matrix Q and an upper-triangular matrix R with positive entries on the diagonal such that

$$A = QR. \tag{6.6.5.29}$$

R The basic idea of the proof is to perform Gram-Schmidt on the columns of A. The columns of Q will then be the the resulting orthonormal set that the algorithm 'spits out'.

Proof. We leave this as an exercise.

Exercise 6.6.5.30 Prove the result.

■

Exercise 6.6.5.31 Let A be an $m \times n$ matrix with complex entries and linearly-independent columns. The previous result says that A has a QR factorization. Is this QR factorization unique?

Another application of projections is to what are called *least squares solution*.

Definition 6.6.5.32 — Least-squares-solution Let V and W be inner-product spaces, let $T: V \to W$ be continuous and linear, let $y_0 \in W$, and $x_0 \in V$. Then, x_0 is a ***least-squares-solution*** to the equation "$T(x) = y_0$" iff

$$\|T(x_0) - y_0\| \leq \|T(x) - y_0\| \tag{6.6.5.33}$$

for all $x \in V$.

R Note of course that if x_0 is an 'actual' solution, that is $T(x_0) = y_0$, then it is a least-squares-solution. The interest in least-squares-solutions is really in the case where there is no "actual". Thus, while we may not be able to have exact equality $T(x_0) = y_0$, we say that x_0 is a *least-squares-solution* iff $T(x_0)$ is as close to y_0 as possible.

R Squaring, we see that this inequality is equivalent to

$$\|T(x_0) - y_0\|^2 \leq \|T(x) - y_0\|^2. \tag{6.6.5.34}$$

We can see from this where the name comes from: if the inner-product is given by the dot product, then both sides of this inequality are a sum of squares, and as x_0 minimizes this quantity, it is referred to as a *least-squares*-solution.

This definition is nice in that it tells you why you should care about least-squares-solutions. But it's also not so great in that it's not particularly amenable to actually finding least-squares-solutions. Instead, the following result is used to compute least-squares-solutions.

Theorem 6.6.5.35 — Fundamental Theorem of Least-Squares. Let V and W be finite-dimensional inner-product spaces, let $T: V \to W$ be continuous and linear, let $y_0 \in W$, and let $x_0 \in V$. Then, the following are equivalent.

(i). x_0 is a least-squares-solution of "$T(x) = y_0$".

(ii). $T(x_0) = \text{proj}_{\text{Im}(T)}(y_0)$.[a]
(iii). $T^*(T(x_0)) = T^*(y_0)$.

R In practice, (iii) tends to be the most useful for computing least-squares-solutions. (ii) is then sort of an intermediate between the 'conceptual' definition (i) and the 'computational' (iii).

[a] That is, x_0 is an 'actual' solution to "$T(x) = \text{proj}_{\text{Im}(T)}(v_0)$".

Proof. We leave this as an exercise.

Exercise 6.6.5.36 Prove the result.

■

6.7 The Spectral Theorem

6.7.1 The theorem itself

We spent perhaps the first half of these notes investigating diagonalizability and its generalization, Jordan Canonical Form. Recall that we said that T was diagonalizable iff there was a basis $\mathcal{B}$ such that $[T]_{\mathcal{B}}$ was diagonal. In the context of inner-product spaces, however, in a perfect world, there wouldn't just be any old basis for which this was so, but in fact there would be an *orthonormal* basis for which this was true. Linear-transformations for which such a diagonalizing orthonormal basis exists are called *orthogonally diagonalizable*.

Definition 6.7.1.1 — Orthogonally diagonalizable Let V be a finite-dimensional inner-product space and let $T\colon V \to V$ be linear. Then, T is ***orthogonally diagonalizable*** iff there is an orthonormal basis $\mathcal{B}$ of V such that $[T]_{\mathcal{B}\leftarrow\mathcal{B}}$ is a diagonal matrix.

Before we were able to give a couple of characterizations of those linear-transformations which were diagonalizable (Theorem 4.3.5). There is an even nicer characterization of those linear-transformations

which are orthogonally diagonalizable. In fact, it is arguably the most important theorem in all of these notes, comparable in significance to the Jordan Canonical Form Theorem: this is the *Spectral Theorem*.

Theorem 6.7.1.2 — Spectral Theorem. Let V be a finite-dimensional inner-product space and let $T: V \to V$ be linear. Then, the following are equivalent.

(i). T is orthogonally diagonalizable.
(ii). There is an orthonormal basis of V consisting of eigenvectors of T.
(iii). T is normal.

R For real inner-product spaces, the same result is true when you replace "normal" with "self-adjoint".

R The Spectral Theorem does generalize to infinite-dimensions, though we refrain from stating it for two reasons: (i) Our motivation for the Spectral Theorem was orthogonal diagonalizability, which, as stated, is a fundamentally finite-dimensional concept (because matrices); and (ii) it requires what for us would be an insane amount of theory to prove. Difficulty itself is never a particularly good reason not to do something, but coupled with (i), I think this makes sense. In any case, you should probably see the finite-dimensional version first to give intuition for the general case.

Proof. $((i) \Leftrightarrow (ii))$ T is orthogonally diagonalizable iff there is an orthonormal basis $\mathcal{B}$ such that $[T]_{\mathcal{B}}$ is diagonal. However, it follows from (3.2.2.3)[a] that $[T]_{\mathcal{B}}$ is diagonal iff $\mathcal{B}$ is a basis of eigenvectors of T.[b]

$((i) \Rightarrow (iii))$ Suppose that T is orthogonally-diagonalizable. Then, there is an orthonormal basis $\mathcal{B}$ such that $[T]_{\mathcal{B}}$ is diagonal. As $\mathcal{B}$ is orthonormal, $[T^*]_{\mathcal{B}} = [T]_{\mathcal{B}}{}^*$. Furthermore, this is likewise a diagonal matrix, and as diagonal matrices commute

with each other, we have that

$$\begin{aligned}[TT^*]_{\mathcal{B}} &= [T]_{\mathcal{B}}[T^*]_{\mathcal{B}} = [T]_{\mathcal{B}}[T]_{\mathcal{B}}{}^* = [T]_{\mathcal{B}}{}^*[T]_{\mathcal{B}} \\ &= [T^*]_{\mathcal{B}}[T]_{\mathcal{B}} = [T^*T]_{\mathcal{B}},\end{aligned} \tag{6.7.1.3}$$

and hence $TT^* = T^*T$.[c]

$((iii) \Rightarrow (i))$ We leave this as an exercise.

Exercise 6.7.1.4 Prove this direction.

■

[a] This equation gives an explicit formula for the coordinates of a linear-transformation with respect to bases.

[b] We go fast as this is essentially the same proof as in Fundamental Theorem of Diagonalizability (Theorem 4.3.5).

[c] This uses the fact that the "take coordinates" map is an isomorphism—see Proposition 3.2.2.16.

In some ways, the condition "has an orthonormal basis consisting of eigenvectors" is nicer than "is orthogonally diagonalizable" because it makes sense in arbitrary dimensions. For example, the following result is really quite useful, and it works in infinite-dimensions as well as finite-dimensions.

Proposition 6.7.1.5 Let V be an inner-product space, let $T\colon V \to V$ be continuous and linear, let $\mathcal{B}$ be an orthonormal basis for V, and for $b \in \mathcal{B}$ let $\lambda_b \in \mathbb{C}$ be the eigenvalue of b. Then,

$$T = \sum_{b\in\mathcal{B}} \lambda_b \, |b\rangle\langle b| \, . \tag{6.7.1.6}$$

R In fact, it is possible to define $f(T)$ for any Borel function $f\colon \mathbb{C} \to \mathbb{C}$,[a] and so in particular for continuous f, in which case we have

$$f(T) = \sum_{b\in\mathcal{B}} f(\lambda_b) \, |b\rangle\langle b| \, . \tag{6.7.1.7}$$

In particular,

$$|T| = \sum_{b\in\mathcal{B}} |\lambda_b|\, |b\rangle\langle b| \,. \tag{6.7.1.8}$$

[a] This requires T to be normal, but of course, that follows from the hypotheses of this result.

Proof. Let $v \in V$. Write

$$v = \sum_{b\in\mathcal{B}} v^b \cdot b \tag{6.7.1.9}$$

for unique $v^b \in \mathbb{C}$. As T is continuous and linear, we have

$$T(v) = \sum_{b\in\mathcal{B}} v^b \cdot T(b) = \sum_{b\in\mathcal{B}} v^b \lambda_b \cdot b. \tag{6.7.1.10}$$

. On the other hand,

$$\begin{aligned}\left[\sum_{b\in\mathcal{B}} \lambda_b\, |b\rangle\langle b|\right](v) &= \sum_{b,c\in\mathcal{B}} \lambda_b v^c\, |b\rangle\, \langle b|c\rangle \\ &= \sum_{b\in\mathcal{B}} \lambda_b v^b \cdot b,\end{aligned} \tag{6.7.1.11}$$

and so we do indeed have equality, as desired. ∎

Just as for ordinary diagonalization, in the common case where the linear-transformation is defined in terms of a matrix, we can give a more or less explicit relationship between the original matrix and its diagonalization. In fact, it's the same relationship as before, [22] For this reason, we informally recall the result here and refer you to Proposition 4.3.1.1 for the full story.

[22] After all, it's still diagonalization—the only thing that has changed is that now the diagonalizing basis is orthonormal.

$$[A]_{\mathcal{B}\leftarrow\mathcal{B}} = [\mathrm{id}]_{\mathcal{B}\leftarrow\mathcal{S}}[A]_{\mathcal{S}\leftarrow\mathcal{S}}[\mathrm{id}]_{\mathcal{S}\leftarrow\mathcal{B}} \quad (6.7.1.12)$$

Or more informally,

$$D = P^*AP. \quad (6.7.1.13)$$

Note the one significant change in this case is that now P *is unitary*, which itself follows from the fact that $\mathcal{B}$ is an orthonormal basis—see Proposition 6.6.4.19.

6.7.2 Eigenvalues in inner-product spaces

As for 'ordinary' diagonalizability, being orthogonally diagonalizable is equivalent to the existence of an *orthonormal* basis consisting of eigenvectors. Thus, if you are concerned with orthogonal diagonalizability (and presumably you are if you're reading this subsection), it is of interest to understand eigenvalues and eigenvectors in the context of inner-product spaces.

You'll recall that (Proposition 4.2.48), if λ is an eigenvalue of T and p is a polynomial, then $p(\lambda)$ is an eigenvalue of $p(T)$. The same thing holds with the complex conjugate and the adjoint.

Proposition 6.7.2.1 — $\mathrm{Eig}(T^*) = \mathrm{Eig}(T)^*$ Let V be an inner-product space and let $T\colon V \to V$ be normal. Then,

$$\mathrm{Eig}^m_{\lambda,T} = \mathrm{Eig}^m_{\lambda^*,T^*} \quad (6.7.2.2)$$

for all $m \in \mathbb{N} \cup \{\infty\}$.

R In other words, λ and λ^* have the same (rank m) generalized-eigenvectors.[a]

R In particular,

$$\mathrm{Eig}(T^*) = \mathrm{Eig}(T)^*. \quad (6.7.2.3)$$

R Warning: The hypothesis of being normal is necessary—see the following exercise.

R The failure for this to hold in case T is not normal can be seen as a defect in the set of eigenvalues. It turns out that there is a notion called the *spectrum* of an operator that is the same as the set of eigenvalues in finite-dimensions, but is better-behaved (for example, it is true that $\mathrm{Spec}(T^*) = \mathrm{Spec}(T)$ irrespective of whether T is normal). Similarly, in finite-dimensions, one can characterize the self-adjoint operators as the operators all of whose eigenvalues are real; however, for the result to hold true in general, one must instead use the spectrum. Perhaps the most significant advantage, however, is that it does not need an 'underlying' vector space to make sense, and so one can discuss the spectrum of any element in any $\mathbb{K}$-algebra.

[a] In particular, they have the same eigenvectors and the same generalized-eigenvectors.

Proof. Suppose that T is normal. Let $\lambda \in \mathbb{C}$ and $m \in \mathbb{N}$. Then, by Corollary 6.6.4.44,

$$\begin{aligned} \mathrm{Eig}^m_{\lambda,T} &= \mathrm{Ker}([T-\lambda]^m) = \mathrm{Ker}([T^*-\lambda^*]^m) \\ &= \mathrm{Eig}^m_{\lambda^*,T^*}. \end{aligned} \tag{6.7.2.4}$$

■

Exercise 6.7.2.5 Find an example of an operator T with eigenvalue λ and such that λ^* is not an eigenvalue of T^*.

R Hint: Shift operators.

Corollary 6.7.2.6 Let V be an inner-product space, let $T: V \to V$ be normal, let $p \in \mathbb{C}[z, z^*]$, and let $\lambda \in \mathbb{C}$ be

an eigenvalue of T with eigenvector $v \in V$. Then,

$$[p(T, T^*)](v) = p(\lambda)v. \tag{6.7.2.7}$$

R Thus, when T is normal, the exact analogue of Proposition 4.2.48 holds except now we are additionally allowed to use polynomials with z^* terms appearing, allowing us to take adjoints (which correspond to complex conjugation for the eigenvalues).

R You can easily see that T must be normal for this to work in the following way. Consider the simple polynomial $p(z, z^*) := zz^*$. As an element of $\mathbb{C}[z, z^*]$, we have $p(z, z^*) := zz^* = z^*z$. So, when we go to plug in T, there is a potential problem: does $p(T, T^*) = TT^*$ or does $p(T, T^*) = T^*T$? The answer is:

> *Don't plug in operators that are not normal into polynomials in z and z^*.*

That is, we just simply take $p(T, T^*)$ to be undefined unless T is normal, in which case it doesn't matter which order of z and z^* we use.

R To clarify, for example, $3z(z^*)^2 - 2z^2z^* + 5z^2 - 3z^* + 2 \in \mathbb{C}[z, z^*]$. Here, "$z^*$" is the name of a single 'variable' independent of z. The notation is suggestive (we plug in T^* for z^* just as we plug in T for z), but everything works the same if I had written x instead of z^*.

Proof. We leave this as an exercise.

Exercise 6.7.2.8 Prove the result.

■

Corollary 6.7.2.9 Let V be an inner-product space, let $T\colon V \to V$ be normal, and let $p \in \mathbb{C}[z, z^*]$. Then, if $p(T, T^*) = 0$, then $p(\lambda, \lambda^*) = 0$ for all $\lambda \in \mathrm{Eig}(T)$.

R In particular:

(i). Eigenvalues of nonnegative operators are nonnegative.
(ii). Eigenvalues of nonpositive operators are nonpositive.
(iii). Eigenvalues of self-adjoint operators are real.
(iv). Eigenvalues of anti-self-adjoint operators are imaginary.
(v). Eigenvalues of unitary operators have absolute value 1.

Proof. Suppose that $p(T, T^*) = 0$. Let $\lambda \in \mathrm{Eig}(T)$ with eigenvector v. By the previous result, we have that

$$0 = [p(T, T^*)](v) = p(\lambda, \lambda^*)v. \tag{6.7.2.10}$$

As v is nonzero, it follows that $p(\lambda, \lambda^*) = 0$. ∎

We saw before that (Proposition 4.4.3.67) the generalized-eigenspaces were linearly-independent. In the context of inner-product spaces, if the operator is additionally normal, we can conclude that the generalized-eigenspaces are in fact *orthogonal*.

Proposition 6.7.2.11 — Generalized-eigenspaces with distinct eigenvalues of a normal operator are orthogonal Let V be an inner-product space and let $T\colon V \to V$ be continuous and linear. Then,

$$\left\{\mathrm{Eig}_\lambda^\infty : \lambda \in \mathrm{Eig}(T)\right\} \tag{6.7.2.12}$$

is orthogonal.

R Explicitly, this means that any collection of generalized-eigenvectors with distinct eigenvectors is orthogonal.

Proof. We leave this as an exercise.

Exercise 6.7.2.13 Prove the result.

■

Exercise 6.7.2.14 — Sturm-Liouville Operators Let $p, q \in C^\infty([-1,1])$ be real-valued with $p(-1) = 0 = p(1)$, and define $T\colon C^\infty([-1,1]) \to C^\infty([-1,1])$ by

$$[T(f)](x) := -\frac{\mathrm{d}}{\mathrm{d}x}\left[p(x)\frac{\mathrm{d}}{\mathrm{d}x}f(x)\right] - q(x)f(x). \quad (6.7.2.15)$$

Show that eigenvectors of T with distinct eigenvalues are orthogonal.

R *Sturm-Liouville Theory* is the study of differential operators of this (or really a slightly more general form) form.

Lastly, we return to a study of the function $v \mapsto \langle v|T(v)\rangle$ and its relationship to the eigenvalues of T.

Theorem 6.7.2.16 — Min-Max Theorem. Let V be a d-dimensional inner-product space, let $T\colon V \to V$ be self-adjoint, and let $\lambda_1 \leq \cdots \leq \lambda_d$ be the eigenvalues of T listed according to their multiplicity. Then,

$$\lambda_k = \min\{\max\{\langle v|T(v)\rangle : v \in V, \|v\| = 1\} : W \subseteq V \text{ a subspace with } \dim(W) = k.\}$$

and

$$\lambda_k = \max\{\min\{\langle v|T(v)\rangle : v \in V, \|v\| = 1\} : \\ W \subseteq V \text{ a subspace} \\ \text{with } \dim(W) = d - (k-1).\}.$$

R In particular,

$$\lambda_1 \leq \langle v|T(v)\rangle \leq \lambda_d \tag{6.7.2.17}$$

for all $v \in V$ with $\|v\| = 1$. In fact,

$$\lambda_1 = \min\{\langle v|T(v)\rangle : v \in V, \|v\| = 1\} \tag{6.7.2.18}$$
$$\lambda_d = \max\{\langle v|T(v)\rangle : v \in V, \|v\| = 1\}. \tag{6.7.2.19}$$

R (6.7.2.18) and (6.7.2.19) are sometimes referred to as ***Rayleigh's Principle***.

Proof. We leave this as an exercise.

Exercise 6.7.2.20 Prove the result.

■

6.8 The polar and singular value decompositions

6.8.1 The polar decomposition

Every complex number $z \in \mathbb{C}$ can be written in the form $re^{i\theta}$ for $r \in \mathbb{R}_0^+$ and $\theta \in (-\pi, \pi]$. The *polar decomposition* of an operator is an analogue of this for linear operators. As you might expect, r is going to be replaced by a nonnegative operator. You also might expect that $e^{i\theta}$ would be replaced by a unitary operator, however, this is not quite true: instead, *partial-isometries* take the place of $e^{i\theta}$.

Definition 6.8.1.1 — Partial-isometry Let V and W be inner-product spaces and let $T\colon V \to W$ be continuous and linear. Then, T is a ***partial-isometry*** iff $T|_{\mathrm{Ker}(T)^\perp}\colon \mathrm{Ker}(T)^\perp \to \mathrm{Im}(T)$ is a unitary isomorphism.

R $\mathrm{Ker}(T)^\perp$ is the ***initial space*** of T, and $\mathrm{Im}(T)$ is the ***final space*** of T.

R According to Proposition 6.6.4.11, an operator is unitary iff it preserves the norm, that is, an *isometry*.[a]

Thus, the condition that T be a partial-isometry says that, except for possibly sending vectors to 0, T preserves the norm.[b]

[a] In general, a function between two metric spaces is said to be an *isometry* iff it 'preserves' the metric. (Different usage of the word metric here than the one we've been using.)

[b] Note that I don't literally mean to say either $T(v) = 0$ or $\|T(v)\|$—one must also consider elements that are a nontrivial sum of an element in $\mathrm{Ker}(T)$ and $\mathrm{Ker}(T)^\perp$.

Theorem 6.8.1.2 — Polar Decomposition. Let V be a Hilbert space and let $T\colon V \to V$ be continuous linear.

(i). There is a unique partial-isometry $U\colon V \to V$ with initial space $\mathrm{Ker}(T)^\perp = \mathrm{Ker}(|T|)^\perp$ such that

$$T = U|T|. \tag{6.8.1.3}$$

Furthermore, the final space of U is $\mathrm{Cls}(\mathrm{Im}(T))$.

(ii). There is a unique partial-isometry $U\colon V \to V$ with final space $\mathrm{Cls}(\mathrm{Im}(T))$. such that

$$T = |T^*|U. \tag{6.8.1.4}$$

Furthermore, the initial space is $\mathrm{Ker}(T)^\perp = \mathrm{Ker}(|T|)^\perp$.

Furthermore, if V is finite-dimensional, then these partial-isometries are unitary.

R The weakening of the condition that U be unitary to only a partial-isometry is necessary—see the following exercise.

Proof. We leave this as an exercise.

Exercise 6.8.1.5 Prove the result.

■

Exercise 6.8.1.6 Compute the polar decomposition $L = U|L|$ of the left-shift operator $L\colon \ell^2(\mathbb{N}) \to \ell^2(\mathbb{N})$ and check that U is *not* unitary.

6.8.2 The singular value decomposition

The polar decomposition is certainly important in it's own right, but it also allows us to prove the existence of another decomposition: the *singular value decomposition*.

Given a linear operator T, the objective of diagonalization is to find a basis $\mathcal{B}$ in which the corresponding matrix $[T]_{\mathcal{B}}$ is diagonal. As we know by now very well, unfortunately, not every linear-transformation is diagonalizable, and our 'fix' to this was Jordan canonical form. But what about linear-transformations that fail to be orthogonally diagonalizable? Is there some sort of analogous fix for inner-product spaces?

You may recall from the very beginning of the section on Jordan canonical form (Section 4.4) that, before investigating Jordan canonical form itself, we first investigated the possibility of using *two* different bases, $\mathcal{B}$ for the domain and $\mathcal{C}$ for the codomain, in the hopes that we could always find such bases such that $[T]_{\mathcal{C}\leftarrow\mathcal{B}}$ was diagonal. We saw there that the answer is "Yes.", but for stupid reasons that were ultimately just not useful. Now, however, if we require that these be

orthonormal bases, the answer is no longer a stupid "Yes." and in fact gives us the *singular value decomposition*.[23]

Before we state the result, we're going to have to actually define *singular values*.

Proposition 6.8.2.1 Let V and W be inner-product spaces, and let $T: V \to W$ be a continuous linear-transformation with adjoint $T^*: W \to V$, let $\lambda \in \mathbb{C}$ be nonzero, and let $v \in V$.

(i). If $v \in \text{Eig}_{\lambda,T^*T}$, then $T(v) \in \text{Eig}_{\lambda,TT^*}$.
(ii). If $v \in \text{Eig}_{\lambda,TT^*}$, then $T^*(v) \in \text{Eig}_{\lambda,T^*T}$.

R In particular, for λ nonzero, $\lambda \in \text{Eig}(T^*T)$ iff $\lambda \in \text{Eig}(TT^*)$.

R Warning: Note that λ must be *nonzero*. It is possible that 0 is an eigenvalue for T^*T but not TT^* or vice-versa—see Example 6.8.2.15.

R Thus, this result in particular says that, ignoring 0, T^*T and TT^* have the same eigenvalues.

R As $|T| := \sqrt{T^*T}$ and $|T^*| := \sqrt{TT^*}$, it follows that $\lambda \in \text{Eig}(|T|)$ and $\lambda \in \text{Eig}(|T^*|)$ (for $\lambda \neq 0$).

R Warning: Despite the fact that they have the same nonzero eigenvalues, $|T|$ *and* $|T^*|$ *will not agree in general*. In fact, $|T| = |T^*|$ iff T is normal.

Proof. We leave this as an exercise.

Exercise 6.8.2.2 Prove the result.

■

[23] The reason the same trick that we used before doesn't work now is because, even if $\mathcal{B}$ is orthonormal, there is no guarantee that $C := T(\mathcal{B})$ be orthonormal.

Definition 6.8.2.3 — Singular-value Let V and W be Hilbert spaces, let $T\colon V \to W$ be a continuous linear-transformation, and let $\lambda \in \mathbb{C}$. Then, λ is a ***singular-value*** of T iff $\lambda \in \text{Eig}(|T|)$.

R Note that one advantage this has over the definition of an eigenvalue is that there is no requirement that the domain and codomain coincide. ($|T|$ is a map from V to V no matter what the codomain of T.)

Proposition 6.8.2.4 Let V and W be Hilbert space, let $T\colon V \to W$ be a continuous linear-transformation, and let $\lambda \in \mathbb{C}$. Then, λ is a singular-value of T iff $\lambda = \sqrt{\mu}$ for some

$$\mu \in \text{Eig}(T^*T) =: \text{Eig}(|T|^2) \tag{6.8.2.5}$$

Furthermore, for $\mu \in \text{Eig}(|T|^2)$,

$$\dim(\text{Eig}^{\infty}_{\sqrt{\mu},|T|}) = \dim(\text{Eig}^{\infty}_{\mu,|T|^2}). \tag{6.8.2.6}$$

R As taking the square-root of a number is much easier than taking the square-root of an operator, this is how the singular-values are computed in practice: compute the eigenvalues of $|T|^2 = T^*T$ and take square-roots of those eigenvalues.

R The equation involving the dimensions is essentially the statement that the multiplicity of μ and $\sqrt{\mu}$ are equal as eigenvalues of $|T|$ and $|T|^2$ respectively.

Proof. We leave this as an exercise.

Exercise 6.8.2.7 Prove the result.

■

Theorem 6.8.2.8 — Singular value Decomposition. Let V and W be finite-dimensional inner-product spaces, and let $T\colon V \to W$ be linear. Then, there are orthonormal bases $\mathcal{B}$ and C consisting of eigenvectors of T^*T and TT^* respectively such that

$$[T]_{C\leftarrow\mathcal{B}} \tag{6.8.2.9}$$

is a diagonal matrix with the singular values of T on the diagonal.

R Thus, this says that if we relax the requirement that the basis for the domain and codomain coincide, then every linear-transformation is 'orthogonally diagonalizable'.

R Another strength this has over 'ordinary' (orthogonal) diagonalization is that there is no requirement the domain and codomain coincide.

R Warning: Not just any orthonormal bases of T^*T and TT^* will work. For example, you could always scale an eigenvector by a complex number with absolute value 1 to obtain another orthonormal basis consisting of eigenvectors, but the corresponding element on the diagonal will have changed by that same factor.

R The convention is to order things so that the singular values are in *nonincreasing* order.

R Note that the definition of a diagonal matrix makes sense even if the matrix is not square—this just means that $A^i{}_j = 0$ if $i \neq j$, and this definition doesn't care about the dimensions of A.

Proof. We leave this as an exercise.

Exercise 6.8.2.10 Prove the result.

■

Again, just as with 'ordinary' diagonalization, if T is a matrix linear-transformation, then we can give a more or less explicit relationship between the original matrix and the diagonal matrix of singular values.

Proposition 6.8.2.11 Let A be an $m \times n$ matrix with complex entries, and let $\mathcal{B}$ and C be corresponding orthonormal bases of eigenvectors for T^*T and TT^* respectively, listed in order of nonincreasing eigenvalue. Then,

$$[A]_{C \leftarrow \mathcal{B}} = [\mathrm{id}_{m\times m}]_{C \leftarrow \mathcal{S}_m} [A]_{\mathcal{S}_m \leftarrow \mathcal{S}_n} [\mathrm{id}_{n\times n}]_{\mathcal{S}_n \leftarrow \mathcal{B}} \quad (6.8.2.12)$$

is diagonal, where $\mathcal{S}_n$ and $\mathcal{S}_m$ are the standard bases for $\mathbb{C}^m$ and $\mathbb{C}^n$ respectively.

Furthermore, you can scale the elements of $\mathcal{B}$ and C so that this matrix actually has the singular values of A along the diagonal.

R Note that $[A]_{\mathcal{S}_m \leftarrow \mathcal{S}_n} = A$ by Proposition 3.2.2.30.

Furthermore, $[A]_{C \leftarrow \mathcal{B}}$ is $m \times n$ matrix with the singular values of A along the diagonal. Thus, writing $\Sigma := [A]_{C \leftarrow \mathcal{B}}$, $V := [\mathrm{id}_{n\times n}]_{\mathcal{S}_n \leftarrow \mathcal{B}}$, and $U := [\mathrm{id}_{m\times m}]_{\mathcal{S}_m \leftarrow C}$, this equation is sometimes written more concisely (but perhaps less transparently) as

$$\Sigma = U^* A V. \quad (6.8.2.13)$$

R Using the same logic as in the analogous remark of Proposition 4.3.1.1, we find the following.

$V := [\mathrm{id}_{n\times n}]_{\mathcal{S}_n \leftarrow \mathcal{B}}$ and $U := [\mathrm{id}_{m\times m}]_{\mathcal{S}_m \leftarrow C}$ are the matrices whose columns are the eigenvectors of A^*A and AA^* respectively.

In particular, note that U and V are both unitary as $\mathcal{B}$ and C are both orthonormal (Proposition 6.6.4.19).

Proof. We leave this as an exercise.

Exercise 6.8.2.14 Prove the result.

■

■ **Example 6.8.2.15** Define

$$A := \begin{bmatrix} 1 & 0 & 3 \\ 4 & 0 & 0 \end{bmatrix}. \tag{6.8.2.16}$$

Then,

$$A^*A = \begin{bmatrix} 17 & 0 & 3 \\ 0 & 0 & 0 \\ 3 & 0 & 9 \end{bmatrix} \tag{6.8.2.17}$$

and

$$AA^* = \begin{bmatrix} 10 & 4 \\ 4 & 16 \end{bmatrix}. \tag{6.8.2.18}$$

We find that

$$\mathrm{Eig}(A^*A) = \{18, 8, 0\} \tag{6.8.2.19}$$

with

$$\mathrm{Eig}_{18} = \mathrm{Span}\left(\begin{bmatrix}3\\0\\1\end{bmatrix}\right) \tag{6.8.2.20a}$$

$$\mathrm{Eig}_{8} = \mathrm{Span}\left(\begin{bmatrix}-1\\0\\3\end{bmatrix}\right) \tag{6.8.2.20b}$$

$$\mathrm{Eig}_{0} = \mathrm{Span}\left(\begin{bmatrix}0\\1\\0\end{bmatrix}\right). \tag{6.8.2.20c}$$

Similarly, we find

$$\mathrm{Eig}(AA^*) = \{18, 8\} \tag{6.8.2.21}$$

with

$$\mathrm{Eig}_{18} = \mathrm{Span}\left(\begin{bmatrix}6\\12\end{bmatrix}\right) \tag{6.8.2.22a}$$

$$\mathrm{Eig}_{8} = \mathrm{Span}\left(\begin{bmatrix}8\\-4\end{bmatrix}\right). \tag{6.8.2.22b}$$

Thus, according to the above result, we should have

$$V^*AU \tag{6.8.2.23}$$

is diagonal, where[a]

$$U := \begin{bmatrix}\frac{3}{\sqrt{10}} & -\frac{1}{\sqrt{10}} & 0\\ 0 & 0 & 1\\ 0 & \frac{1}{\sqrt{10}} & \frac{3}{\sqrt{10}}\end{bmatrix}, \tag{6.8.2.24}$$

and

$$V := \frac{1}{\sqrt{5}}\begin{bmatrix}1 & -2\\ 2 & 1\end{bmatrix}. \tag{6.8.2.25}$$

And indeed, computing, we find

$$V^*AU = \begin{bmatrix} \sqrt{18} & 0 & 0 \\ 0 & -\sqrt{8} & 0 \end{bmatrix}. \tag{6.8.2.26}$$

This is almost what we want, except for that pesky minus sign. The solution is to go back and simply scale one of the corresponding eigenvectors by -1. For example, let us instead use

$$U := \begin{bmatrix} \frac{3}{\sqrt{10}} & \frac{1}{\sqrt{10}} & 0 \\ 0 & 0 & 1 \\ 0 & -\frac{1}{\sqrt{10}} & \frac{3}{\sqrt{10}} \end{bmatrix}, \tag{6.8.2.27}$$

Now we in fact have

$$\Sigma = V^*AU, \tag{6.8.2.28}$$

where

$$\Sigma := \begin{bmatrix} \sqrt{18} & 0 & 0 \\ 0 & \sqrt{8} & 0 \end{bmatrix}, \tag{6.8.2.29}$$

as desired.

[a] Note that I normalized the vectors before putting them as the columns of U and V.

6.9 Summary

An *inner-product* space is a complex vector space together with a bilinear map $\bar{V} \times V \to \mathbb{C}$ (Definition 6.3.1.2).

$\bar{V}$ is the *conjugate space* of V, which is defined to be the same as V except for scaling, which differs by a complex conjugate from that of V (Definition 6.2.2). The point of this concept is that conjugate-linear maps $V \to W$ are 'the same as' linear maps $\bar{V} \to W$ are 'the same as' linear maps $V \to \bar{W}$ (Theorem 6.2.7).

We saw that the inner-product defines a norm, $\|v\| := \sqrt{\langle v|v\rangle}$, and furthermore that a norm comes from a unique inner-product in this way iff it satisfies the Parallelogram Identity (Theorems 6.3.2.12 and 6.3.2.16). We also met the Cauchy-Schwarz Inequality, $|\langle v|w\rangle| \leq \|v\|\|w\|$ (Theorem 6.3.2.1).

We then noted that the existence of this norm gave us a notion of convergence, which resulted in a fundamental change from what we were used to: *arbitrary linear-combinations were now permitted to be infinite*. Before, they had to be finite because there was no definition of what infinite sums meant; now that we have a notion of convergence, infinite sums do make sense, and the 'right' notion of linear-combination means, well, *any* linear-combination, finite or not. (See Section 6.4.)

This in turn gave rise to the important of *completeness* (Definition 6.4.3.5), as such inner-product spaces are, in a sense, closed under 'all' linear-combinations. Similarly, this implied that it was the *closed* subspaces that played a more fundamental role in the theory, as these were the subspaces that were closed under taking *arbitrary* linear-combinations, not just finite one.

Furthermore, while none of this technically changed the definition of linear-independence, basis, etc.., one must be cautious as allowing the sums in these definitions changes the *consequences* of the definitions (though not the definitions themselves).

Having clarified this, we defined orthogonality (Definition 6.5.1.1) and orthonormality (Definition 6.5.1.6), gave several characterizations of orthonormal bases (Theorem 6.5.2.8), and proved that every Hilbert space has an orthonormal basis (Theorem 6.5.2.14). We also saw that one of the most important properties of *orthonormal* bases was that they easily allowed us to compute coordinates: if

$$v = \sum_{b\in\mathcal{B}} v^b \cdot b, \tag{6.9.1}$$

$\mathcal{B}$ an orthonormal basis, then

$$v^b = \langle b|v\rangle. \tag{6.9.2}$$

We then discussed the fundamental result that essentially says:

> For any vector and closed convex subset of a Hilbert space, there is a unique element in the subset closest to the given vector.

This allowed us to prove the Riesz Representation Theorem (Theorem 6.6.3.1):

> The canonical map $\bar{V} \to V^\dagger$ is an isomorphism.
>
> Equivalently, $\langle\cdot|\cdot\rangle\colon \bar{V} \times V \to \mathbb{C}$ is a nonsingular dual-pair.

It also allowed us to prove that (Corollary 6.6.2.1)

$$V = W \oplus W^\perp, \tag{6.9.3}$$

for $W \subseteq V$ a closed subspace of a Hilbert space, and define the projection $\text{proj}_W\colon V \to V$ onto a closed subspace $W \subseteq V$ (Theorem 6.6.2.10).

The Riesz Representation Theorem allowed us to show that the adjoint (Theorem 6.6.3.29) always exists in Hilbert spaces:

$$\langle T^*(v)|w\rangle = \langle v|T(w)\rangle. \tag{6.9.4}$$

The adjoint in hand, we were able to study normal (Definition 6.6.4.34), self-adjoint (Definition 6.6.4.1), unitary (Definition 6.6.4.9), and nonnegative (Definition 6.6.4.21) operators, these, roughly speaking, being the operator-theoretic analogue of complex numbers, real numbers, absolute value 1 complex numbers, and nonnegative real numbers respectively.

We subsequently discussed the Gram-Schmidt Algorithm (Proposition 6.6.5.23) and least-squares solutions. The former was an algorithm for taking in linearly-independent sets and spitting out orthonormal sets with the same span as the original set. This was also used to obtain the QR factorization of complex matrices (Proposition 6.6.5.28). As for the latter, a *least-squares solution* to the equation $T(x) = y_0$ was an $x_0 \in V$ that made $T(x_0)$ as close to y_0 as possible. The key result in this regard was Theorem 6.6.5.35, which

characterized the least-squares solutions of the equation $T(x) = y_0$ as the 'actual' solutions of the equation $T^*(T(x)) = T^*(y_0)$.

We ended the chapter with three big theorems: the Spectral Theorem (Theorem 6.7.1.2), the polar decomposition (Theorem 6.8.1.2), and the singular value decomposition (Theorem 6.8.2.8).

The Spectral Theorem gave a characterization of which operators are orthogonally diagonalizable in finite-dimensions: precisely the normal ones. One incredibly important fact for orthogonally diagonalizable operators is that (Proposition 6.7.1.5)

$$T = \sum_{b \in \mathcal{B}} \lambda_b \, |b\rangle\langle b| \,, \tag{6.9.5}$$

where $\mathcal{B}$ is an orthonormal basis consisting of eigenvectors of T and λ_b is the eigenvalue of $b \in \mathcal{B}$. It follows from this that

$$f(T) = \sum_{b \in \mathcal{B}} f(\lambda_b) \, |b\rangle\langle b| \tag{6.9.6}$$

for 'any' function f.

The polar decomposition allowed us to write any operator T in the form $T = U|T|$ for a unique partial isometry U with initial space $\mathrm{Ker}(T)^\perp$. This of course is the analogue of polar form for complex numbers: $z = re^{i\theta}$ in the usual notation.

Finally, the singular value decomposition said that for *any* linear-transformation T in finite dimensions, there are orthonormal bases $\mathcal{B}$ and $\mathcal{C}$ for the domain and codomain respectively such that $[T]_{\mathcal{C}\leftarrow\mathcal{B}}$ was diagonal.

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

7. Applications

So, apparently I'm expected to teach you applications or something like that. I thought it blatantly obvious all the myriad applications these ideas might have, but lest I get in trouble for not explicitly giving one, I present unto thee *applications of linear algebra*.

So, suppose you're walking down the street one night. The night is calm and peaceful. But then all of the sudden you are ambushed! A man is holding you at gunpoint and demands "If $2x = 4$, what is x?".

At first you are terrified, but very quickly realize, "OMG. I know how to solve this thanks to Jonny's MATH 110 class!". And so you begin to think: modules, Jordan canonical form, Hilbert spaces, index notation, the tensor-hom adjunction for bimodules.... And then it hits you: you can row-reduce!

So, using your ultra-sophisticated knowledge of linear-algebra, you consider the following augmented matrix.

$$\left[\begin{array}{c|c} 2 & 4 \end{array}\right] \tag{7.1}$$

This is a tricky one, especially to do in your head, but after hours of deliberation with a particularly patient criminal holding a gun to your head, you find the reduced echelon form

$$\left[\begin{array}{c|c} 1 & 2 \end{array}\right]. \tag{7.2}$$

Finally finished after such intense problem solving, you begin to explain your solution to the gunman. Upon finding out that you used row-reduction to solve the problem, the gunman is triggered and flees in terror.

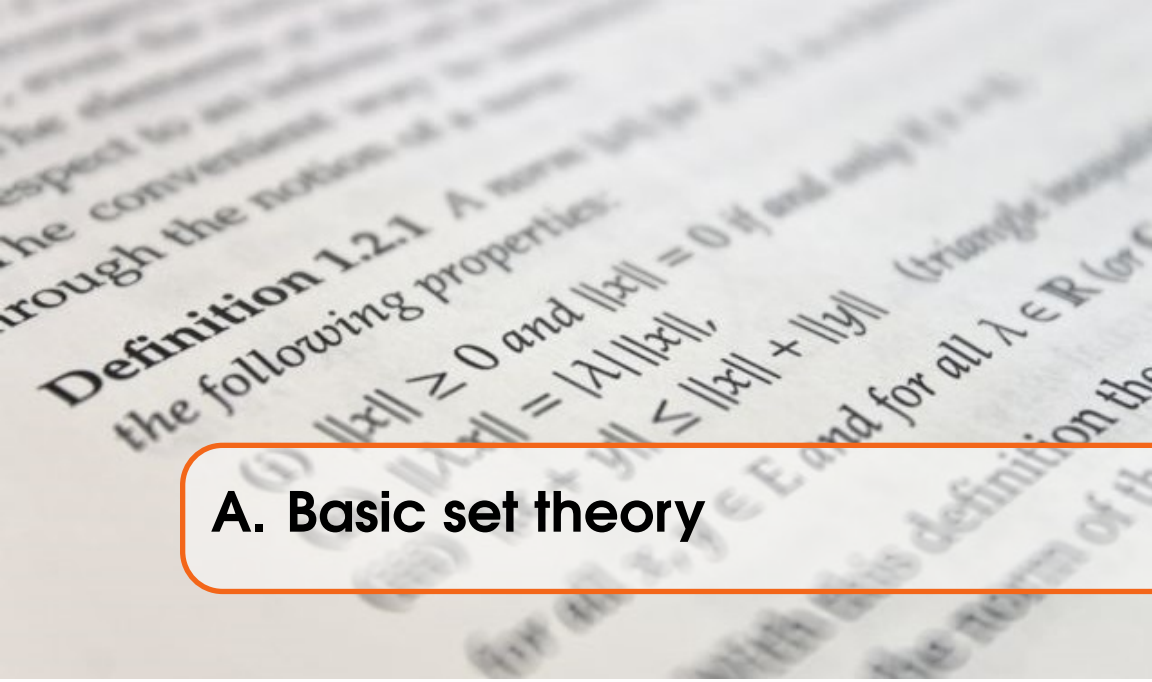
Congratulations. Linear algebra has just saved your life. #applications

A Basic set theory 495
A.1 What is a set?
A.2 The absolute basics
Some comments on logical implication
A bit about proofs
Iff 502
The following are equivalent 503
For all 503
The [illegible] proof by contradiction 503
Without loss of generality. 506
If XYZ we are done, so suppose that ¬XYZ . 506
Proving two sets are equal 507
Induction 507
Sets
A.3 Relations, functions, and orders
Arbitrary disjoint-unions and products
Equivalence relations
Preorders
Well-founded induction
Zorn's Lemma
A.4 Sets with algebraic structure
Quotient groups and quotient rngs
A.5 Cardinality, countability, and the naturals
Cardinality
The natural numbers
Countability

B Basic category theory 577
B.1 What is a category?
B.2 Some basic concepts
B.3 Functors and natural-transformations
Functors
Natural-transformations

C Results from ring theory 599
C.1 Prerequisites
C.2 Ideals and their quotients
Some properties of rings
Some properties of ideals
Their noncommutative variants
The dictionary
Summary
C.3 The integral closure
Associative algebras
Polynomials
Polynomials vs. polynomial functions 627
Algebraic and integral
Summary
C.4 Perfect fields
C.5 (Semi)simplicity

Appendices



A. Basic set theory

A.1 What is a set?

While set theory is of course not the object of study of these notes, a certain amount of basic knowledge about sets is necessary for the study of essentially any area of mathematics. As this is possibly the first upper-division mathematics course you've taken, I cannot assume you know any set theory. On the other hand, as it isn't of direct interest in its own right, the requisite material has been placed in this appendix.

Though at this level we're really talking about philosophy and I'm sure other mathematicians have different viewpoints than me on this, my understanding of the foundations of mathematics is as follows. First of all, one cannot get something from nothing; if you want to be able to make deductions, you're going to have to assume certain things. For example, if you don't accept basic logical truths (e.g., from "A implies B." and "A" one can deduce B), you're not going to get anywhere. Similarly, if we don't accept the fact that it makes sense to give names to certain ideas so that we can later refer to them (as I just did, e.g. "A"), then we're likewise not going to get very far. However, if we do make very simple assumptions about the type of mental tools one is able to use when doing mathematics, one is able to

deduce all sorts of wondrous things. I thus ask that you that grant me (i) that naive logical deduction is valid; and (ii) that the naive concept of a 'set' is valid.

When I say "naive concept of a 'set"', I am referring to the idea that, if you have a collection of things, whatever they may be, you are allowed to give that collection of things a name (e.g. "X"), and now X is a new thing that we may talk about, the *set* of the aforementioned things. From this perspective, you might say that the naive notion of a set is more a linguistic tool than anything else, and in this sense is a special case of the idea mentioned in the previous paragraph that one should be allowed to assign names to ideas so that we may later refer to them. Indeed, because of this, for the most part, we will completely ignore any set-theoretic concerns in these notes, but before we do just blatantly ignore any potential issues, we should first probably (attempt to) justify this dismissal.

Intuitively, a set is just a thing that 'contains' a bunch of other things, but this itself is of course not a precise mathematical definition. Ultimately, I claim there there is no need to have such a precise definition, but let's suppose for the moment that we would like to define what a set is. One way to do this would be to attempt to develop an axiomatic set theory, but there is a certain 'circularity' problem in doing this.

The term "axiomatic set theory" here refers to any collection of axioms which attempt to make precise the intuitive idea of a set. In a given theory, however, the symbols which we make use of to write down the axioms themselves form a *set*. The point is that, in attempting to write down a mathematically precise definition of a set, one must make use of the naive notion of a set.

Of course this example might not be very convincing. Why not just not think of all the symbols together and just think of them individually? It is true that if you fudge things around a bit you may be able to convince yourself that you're not really making use of the naive notion of a set here. That being said, even if you can convince yourself that you can get around the problem of first requiring a 'set' of symbols, sooner or later, in attempting to make sense out of an axiomatic set theory, you will need to make use of the naive notion of a set.

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Because of this, we consider the idea of a set to be so fundamental as to be undefinable, and we simply assume that we can freely work with this intuitive idea of a collection of things all thought of as one thing, namely a set.

One has to be careful however. Naive set theory has paradoxes, a famous example of which is Russel's Paradox. Consider for example the set[1]

$$X := \{Y : Y \notin Y\}\,. \tag{A.1.1}$$

Is $X \in X$? One resolution of this paradox is that it is nonsensical to construct the set of *all* things satisfying a certain property. Whenever you construct a set in this manner, your objects have to be already 'living inside' some other set. For example, we can write

$$X := \{Y \in U : Y \notin Y\} \tag{A.1.2}$$

for some fixed set U.[2] Russel's Paradox now becomes the statement that $X \notin U$.

This is still somehow not enough. For example, if you turn to Example B.1.3, the category of sets, you'll see that we do need to make use of the notion of the collection of "all sets", and we've just said that we are not allowed to quantify over *everything*, but only over things that are elements of a fixed set. One way to do this is to fix a set U which is closed under all the usual operations of set theory,[3] and then to interpret statements that refer to something like "All sets such that. . . " as in fact meaning "All elements of U such that. . . ". Upon doing this, the construction involved in Russel's Paradox is perfectly valid, and indeed, does give us a new set, and the 'paradox' itself now simply becomes the argument that this new set is not an element of U.[4]

[1] Hopefully you have seen notation like this before. If not, really quickly skip ahead to Appendix A.2 The absolute basics to look up the meaning of this notation.

[2] "U" is for "universe".

[3] One way in which to make this precise is what is called a *Grothendieck universe*. The details of this will not matter for us, but if you're curious feel free to Google the term.

[4] One nice thing about this approach of avoiding paradoxes is that *everything* is still a set, that is, there is no need to make this awkward distinction between 'actual' sets and what would be referred to as *proper classes* .

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

The content of this section was meant only to convince you that (i) there is no way of getting around the fact that the idea of collecting things together is undefinably fundamental, and that (ii) ultimately this naive idea is not paradoxical.

Disclaimer: I am neither a logician nor a set-theorist, so take what I say with a grain of salt.

A.2 The absolute basics

A.2.1 Some comments on logical implication

For us, the term ***statement*** will refer to something that is either true or false. The word ***iff*** is short-hand for the phrase *if and only if*. So, for example, if A and B are statements, then the sentence "A iff B." is logically equivalent to the two sentences "A if B." and "A only if B.". In symbols, we write $B \Rightarrow A$ and $A \Rightarrow B$ respectively. The former logical implication is perhaps more obvious; the other might be slightly trickier to translate from the English to the mathematics. The way you might think about it is this: if A is true, then, because A is true *only if* B is true, it must have been the case that B was true too. Thus, "A only if B." is logically equivalent to "A implies B.". We then write "$A \Leftrightarrow B$ as alternative notation for the English "A iff B".

If A and B are statements, then $A \Rightarrow B$ is a statement: True $\Rightarrow$ True is considered true, True $\Rightarrow$ False is considered false, False $\Rightarrow$ True is considered true, and False $\Rightarrow$ False is considered true. Hopefully the first two of these make sense, but how does one understand why it should be the case that False $\Rightarrow$ True is true? To see this, I think it helps to first note the following.[5]

$$\text{"}\forall x \in X,\ \mathcal{P}(x)\text{."} \text{ is logically equivalent to "} x \in X \Rightarrow \mathcal{P}(x)\text{."}, \tag{A.2.1.1}$$

where $\mathcal{P}(x)$ is a statement that depends on x.

Now consider the following example in English.

Every pig on Mars owns a shotgun. (A.2.1.2)

[5]The symbol "$\forall$" in English reads "for all". Similarly, the symbol "$\exists$" is read as "there exists".

Is this statement true or false? Under the (hopefully legitimate assumption) that there is no pig on Mars at all, my best guess is that most native English speakers would say that this is a true statement. In any case, this is mathematics, not linguistics, and for the sake of definiteness, we simply declare a statement such as this to be *vacuously true* (unless of course there are pigs on Mars, in which case we would need to determine if they all owned shotguns). This example is meant to convince you that, in the case that X is empty, it is reasonable to declare the statement $\forall x \in X, P(x)$ to be true for tautological reasons.

Now, appealing back to (A.2.1.1), hopefully it now also seems reasonable to declare statements of the form False $\Rightarrow B$ to be true (where B is any statement), likewise for tautological reasons.

If we know a certain statement to be true, there are several other statements that we know automatically to be true. For example, if A is true, then $\neg\neg A$ is automatically true.[6] Another important example of this is given by the *contrapositive*.

Definition A.2.1.3 — Converse, inverse, and contrapositive Let A and B be statements. Then,

(i). the ***converse*** of the statement $A \Rightarrow B$ is the statement $B \Rightarrow A$;
(ii). the ***inverse*** of the statement $A \Rightarrow B$ is $\neg A \rightarrow \neg B$; and
(iii). the ***contrapositive*** of the statement $A \Rightarrow B$ is $\neg B \rightarrow \neg A$.

R Referring back to our earlier comments on the phrase "iff", if ever you want to prove "A iff B", you must prove $A \Rightarrow B$ (i.e. "A only if B.") as well as its *converse*, $B \Rightarrow A$ (i.e. A if B).

Proposition A.2.1.4 Let A and B be statements. Then, $A \Rightarrow B$ is true iff its contrapositive $\neg B \Rightarrow \neg A$ is true.

[6] $\neg A$, read "not A", is a statement which is false if A and is true if A is false.

Proof. ($\Rightarrow$) Suppose that $A \Rightarrow B$ is true. We would like to show that $\neg B \Rightarrow \neg A$. So, suppose that $\neg B$ is true. We would then like to prove $\neg A$. We proceed by contradiction: suppose that A is true. Then, as $A \Rightarrow B$, it must be that B is true: a contradiction of the fact that we have assumed that $\neg B$ is true. Therefore, our assumption that A is true must have been false. Thus, it must be that $\neg A$ is true.

($\Leftarrow$) As the contrapositive of the contrapositive is the original statement, this follows from ($\Rightarrow$). ■

▪ **Example A.2.1.5** Let P be the statement "If it is raining, then it is wet.".

The converse of P is "If it is wet, then it is raining.".

The inverse of P is "If it is not raining, then it is not wet.".

The contrapositive of P is "If it is not wet, then it is not raining.

Hopefully this makes it clear how the converse can be false even if the original statement is true. Also be sure to understand in this example how the contrapositive is indeed equivalent to the original statement.

Given that a statement is true iff its contrapositive is true, it is important to know how to correctly negate statements (and of course this is important to know for other reasons as well).

▪ **Example A.2.1.6** Let $\mathcal{P}(x)$ be a statement that depends on x.

(i). "$\neg(\forall x,\ \mathcal{P}(x))$" is equivalent to "$\exists x,\ \neg\mathcal{P}(x)$".
(ii). "$\neg(\exists x,\ \mathcal{P}(x))$" is equivalent to "$\forall x,\ \neg\mathcal{P}(x)$".
(iii). "$\neg(A$ and $B)$" is equivalent to "$\neg A$ or $\neg B$".
(iv). "$\neg(A$ or $B)$" is equivalent to "$\neg A$ and $\neg B$".

R For example, suppose you want to prove the statement "Every positive integer is even." is *false*. To do

this, you want to exhibit a positive integer which is not even. Explicitly, the original statement is "$\forall x \in \mathbb{Z}^+,\ x$ is even.", and so its negation is "$\exists x \in \mathbb{Z}^+,\ x$ is not even.". For some reason, this tends to trip students up when I ask them to show that a statement is false: to prove that statements of this form[a] are false, you *must* exhibit a counter-example—explaining why a counter-example should exist, without *proving*[b] one exists, is not enough. For example, don't say "The statement "Every partially-ordered set is totally-ordered." is false because there is an extra condition in the definition of totally-ordered."—in this case, you *must* give an example of a partially-ordered set which is not totally-ordered.[c]

[a] That is, of the form "$\forall x,\ \mathcal{P}(x)$". Of course, not every statement is of this form, and so proving a statement is false doesn't necessarily mean you have to give a counter-example (for example, if I ask you to prove that $|\mathbb{N}| = |\mathbb{R}|$ is false, it would not make sense to give a counter-example).

[b] It is almost always the case that the easiest way to prove a counter-example exists is simply to write one down.

[c] See Definitions A.3.3.6 and A.3.3.13.

A.2.2 A bit about proofs

Proofs are absolutely fundamental to mathematics. Indeed, you might say that mathematics *is* the study of those truths which are provable.[7] But what actually *is* a proof?

A proof is essentially just a particularly detailed argument that a statement is true. The question then is "How much detail?". Well, an extremist might say that a proof should be detailed enough so as to be verifiable by a computer—if a computer can verify it using axioms alone, then there can be no doubt at all as to the truth of the statement. Doing this in practice, however, well, would be a little bit insane—no one (or almost no one) writes proofs in this amount of detail.

[7] In contrast to those truths are which true by observation. For example, while the statements "$x \in \mathbb{R}$ implies $x^2 \geq 0$." and "The mass of the electron is $9.109\,383\,56(11) \times 10^{-31}$ kg." are both true, they are true in fundamentally different ways—the former is true because we can prove it and the latter is true because we measure it.

The objective then I would say it to provide enough detail so as to convince *your target audience* that enough detail could be filled in, at least *in principle*, so as to be verified by a computer, if a member of your target audience really wanted to take (waste?) their time doing so. This is why two different proofs of the same statement, one several pages long and another a paragraph long, can both be considered equally valid proofs: one proof could have been written to be accessible to undergraduates and the other to be accessible to professional mathematicians. As a student, however, I would recommend you consider your target audience to be *yourself*. You should put down enough detail so that, if you came back to your proof after a year of not thinking about it, you should be able to follow your work no problem. In particular, if you're ever writing a proof and you wonder "Is this valid?", the answer is "No, it's not valid."—you need to add more detail until there is *no doubt* whatsoever that your argument is correct. Tricking me (or yourself) into thinking you know the details when in fact you do not is not the way to go about learning mathematics.

Okay, so enough with this wishy-washy philosophical BS. I should probably at least give you some *concrete* advice about proof-writing. I think probably most of proof-writing should be learned by doing, but I suppose I can say at least a couple of things.[8][9]

Iff

We mentioned the meaning of the word "iff" in the previous section, and we wound up giving an example of a proof which involved the phrase (Proposition A.2.1.4). Allow us to elaborate.

[8]Keep in mind that in the following subsubsections we will often make use of examples to illustrate concepts that we technically have not yet developed the mathematics for yet. First of all, you needn't worry, as because we are just using the examples for the purposes of illustration, this doesn't make our development circular. Secondly, if you can't follow an example because you haven't seen it before, don't worry—just get what you can out of it and move on.

[9]If you are fine with proofs, you can probably safely skip to the next subsection, Appendix A.2.3 Sets.

> If ever asked to prove a statement of the form "A iff B", you need to prove *two things*: first, assuming A, you prove B; then, assuming B, you prove A.

See Proposition A.2.1.4 for a concrete example of this.

The following are equivalent

The phrase "The following are equivalent." is similar to the phrase "iff", but is used when dealing with more than two statements. For example, consider the following claim.

> Let $m, n \in \mathbb{Z}$. Then, the following are equivalent.
>
> (i). $m < n$.
> (ii). $m \leq n - 1$.
> (iii). $m + 1 \leq n$.

To prove this, you need to prove that (i) iff (ii), (i) iff (iii), and (ii) iff (iii)—this is exactly what it means for all the three statements to be logically-equivalent to one another. On the face of it, it seems like this would mean we would have to do $2 \times 3 = 6$ proofs. Not so. In fact, it is enough to prove (i) implies (ii), (ii) implies (iii), and (iii) implies (i). Using these three implications alone, you can go from any one statement to any other. For example, (ii) implies (i) because, if (ii), then (iii), and hence (i).

For all...

If the statement you are trying to prove is of the form "$\forall X \in X$, $\mathcal{P}(x)$", you should almost certainly start your proof with something like "Let $x \in X$ be arbitrary." You then prove $\mathcal{P}(x)$ itself. Pretty self-explanatory.

The contrapositive and proof by contradiction

Proof by contradiction and *proof by contraposition* are two closely related proof techniques. In fact, in a sense to be explained below, they're the *same* proof technique. Before we get there, however, let us first explain what these two techniques refer to.

First, we explain "contradiction". Assume you want to prove the statement "A implies B.". Of course, you first assume that A is true. You now try to prove that B is true. Sometimes doing this directly can prove difficult, and in such cases, you can try what is referred to as *proof by contradiction*: Suppose that $\neg B$ is true. Now, using A *and* $\neg B$, try to prove something you already know to be false. As the *only* assumption you made was $\neg B$, that assumption must have been incorrect, and therefore $\neg\neg B$ is true, and hence B is true.[10]

On the other hand, *proof by contraposition* refers to nothing more than an application of Proposition A.2.1.4. That is, if you would like to prove that "A implies B", you instead prove that "$\neg B$ implies $\neg A$".

All that remains in this subsubsection is an explanation of the relationship between proof by contraposition and proof by contradiction. As this relationship is not particularly important, feel free to skip to the next subsubsection.

Superficially, proof by contradiction and proof by contraposition appear to be distinct, but related techniques. On the other hand, they are equivalent in a sense to be described as follows.[11] First of all, we have to be precise about what we mean by "proof by contradiction" and "proof by contraposition". The precise statement of "proof by contraposition" is given in Proposition A.2.1.4: "A implies B" is equivalent to "$\neg B$ implies $\neg A$". On the other hand, the precise statement of "proof by contradiction" is given in the following statement.

Proposition A.2.2.1 Let A and B be statements. Then, $A \Rightarrow B$ is true iff (A and $\neg B$) $\Rightarrow$ False is true.

[10]This logic implicitly uses what is called the *Principle of the Excluded Middle*, which says that, if A is a statement, then A is true or A is false. Some mathematicians reject this as valid (or so Wikipedia claims). They are crazy. Such crazy mathematicians thus cannot use proofs by contradiction. Pro-tip: don't be crazy.

[11]The explanation of exactly in what sense these two proof techniques are equivalent is not particularly useful. Certainly, I find it highly unlikely that what follows in this subsubsection will be of significant use in actual proof writing. Thus, feel free to skip to the end of the following proof unless you are particularly curious.

Proof. ($\Rightarrow$) Suppose that $A \Rightarrow B$ is true. We would like to show that (A and $\neg B$) $\Rightarrow$ False. So, suppose that A and $\neg B$ are true. As $A \Rightarrow B$ is true, it follows that B is true. But then, B and $\neg B$ are true, and hence FALSE.

($\Leftarrow$) Suppose that (A and $\neg B$) $\Rightarrow$ False is true. Taking the contrapositive, it follows that $\neg A$ or B is true. We would like to show that $A \Rightarrow B$ is true. Taking the contrapositive again, it suffices to show that $\neg B \Rightarrow \neg A$. So, suppose $\neg B$. We wish to prove $\neg A$. However, as we know that $\neg A$ or B is true, it in fact must be the case that $\neg A$ is true. ■

If you examine the proofs of Proposition A.2.1.4 and Proposition A.2.2.1,[12] you will find respectively that the former makes use of proof by contradiction and that the latter makes use of proof by contraposition. It is in this sense that they are equivalent proof techniques.

Okay, so up until now, this has all be pretty precise, but I would like to give an intuitive explanation as to the difference between the two. Every proof by contraposition and be reduced to a proof by contradiction in the following way: assume your hypotheses A, proceed by contradiction and assume $\neg B$, and proceed to prove $\neg A$: contradiction. The key is that in a proof by contraposition your contradiction is of the form A and $\neg A$, whereas with proof by contradiction you obtain more general contradictions. Thus, while superficially proof by contradiction might seem much stronger, it is in fact not actually so. This is similar to how "the Principle of Strong Induction seems stronger than (just) the Principle of Induction, but in fact they are equivalent statements—see below.

Finally, we end with a quick comment on usage. First of all, it is very easy to rephrase a proof by contraposition as a proof by contradiction (as explained above), and so, if you like, you needn't worry about proof by contraposition at all. Furthermore, proof by contradiction tends to be most useful when "B" in "A implies B." is

[12] The precise statements of "proof by contraposition" and "proof by contradiction" respectively.

somehow 'already negated'—for example, think of how one might try to prove the statement "If $x \in \mathbb{R}$ and $x^2 = 2$, then $\sqrt{x} \notin \mathbb{Q}$.".

Without loss of generality...

You will often see the phrase "Without loss of generality..." used in proofs. It is easiest to demonstrate what this means, and how to use it yourself, with an example.

The definition of integral (Definition A.4.22) reads

> A rg $\langle X, +, 0, \cdot \rangle$ is *integral* iff it has the property that, whenever $x \cdot y = 0$, it follows that either $x = 0$ or $y = 0$.

So, imagine you were doing a proof, and you know that $\langle X, +, 0, \cdot \rangle$ was an integral rg,[13] and that $x \cdot y = 0$ for $x, y \in X$. The definition of integral implies that $x = 0$ or $y = 0$. *At this point, you could say*, "Without loss of generality, suppose that $x = 0$.". You then continue the proof using the fact that $x = 0$.

Logically, you would first have to assume that $x = 0$, finish the proof in that case, and then go back to the case where $y = 0$, and finish the proof again. However, if the proofs are essentially identical[14] in these two cases, you are 'allowed' to cut your work in half with the phrase "Without loss of generality..."—there is no point in repeating the same logic with a different letter twice.

If XYZ we are done, so suppose that ¬XYZ

As with "Without loss of generality...", the use of this phrase is easiest to demonstrate with an example.

The definition of *prime* reads

[13] You shouldn't need to know what a rg is to understand the explanation of "Without loss of generality...".

[14] Obviously, if the proof needed to do the case $x = 0$ is significantly different from the proof needed to do the case $y = 0$ (i.e. is more than just a letter swap $x \leftrightarrow y$), you should not use this phrase and instead write up the proofs of both cases individually.

> Let $p \in \mathbb{Z}$. Then, p is *prime* iff . . . whenever $p \mid (mn)$, it follows that $p \mid m$ or $p \mid n$.[a]
>
> [a] We have omitted part of the definition in the ". . . " that is irrelevant for us at the moment (essentially the requirement that $p \neq -1, 0, 1$).

So, let $p \in \mathbb{Z}$ and suppose that you want to prove that p is prime. To prove this condition, you would say "Let $m, n \in \mathbb{Z}$ and suppose that $p \mid (mn)$." From here, you now want to prove that $p \mid m$ or $p \mid n$. At this point, you can say "If $p \mid m$ we are done, so suppose that $p \nmid m$.".

Hopefully, the logic of this is pretty self-explanatory. If it helps, however, you can view this as essentially the same as proof by contradiction. If we were to proceed by contradiction, instead we would say "Suppose that $p \nmid m$ and $p \nmid n$.", and from that deduce a contradiction. Instead, in this case, we shall assume $p \nmid m$, and use that to prove that $p \mid m$.

Proving two sets are equal

A lot of proofs require you to show that two different sets are in fact one in the same. The way to prove this is made precise with Exercise A.2.3.4. In the meantime, however, we can say the following.

> Let S and T be sets and suppose that you want to prove that $S = T$. You then need to prove *two* things: if $s \in S$, then $s \in T$; and if $t \in T$, then $t \in S$.

This logic is very much identical to that used for proving "iff" statements.

Induction

Induction

Let $\mathcal{P}_m$ be a statement for $m \in \mathbb{N}$. The ***Principle of Induction*** says that

> If (i) $\mathcal{P}_0$ is true and (ii) $\mathcal{P}_m \Rightarrow \mathcal{P}_{m+1}$ is true for all $m \in \mathbb{N}$, then $\mathcal{P}_m$ is true for all $m \in \mathbb{N}$.[a]
>
> [a](i) is referred to as the ***initial case*** or the ***initial step***, and (ii) is referred to as the ***inductive step***.

The logic is as follows. Suppose we want to prove $\mathcal{P}_3$. Then, because $\mathcal{P}_0$ and $\mathcal{P}_0 \Rightarrow \mathcal{P}_1$, it follows that $\mathcal{P}_1$.[15] Then, because $\mathcal{P}_1$ and $\mathcal{P}_1 \Rightarrow \mathcal{P}_2$, it follows that $\mathcal{P}_2$. Then, because $\mathcal{P}_2$ and $\mathcal{P}_2 \Rightarrow \mathcal{P}_3$, it follows that $\mathcal{P}_3$. Of course, nothing is special about $m = 3$, and so this logic can be used to prove $\mathcal{P}_m$ for all $m \in \mathbb{N}$.[16]

You can also use similar logic to define things. For example, you might define a bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ by

$$f(0) := \langle 0, 0 \rangle$$
$$f(m+1) := \begin{cases} \langle f(m)_x - 1, f(m)_y + 1 \rangle & \text{if } f(m)_x \geq 1 \\ \langle f(m)_x + f(m)_y + 1, 0 \rangle & \text{otherwise.}[17] \end{cases} \quad \text{(A.2.2.2)}$$

Strong Induction

Equally as valid, for the exact same reason, is what is sometimes referred to the ***Principle of Strong Induction***, which says that

> If (i) $\mathcal{P}_0$ is true and (ii) $(\forall 0 \leq k \leq m,\ \mathcal{P}_k) \Rightarrow \mathcal{P}_{m+1}$ is true for all $m \in \mathbb{N}$, then $\mathcal{P}_m$ is true for all $m \in \mathbb{N}$.

The key difference between this and 'regular' induction is that, in the induction step, you don't just assume $\mathcal{P}_m$, but instead, you assume $\mathcal{P}_0$, and $\mathcal{P}_1$, and $\mathcal{P}_2$, and $\ldots \mathcal{P}_m$. Superficially, this does indeed seem

[15]Incidentally, the passage from "A and $A \Rightarrow B$" to B is called *modus ponens*, which itself is short for "modus pōnendō pōnēns", which is Latin for (literally) "the method to be affirmed, affirms".

[16]Though it won't be able to prove $\mathcal{P}_\infty$! For example, a common fake proof that π is rational essentially proves by induction that, for all $m \in \mathbb{Z}^+$, the decimal approximation of π with m digits is rational, and 'therefore' π is rational. Sorry, but that's not how induction works.

[19]The picture is that you go 'down the diagonal', unless you 'hit the edge', in which case you 'hop to the top of the next diagonal'.

stronger,[20] but in fact 'regular' induction and strong induction are equivalent, though sometimes it can be quite convenient to be make use of all of $\mathcal{P}_0, \ldots, \mathcal{P}_m$ instead of just $\mathcal{P}_m$.

For example, suppose that you want to prove that every positive integer greater-than-or-equal to 2 is divisible by some prime. In this case, the initial step is simply to prove that "2 is divisible by some prime.". This is of course trivial: 2 is divisible by 2, which is prime. Here's where things get a bit different, however: for the inductive step, assume that $2, 3, 4, \ldots, m$ are all divisible by some prime. Using this, we want to show that $m + 1$ is divisible by some prime. Well, either $m + 1$ is prime itself, in which case $m + 1$ is divisible by $m + 1$, or it is not prime, in which case $m + 1$ is divisible by some integer k with $2 \leq k \leq m$. By the induction hypothesis, k is divisible by some prime, and hence $m + 1$ is in turn divisible by some prime.

Note that we will not usually make a distinction between 'regular' induction and strong induction in these notes. When using either method, we shall simply say something like "We proceed by induction. . . ".

Well-founded induction

The most powerful form of induction which subsumes all other 'types' of induction is known as *well-founded induction*. As it is less elementary than what we have discussed thus far, we leave a detailed discussion of this until Appendix A.3.4. We can, however, at least say a little for the time being..

The basic idea is to replace the set with which you index your statements (previously $\mathbb{N}$) with a more general type of set X. It turns out that the only structure on $\mathbb{N}$ relevant to induction is the ordering, and so you don't just replace $\mathbb{N}$ with a set X, you replace $\langle \mathbb{N}, \leq \rangle$ with a pair $\langle X, \preceq \rangle$, where X is a set and $\preceq$ is a *relation* (Definition A.3.1) on X. It turns out that (Theorem A.3.4.3) the only property of $\leq$ on $\mathbb{N}$ that was necessary for induction to work is what is called *well-foundedness* (Definition A.3.5.3), which states that every nonempty subset has a minimal element (Definition A.3.5.3).

The ***Principle of Well-Founded Induction*** then says that

[20] Because during the inductive step, you don't get to assume just the single statement $\mathcal{P}_m$, but rather the $m + 1$ statements $\mathcal{P}_0$, and $\mathcal{P}_1$, and $\mathcal{P}_2$, and $\ldots \mathcal{P}_m$.

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

If for every $x_0 \in X$, $(\forall x < x_0, \mathcal{P}_x) \Rightarrow \mathcal{P}_{x_0}$, then $\mathcal{P}_x$ is true for all $x \in X$.

If you ever want to perform an induction-like argument, but it's not working because you have more than countably-infinite many statements, try well-founded induction.

Finally, we mention that there is a method of proof called *transfinite induction*. It is technically a special case of well-founded induction, but much more common.[21] Roughly speaking, transfinite induction is to well-ordered as well-founded induction is to well-founded. We refrain from discussing it because (i) we don't need to—well-founded induction is stronger and (ii) the usual way it's stated requires the development of what are called *ordinals*), which would take us quite astray. Still, you should be aware of it so you can go and learn it if you ever feel this will be useful to you (if you become a mathematician, it almost certainly will be at some point).

A.2.3 Sets

The idea of a set is something that contains other things.

If X is a ***set*** which contains an ***element*** x, then we write $x \in X$.[23] Two sets are equal iff they contain the same elements. (A.2.3.1)

Definition A.2.3.2 — Empty-set The ***empty-set***, $\emptyset$, is the set $\emptyset := \{\}$.

R That is, $\emptyset$ is the set which contains no elements.

R If ever you see an equals sign with a colon in front of it (e.g. in "$\emptyset := \{\}$"), it means that the equality is true *by definition*. This is used in definitions themselves, but also outside of definitions to serve as a reminder as to why the equality holds.

[21] For some reason, not too many people seem to know of well-founded induction.

[27] Sometimes we will also write $X \ni x$ if it happens to be more convenient to write it in that order (for example, in $\mathbb{R} \ni x \mapsto x^2$).

Definition A.2.3.3 — Subset Let X and Y be sets. Then, X is a ***subset*** of Y, written $X \subseteq Y$, iff whenever $x \in X$ it is also the case that $x \in Y$.

R Generally speaking we put slashes through symbols to indicate that the statement that would have been conveyed without the slash is false. For example, $x \notin X$ means that x is not an element of X, the statement that $X \not\subseteq Y$ means that X is not a subset of Y, etc..

Exercise A.2.3.4 Let X and Y be sets. Show that $X = Y$ iff $X \subseteq Y$ and $Y \subseteq X$.

Definition A.2.3.5 — Proper subset Let X be a subset of Y. Then, X is a ***proper subset*** of Y, written $X \subset Y$, iff there is some $y \in Y$ that is not also in X.

R You should note that many authors use the notation "$X \subset Y$" simply to indicate that X is a (*not-necessarily-proper*) subset of Y.

R Let X be a set, let $\mathcal{P}$ be a property that an element in X may or may not satisfy, and let us write $\mathcal{P}(x)$ iff x satisfies the property $\mathcal{P}$. Then, the notation

$$\{x \in X : \mathcal{P}(x)\}$$

is read "The set of all elements in X such that $\mathcal{P}(x)$." and represents a set whose elements are precisely those elements of X for which $\mathcal{P}$ is true. Sometimes this is also written as

$$\{x \in X | \mathcal{P}(x)\},$$

but my personal opinion is that this can look ugly (or even slightly confusing) if, for example, $\mathcal{P}(x)$ contains an absolute value in it, e.g.

$$\{x \in \mathbb{R} | |x| < 1\}.$$

Definition A.2.3.6 — Complement Let X and Y be sets. Then, the ***complement*** of Y in X, $X \setminus Y$, is defined by

$$X \setminus Y := \{x \in X : x \notin Y\}. \tag{A.2.3.7}$$

If X is clear from context, sometimes we write $Y^{\mathsf{C}} := X \setminus Y$.

Definition A.2.3.8 — Union and intersection Let A, B be subsets of a set X. Then, the ***union*** of A and B, $A \cup B$, is defined by

$$A \cup B := \{x \in X : x \in A \text{ or } x \in B\}. \tag{A.2.3.9}$$

The ***intersection*** of A and B, $A \cap B$, is defined by

$$A \cap B := \{x \in X : x \in A \text{ and } x \in B\}. \tag{A.2.3.10}$$

R More generally, if $\mathscr{S}$ is a collection[a] of subsets of X, then the *union* and *intersection* of all sets in $\mathscr{S}$ are defined by

$$\bigcup_{S \in \mathscr{S}} S := \{x \in X : \exists S \in \mathscr{S} \text{ such that } x \in S.\}$$

and

$$\bigcap_{S \in \mathscr{S}} S := \{x \in X : \forall S \in \mathscr{S},\ x \in S.\}.$$

[a] Technically, the term ***collection*** is just synonymous with the term "set", though it tends to be used in cases when the elements of the set itself are to be thought of as other sets (e.g. here where the elements of $\mathscr{S}$ are subsets of X).

Definition A.2.3.11 — Disjoint and intersecting Let A, B be subsets of a set X. Then, A and B are ***disjoint*** iff $A \cap B = \emptyset$. A and B ***intersect*** (or ***meet***) iff $A \cap B \neq \emptyset$.

Exercise A.2.3.12 — De Morgan's Laws Let $\mathscr{S}$ be a collection of subsets of a set X. Show that

$$\left(\bigcup_{S\in\mathscr{S}} S\right)^{\mathsf{C}} = \bigcap_{S\in\mathscr{S}} S^{\mathsf{C}} \text{ and } \left(\bigcap_{S\in\mathscr{S}} S\right)^{\mathsf{C}} = \bigcup_{S\in\mathscr{S}} S^{\mathsf{C}}. \quad \text{(A.2.3.13)}$$

Exercise A.2.3.14 Let X be a set and let $S, T \subseteq X$. Show that $S \setminus T = S \cap T^{\mathsf{C}}$.

Definition A.2.3.15 — Symmetric-difference Let A, B be subsets of a set X. Then, the ***symmetric-difference*** of A and B, $A \triangle B$, is defined by

$$A \triangle B := (A \cap B^{\mathsf{C}}) \cup (A^{\mathsf{C}} \cap B). \quad \text{(A.2.3.16)}$$

R If you draw a "Venn diagram", you break up X into four disjoint pieces: everything outside A and B, things inside both A and B, things inside A but not B, and things inside B but not A. The symmetric difference is the union of the last two regions.

Put another way, the symmetric difference is the elements in $A \cup B$ that A and B do *not* have in common.

The union and intersection of two sets are ways of constructing new sets, but one important thing to keep in mind is that, a priori, the two sets A and B are assumed to be contained within another set X. But how do we get entirely new sets without already 'living' inside another? There are several ways to do this.

Definition A.2.3.17 — Cartesian-product Let X and Y be sets. Then, the *Cartesian-product* of X and Y, $X \times Y$, is

$$X \times Y := \{\langle x, y\rangle : x \in X, y \in Y\} . \tag{A.2.3.18}$$

R If you really insist upon everything being defined in terms of sets we can take

$$\langle x, y\rangle := \{x, \{x, y\}\} . \tag{A.2.3.19}$$

The reason we use the notation $\langle x, y\rangle$ as opposed to the probably more common notation (x, y) is to avoid confusion with the notation for open intervals.

R If $Y = X$, then it is common to write $X^2 := X \times X$, and similarly for products of more than two sets (e.g. $X^3 := X \times X \times X$). Elements in finite products are called ***tuples*** or sometimes ***lists***. For example, the elements of X^2 are 2-tuples (or just ***ordered pairs***), the elements in X^3 are 3-tuples, etc..[a]

[a] If you really want to be pedantic about things, you might complain "OMG what is this crazy new symbol '3'!? We haven't defined the naturals yet!". In this case, you should merely interpret X^3 as short-hand for $X \times X \times X$. Similar comments apply throughout this appendix.

Definition A.2.3.20 — Disjoint-union Let X and Y be sets. Then, the ***disjoint-union*** of X and Y, $X \sqcup Y$, is

$$\begin{aligned} X \sqcup Y := \{\langle a, m\rangle : m \in \{0, 1\}, \\ a \in X \text{ if } m = 0,\ a \in Y \text{ if } m = 1\} . \end{aligned} \tag{A.2.3.21}$$

R Intuitively, this is supposed to be a copy of X together with a copy of Y. a can come from either set, and the 0 or 1 tells us which set a is supposed to come from. Thus, we think of $X \subseteq X \sqcup Y$ as $X = \{\langle a, 0\rangle : a \in X\}$ and $Y \subseteq X \sqcup Y$ as $Y \{\langle a, 1\rangle : a \in Y\}$.

The key difference between the union and disjoint-union is that, in the case of the union of A and B, an element that x is both in A and in B is a *single* element in $A \cup B$, whereas in the disjoint-union there will be two copies of it: one in A and one in B. Hopefully the next example will help clarify this.

▪ **Example A.2.3.22 — Union vs. disjoint-union** Define $A := \{a, b, c\}$ and $B := \{c, d, e, f\}$. Then, $A \cup B = \{a, b, c, d, e, f\}$. On the other hand, $A \sqcup B = \{a, b, c_A, c_B, d, e, f\}$, where $A \sqcup B \supseteq A = \{a, b, c_A\}$ and $A \sqcup B \supseteq B = \{c_B, d, e, f\}$.

Definition A.2.3.23 — Power set Let X be a set. Then, the ***power set*** of X, 2^X, is the set of all subsets of X,

$$2^X := \{A : A \subseteq X\}. \tag{A.2.3.24}$$

R We will discuss the motivation for this notation in the next subsection (see Exercise A.3.31).

A.3 Relations, functions, and orders

Having defined Cartesian products, we can now make the following definition.

Definition A.3.1 — Relation A *relation* between two sets X and Y is a subset R of $X \times Y$.

R For a given relation R, we write $x \sim_R y$, or just $x \sim y$ if R is clear from context, iff $\langle x, y \rangle \in R$. Often we will simply refer to the relation by the symbol $\sim$ instead of R.

R It is important to be able to understand how to translate between the two different notations for

writing a relation. In one direction, if you know $R \subseteq X \times Y$, then $x \sim y$ iff $\langle x, y\rangle \in R$, as already mentioned. In the other direction, if you know $\sim$, then $R = \{\langle x, y\rangle \in X \times Y : x \sim y\}$.

R If $X = Y$, we will say that $\sim$ is a relation *on* X.

Definition A.3.2 — Composition Let X, Y, and Z be sets, and let R be a relation on X and Y, and let S be a relation on Y and Z. Then, the ***composition***, $S \circ R$, of R and S is the relation on X and Z defined by

$$S \circ R := \{\langle x, z\rangle \in X \times Z : \exists y \in Y \text{ such that } \langle x, y\rangle \in R \text{ and } \langle y, z\rangle \in S.\}\,. \tag{A.3.3}$$

R If R is a relation on X (so that $R \circ R$ makes sense), for $k \in \mathbb{N}$, we shall abbreviate $R^k := \underbrace{R \circ \cdots \circ R}_{k}$, with $R^0 := \{\langle x, x\rangle \in X \times X : x \in X\}$.[a]

R You will see in the next definition that a function is in fact just a very special type of relation, in which case, this composition is exactly the composition that you (hopefully) know and love.

[a] R^0 is of course the identity function on X—see Example A.3.12.

Exercise A.3.4 Let R, S, and T be relations between X and Y, Y and Z, and Z and W respectively. Show that

$$(T \circ S) \circ R = T \circ (S \circ R). \tag{A.3.5}$$

While the appropriate generality in which to make the next definitions of restriction and corestriction is for arbitrary relations, the intuition you should use to understand the concepts will almost

certainly come from your understanding of functions (and we will have little to no need to make use of these concepts in this amount of generality), so feel free to first read the definition of a function (Definition A.3.9) and related concepts and then come back to this if at first this seems confusing.

Definition A.3.6 — Restriction and corestriction Let f be a relation between two sets X and Y, let $S \subseteq X$, and let $T \subseteq Y$. Then, the ***restriction*** of f to S, $f|_S$, is a relation between S and Y defined by

$$f|_S := f \circ \{\langle s, x\rangle \in S \times X : s = x\} .^a \tag{A.3.7}$$

The ***corestriction*** of f to T, $f|^T$, is a relation between X and T defined by

$$f|^T := \{\langle y, t\rangle \in Y \times T : y = t\} \circ f .^b \tag{A.3.8}$$

If $g = f|_S$, then we will also say that f ***extends*** g. If $g = f|^T$, then we will also say that f ***coextends*** g.

R As mentioned before, to understand this, it probably helps to think of what these concepts mean in the case that the relation is in fact a function (note that a function is just a special type of relation—see Definition A.3.9). For example, if we have the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) := x^2$, then we can obtain a new function $f|_{(-1,1)} : (-1, 1) \to \mathbb{R}$ by restricting to $(-1, 1) \subseteq \mathbb{R}$, and that new function is still given by the same 'rule', $f(x) := x^2$—the only thing that has changed is the domain.[c]

Corestriction, on the other hand, is when we change the codomain of the relation. For example, we can corestrict this same function to $\mathbb{R}_0^+$ to obtain the function $f|^{\mathbb{R}_0^+} : \mathbb{R} \to \mathbb{R}_0^+$, once again, still with the 'rule' $f(x) := x^2$.[d]

R These concepts will almost always arise in the case where the relation f is in fact a function. One reason we state the definitions in this more general case, besides just to be more general, is that *the*

corestriction of a function is not always going to be a new function. For example, if we again define $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) := x^2$, $f|^{(-1,1)}$ is a relation that is no longer a function—the reason is that, for example, $\langle 2, y\rangle \notin f|^{(-1,1)}$ for any $y \in (-1, 1)$. This is easy, but quite subtle, and not super important, so don't worry if this doesn't make sense to you at the moment. In fact, the corestriction of a function to $T \subseteq Y$ is another function iff T is contained in the image of f.

[a]Here, $\{\langle s, x\rangle \in S \times X : s = x\}$ is of course to be interpreted as a relation between S and X.

[b]Similarly as before, $\{\langle y, t\rangle \in Y \times T : y = t\}$ is to be interpreted as a relation between Y and T.

[c]I realize we are making use of notation we have not yet technically. This is not a problem from a mathematical perspective as I am only trying to explain. From a pedagogical perspective, hopefully I'm not making use of anything unfamiliar to you—if so, flip ahead.

[d]The term "corestriction" is incredibly uncommon, as one often simply changes the codomain of the function without explicitly mentioning so. This is technically sloppy, but almost never actually causes problems. Still, it is important to realize that functions with different codomains are always different functions.

There are several different important types of relations. Perhaps the most important is the notion of a function.

Definition A.3.9 — Function A ***function*** from a set X to a set Y is a relation $\sim_f$ that has the property that for each $x \in X$ there is exactly one $y \in Y$ such that $x \sim_f y$. For a given function $\sim_f$, we denote by $f(x)$ that unique element of Y such that $x \sim_f f(x)$. X is the ***domain*** of f and Y is the ***codomain*** of f. The notation $f\colon X \to Y$ means "f is a function from X to Y.". The set of all functions from X to Y is denoted Y^X.

R The motivation for this notation is that, if X and Y are finite sets, then the cardinality of the set of all functions from X to Y is $|Y|^{|X|}$.

R The arrow "$\mapsto$" can be used to define a function with necessarily giving it a name. For example, one can

write

$$\mathbb{R} \ni x \mapsto 3x^2 - 5 \in \mathbb{R} \tag{A.3.10}$$

as notation for the function $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) \coloneqq 3x^2 - 5$. Of course, this is convenient if it is unnecessary to give a specific name.

R The "x" in "$f(x)$" is sometimes referred to as the ***argument*** of the function.

Notation A.3.11 — Placeholders for arguments Let f be a function. A lot of the time, if we want to refer to f, we just say, well, "f". Besides this, however, we also frequently write "$f(x)$". Strictly speaking, this is incorrect—the function itself is $x \mapsto f(x)$, whereas $f(x)$ is the value of the function f at x in the domain. In practice, however, it is very common to write "$f(x)$" to denote the function itself, and not just a particular value.

We may also use the symbols "$\cdot$" or "$-$" to indicate the argument of a function. For example, we might denote a function using the notation $\langle \cdot, \cdot \rangle\colon V \times V \to \mathbb{K}$ or $\langle -, - \rangle\colon V \times V \to \mathbb{K}$. This notation means that "$\langle \cdot, \cdot \rangle$" is the name of a function, and furthermore, we denote its value at the element $\langle v_1, v_2 \rangle \in V \times V$ as "$\langle v_1, v_2 \rangle$". Thus, the dots tell you where to 'plug in' the variables. Similarly for "$-$".

▪ **Example A.3.12 — Identity function** For every set X, there is a function, $\mathrm{id}_X : X \to X$, the ***identity function***, defined by

$$\mathrm{id}_X(x) \coloneqq x. \tag{A.3.13}$$

Definition A.3.14 — Inverse function Let $f\colon X \to Y$ and $g\colon Y \to X$ be functions. Then, g is a ***left-inverse*** of f iff

$g \circ f = \mathrm{id}_X$; g is a ***right-inverse*** of f iff $f \circ g = \mathrm{id}_Y$; g is a ***two-sided-inverse***, or just ***inverse***, iff g is both a left- and right-inverse of f.

Exercise A.3.15 Let g and h be two (two-sided)-inverses of f. Show that $g = h$.

Because of the uniqueness of two-sided-inverses, we may write f^{-1} for the unique two-sided-inverse of f.

Exercise A.3.16 Provide examples to show that left-inverses and right-inverses need not be unique.

Exercise A.3.17 Let X be a nonempty set.

(i). Explain why there is *no* function $f : X \to \emptyset$.
(ii). Explain why there is *exactly one* function $f : \emptyset \to X$.
(iii). How many functions are there $f : \emptyset \to \emptyset$?

Definition A.3.18 — Image Let $f : X \to Y$ be a function and let $S \subseteq X$. Then, the ***image*** of S under f, $f(S)$, is

$$f(S) := \{f(x) : x \in S\}. \tag{A.3.19}$$

The ***range*** of f, $f(X)$, is the image of X under f.

R We may also write $\mathrm{Im}(f) := f(X)$ for the range of f. If we simply say "image of f", you should interpret this to mean "image of X under f", i.e., the range $f(X)$.

R Note the difference between range and codomain. For example, consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) := x^2$. Then, the codomain is $\mathbb{R}$ but the range is just $[0, \infty)$. In fact the range and codomain are the same precisely when f is surjective (see Exercise A.3.24.(ii)).

Definition A.3.20 — Preimage Let $f : X \to Y$ be a function and let $T \subseteq Y$. Then, the ***preimage*** of T under f, $f^{-1}(T)$, is

$$f^{-1}(T) := \{x \in X : f(x) \in T\}. \tag{A.3.21}$$

Exercise A.3.22 Let $f : X \to Y$ be a function and let $T \subseteq Y$. Show that $f^{-1}(T^{\mathsf{C}}) = f^{-1}(T)^{\mathsf{C}}$. For $S \subseteq X$, find examples to show that we need not have either $f(S^{\mathsf{C}}) \subseteq f(S)^{\mathsf{C}}$ nor $f(S)^{\mathsf{C}} \subseteq f(S^{\mathsf{C}})$.

Definition A.3.23 — Injectivity, surjectivity, and bijectivity Let $f : X \to Y$ be a function. Then,

(i). (Injective) f is ***injective*** iff for every $y \in Y$ there is at most one $x \in X$ such that $f(x) = y$.
(ii). (Surjective) f is ***surjective*** iff for every $y \in Y$ there is at least one $x \in X$ such that $f(x) = y$.
(iii). (Bijective) f is ***bijective*** iff for every $y \in Y$ there is exactly one $x \in X$ such that $f(x) = y$.

R It follows immediately from the definitions that a function $f : X \to Y$ is bijective iff it is both injective and surjective.

Exercise A.3.24 Let $f : X \to Y$ be a function.

(i). Show that f is injective iff whenever $f(x_1) = f(x_2)$ it follows that $x_1 = x_2$.
(ii). Show that f is surjective iff $f(X) = Y$.

▪ **Example A.3.25 — The domain and codomain matter** Consider the 'function' $f(x) := x^2$. Is this 'function' injective or surjective? Defining functions like this may have been kosher back when you were doing mathematics that wasn't actually mathematics, but no longer. The question does not

make sense because you have not specified the domain or codomain. For example, $f\colon \mathbb{R} \to \mathbb{R}$ is neither injective nor surjective, $f\colon \mathbb{R}_0^+ \to \mathbb{R}$ is injective but not surjective, $f\colon \mathbb{R} \to \mathbb{R}_0^+$ is surjective but not injective, and $f\colon \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is both injective and surjective. Hopefully this example serves to illustrate: functions are not (just) 'rules'—if you have not specified the domain and codomain, then *you have not specified the function*.

Exercise A.3.26 Let $f\colon X \to Y$ be a function between nonempty sets. Show that

(i). f is injective iff it has a left inverse;
(ii). f is surjective iff it has a right inverse; and
(iii). f is bijective iff it has a (two-sided) inverse.

R By Exercise A.3.17.(ii), there *is* exactly one function from $\emptyset$ to $\{\emptyset\}$. This function is definitely injective as every element in the codomain has *at most one* preimage. On the other hand, there is *no* function from $\{\emptyset\}$ to $\emptyset$ (by Exercise A.3.17.(i)), and so certainly no left-inverse to the function from $\emptyset$ to $\{\emptyset\}$. This is why we require the sets to be nonempty.

Exercise A.3.27 Let $f\colon X \to Y$ be a function, and let $\mathscr{S}$ and $\mathscr{T}$ be a collection of subsets of X and Y respectively. Show that the following statements are true.

(i). $f^{-1}\left(\bigcup_{T\in\mathscr{T}} T\right) = \bigcup_{T\in\mathscr{T}} f^{-1}(T)$.
(ii). $f^{-1}\left(\bigcap_{T\in\mathscr{T}} T\right) = \bigcap_{T\in\mathscr{T}} f^{-1}(T)$.
(iii). $f\left(\bigcup_{S\in\mathscr{S}} S\right) = \bigcup_{S\in\mathscr{S}} f(S)$
(iv). $f\left(\bigcap_{S\in\mathscr{S}} S\right) \subseteq \bigcap_{S\in\mathscr{S}} f(S)$.

Find an example to show that we need not have equality in (iv). On the other hand, show that (iv) is true if f is injective.

Exercise A.3.28 Show that

(i). the composition of two injections is an injection;
(ii). the composition of two surjections is a surjection; and
(iii). the composition of two bijections is a bijection.

Exercise A.3.29 Let $f : X \to Y$ be a function, let $S \subseteq X$, and let $T \subseteq Y$. Show that the following statements are true.

(i). $f\left(f^{-1}(T)\right) \subseteq T$, with equality for all T iff f is surjective.
(ii). $f^{-1}\left(f(S)\right) \supseteq S$, with equality for all S iff f is injective.

Find examples to show that we need not have equality in general.

R Maybe this is a bit silly, but I remember which one is which as follows. First of all, write these both using $\subseteq$, not $\supseteq$, that is, $S \subseteq f^{-1}(f(S))$ and $f(f^{-1}(S)) \subseteq S$. Then, the "-1" is always closest to the symbol that represents being 'smaller' (that is "$\subseteq$"). It is easy to remember which conditions imply equality if you remember that surjective functions have right-inverses and injective functions have left-inverse.[a]

[a] Modulo the stupid case when the domain is the empty-set—see the remark in Equation (A.3.26).

Exercise A.3.30 Let X and Y be sets, and let $x_0 \in X$ and $y_0 \in Y$. If there is some bijection from X to Y, show that in fact there is a bijection from X to Y which sends x_0 to y_0.

Exercise A.3.31 Let X be a set. Construct a bijection from 2^X, the power set of X, to $\{0,1\}^X$, the set of functions from X into $\{0,1\}$.

R This is the motivation for the notation 2^X to denote the power set.

A.3.1 Arbitrary disjoint-unions and products

Definition A.3.1.1 — Disjoint-union (of a collection) Let $\mathscr{X}$ be an indexed collection[a] of sets. Then, the ***disjoint-union*** over all $X \in \mathscr{X}$, $\coprod_{X\in\mathscr{X}} X$, is

$$\coprod_{X\in\mathscr{X}} X := \{\langle x, X\rangle : X \in \mathscr{X}\ x \in X\}. \tag{A.3.1.2}$$

R The intuition and way to think of notation is just the same as it was in the simpler case of the disjoint-union of two sets (Definition A.2.3.20).

[a] By ***indexed collection*** we mean a set in which elements are allowed to be repeated. So, for example, $\mathscr{X}$ is allowed to contain two copies of $\mathbb{N}$. The reason for the term "*indexed* collection" is that indices are often used to distinguish between the two identical copies, e.g., $\mathscr{Y} = \{\mathbb{N}_1, \mathbb{N}_2\}$—as sets are not allowed to 'repeat' elements, we add the indices so that, strictly speaking, $\mathbb{N}_1 \neq \mathbb{N}_2$ as elements of $\mathscr{X}$, even though they represent the same set. (If this is confusing, don't think about it too hard—it's just a set where elements are allowed to be repeated.)

Definition A.3.1.3 — Restrictions (of functions on a disjoint-union) Let $\mathscr{X}$ be an indexed collection of sets, let Y be a set, and let $f\colon \coprod_{X\in\mathscr{X}} X \to Y$ be a function. Then, the ***restriction of*** f ***to*** X, $f|_X : X \to Y$, is defined by

$$f|_X(x) := f(\langle x, X\rangle). \tag{A.3.1.4}$$

In particular, the ***inclusion*** is defined to be

$$\iota_X := [\mathrm{id}_{\coprod_{X\in\mathscr{X}}}]\big|_X, \tag{A.3.1.5}$$

that is, the restriction of the identity $\mathrm{id}_{\coprod_{X\in\mathscr{X}} X} : \coprod_{X\in\mathscr{X}} X \to \coprod_{X\in\mathscr{X}} X$.

R While from a set-theoretic perspective, this is just a special case of restriction (see Definition A.3.6), we state it separately because we wish to draw an

analogy with projections (see Definition A.3.1.9), a concept which is not a special case of something we have seen before.

Definition A.3.1.6 — Cartesian-product (of a collection) Let $\mathscr{X}$ be an indexed collection of sets. Then, the ***Cartesian-product*** over all $X \in \mathscr{X}$, $\prod_{X\in\mathscr{X}} X$, is

$$\prod_{X\in\mathscr{X}} X := \left\{ f : \mathscr{X} \to \coprod_{X\in\mathscr{X}} X : f(X) \in X \right\}. \quad \text{(A.3.1.7)}$$

R Admittedly this notation is a bit obtuse. The cartesian-product is still supposed to be thought of a collection of ordered-'pairs', except now the pairs aren't just pairs, but can be 3, 4, or even infinitely many 'coordinates'. The coordinates are indexed by elements of $\mathscr{X}$, and the X-coordinate for $X \in \mathscr{X}$ must lie in X itself. Thus, for example, $X_1 \times X_2 = \prod_{X\in\mathscr{X}} X$ for $\mathscr{X} = \{X_1, X_2\}$. The key that is probably potentially the most confusing is that the elements of $\mathscr{X}$ are playing more than one role: on one hand, they index the coordinates, and on the other hand, they are the set in which the coordinates take their values. Hopefully keeping in mind the case $\mathscr{X} = \{X_1, X_2\}$ helps this make sense. So, for example, in the statement "$f(X) \in X$", on the left-hand side, X is being thought of as an 'index', and on the right-hand side it is being thought of as the 'space' in which a coordinate 'lives'. This is thus literally just the statement that the X-coordinate of $f \in \prod_{X\in\mathscr{X}} X$ must be an element of the set X.

R For $x \in \prod_{X\in\mathscr{X}} X$, we write $x_X := x(X)$ for the ***X-component*** or ***X-coordinate***.

R For $x \in \mathscr{I}$, we may also suggestively write

$$\langle x_i : i \in \mathscr{I} \langle := x, \quad \text{(A.3.1.8)}$$

analogous to how one writes $\langle x, y\rangle \in X \times Y$ for elements in a Cartesian product of two sets. (We have only changed the letter of our indexing set[a] for legibility.)

R For a function defined on a Cartesian product, say $f\colon X \times Y \to Z$, we shall write $f(x, y) \coloneqq f(\langle x, y\rangle)$.

[a] Like the term "collection", the term ***indexing set*** is technically just synonymous with the word "set". There is nothing mathematically different about it. This term is only used to clarify to the human readers out there how one should intuitively think of the set, specifically that it is a set whose elements are being used to "index" other things.

Definition A.3.1.9 — Components (of functions into a product) Let $\mathscr{X}$ be an indexed collection of sets, let Y be a set, and let $f\colon Y \to \prod_{X\in\mathscr{X}} X$ be a function. Then, the ***X*-component**, $f_X : Y \to X$, is defined by

$$f_X(y) \coloneqq f(y)_X. \tag{A.3.1.10}$$

In particular, the ***projection***, π_X, is defined to be

$$\pi_X \coloneqq [\mathrm{id}_{\prod_{X\in\mathscr{X}} X}]_X, \tag{A.3.1.11}$$

that is, it is the X-component of the identity $\mathrm{id}_{\prod_{X\in\mathscr{X}} X} : \prod_{X\in\mathscr{X}} X \to \prod_{X\in\mathscr{X}} X$.

R For example, in the case $f\colon Y \to X_1 \times X_2$, then $f(y) = \langle f_1(y), f_2(y)\rangle$.

Exercise A.3.1.12 Let $\mathscr{I}$ and X be sets.

(i). Find a bijection

$$\mathscr{I} \times X \to \coprod_{i\in\mathscr{I}} X. \tag{A.3.1.13}$$

(ii). Find a bijection

$$X^{\mathscr{I}} \to \prod_{i \in \mathscr{I}} X. \tag{A.3.1.14}$$

R (i) says that if all the sets appearing in a disjoint-union are the same, then that disjoint-union is 'the same as' the Cartesian product of the indexing set and the single set appearing in the disjoint union.

Similarly, (ii) says that if all the sets appearing in are Cartesian-product are the same, then it is 'the same as' the set of all functions from the indexing set to the single set appearing in the product.

Before introducing other important special cases of relations, we must first introduce several properties of relations.

Definition A.3.1.15 Let $\sim$ be a relation on a set X.

(i). (Reflexive) $\sim$ is ***reflexive*** iff $x \sim x$ for all $x \in X$.
(ii). (Symmetric) $\sim$ is ***symmetric*** iff $x_1 \sim x_2$ is equivalent to $x_2 \sim x_1$ for all $x_1, x_2 \in X$.
(iii). (Transitive) $\sim$ is ***transitive*** iff $x_1 \sim x_2$ and $x_2 \sim x_3$ implies $x_1 \sim x_3$.
(iv). (Antisymmetric) $\sim$ is ***antisymmetric*** iff $x_1 \sim x_2$ and $x_2 \sim x_1$ implies $x_1 = x_2$.[a]
(v). (Total) $\sim$ is ***total*** iff for every $x_1, x_2 \in X$, $x_1 \sim x_2$ or $x_2 \sim x_1$.

[a] Admittedly the terminology here with "symmetric" and "antisymmetric" is a bit unfortunate.

A.3.2 Equivalence relations

Definition A.3.2.1 — Equivalence relation An ***equivalence relation*** on a set X is a relation on X that is reflexive, symmetric, and transitive.

▪ **Example A.3.2.2 — Integers modulo m** Let $m \in \mathbb{Z}^+$ and let $x, y \in \mathbb{Z}$. Then, x and y are ***congruent modulo*** m, written $x \cong y \pmod{m}$, iff $x - y$ is divisible by m.

Exercise A.3.2.3 Check that $\cong \pmod{m}$ is an equivalence relation.

For example, 3 and 10 are congruent modulo 7, 1 and -3 are congruent modulo 4, -2 and 6 are congruent modulo 8, etc..

R We will see a 'better' way of viewing the integers modulo m in Example A.4.1.17. It is better in the sense that it is much more elegant and concise, but requires a bit of machinery and will probably not be as transparent if you have never seen it before. Thus, it is probably more enlightening, at least the first time, to see things spelled out in explicit detail.

Definition A.3.2.4 — Equivalence class Let $\sim$ be an equivalence relation on a set X and let $x_0 \in X$. Then, the ***equivalence class*** of x_0, $[x_0]_\sim$, is

$$[x_0]_\sim := \{x \in X : x \sim x_0\} = \{x \in X : x_0 \sim x\}\,. \quad \text{(A.3.2.5)}$$

R If $\sim$ is clear from context, we may simply write $[x_0] := [x_0]_\sim$.

R We may also on occasion write $x_0/\sim := [x_0]_\sim$ for the equivalence class.

R In words, the equivalence class of x_0 is the set of elements equivalent to x.

R Note that the second equation of (A.3.2.5) uses the symmetry of the relation.

▪ **Example A.3.2.6 — Integers modulo m** This is a continuation of Example A.3.2.2. For example, the equivalence class of 5 modulo 6 is

$$[5]_{\cong (\mathrm{mod}\ 6)} = \{\ldots, -1, 5, 11, 17, \ldots\}, \tag{A.3.2.7}$$

the equivalence class of -1 modulo 8 is

$$[1]_{\cong (\mathrm{mod}\ 8)} = \{\ldots, -17, -9, -1, 7, 15, \ldots\}, \tag{A.3.2.8}$$

etc..

An incredibly important property of equivalence classes is that they form a partition of the set.

Definition A.3.2.9 — Partition Let X be a set. Then, a ***partition*** of X is a collection $\mathscr{X}$ of subsets of X such that

(i). $X = \bigcup_{U \in \mathscr{X}} U$; and
(ii). for $U_1, U_2 \in \mathscr{X}$ either $U_1 = U_2$ or U_1 is disjoint from U_2.

Proposition A.3.2.10 Let $\sim$ be an equivalence relation on a set X and let $x_1, x_2 \in X$. Then, either (i) $x_1 \sim x_2$ or (ii) $[x_1]_\sim$ is disjoint from $[x_2]_\sim$.

Proof. If $x_1 \sim x_2$ we are done, so suppose that this is not the case. We wish to show that $[x_1]_\sim$ is disjoint from $[x_2]_\sim$, so suppose that this is not the case. Then, there is some $x_3 \in X$ with $x_1 \sim x_3$ and $x_3 \sim x_2$. Then, by transitivity $x_1 \sim x_2$: a

contradiction. Thus, it must be the case that $[x_1]_\sim$ is disjoint from $[x_2]_\sim$. ■

Corollary A.3.2.11 Let X be a set and let $\sim$ be an equivalence relation on X. Then, the collection $\mathscr{X} := \{[x]_\sim : x \in X\}$ is a partition of X.

Proof. The previous proposition, Proposition A.3.2.10, tells us that $\mathscr{X}$ has property (ii) of the definition of a partition, Definition A.3.2.9. Property (i) follows from the fact that $x \in [x]_\sim$, so that indeed

$$X = \bigcup_{x \in X} [x]_\sim = \bigcup_{U \in \mathscr{X}} U. \tag{A.3.2.12}$$

■

Conversely, a partition of a set defines an equivalence relation.

Exercise A.3.2.13 Let X be a set, let $\mathscr{X}$ be a partition of X, and define $x_1 \sim x_2$ iff there is some $U \in \mathscr{X}$ such that $x_1, x_2 \in U$. Show that $\sim$ is an equivalence relation.

▪ **Example A.3.2.14 — Integers modulo m** This in turn is a continuation of Example A.3.2.6. The equivalence classes modulo 4 are

$$\begin{aligned} [0]_{\cong (\mathrm{mod}\ 4)} &= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\ [1]_{\cong (\mathrm{mod}\ 4)} &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\ [2]_{\cong (\mathrm{mod}\ 4)} &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\ [3]_{\cong (\mathrm{mod}\ 4)} &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}\,. \end{aligned} \tag{A.3.2.15}$$

You can verify directly that (i) each integer appears in at least one of these equivalence classes and (ii) that no integer appears in more than one. Thus, indeed, the set $\left\{[0]_{\cong (\mathrm{mod}\ 4)}, [1]_{\cong (\mathrm{mod}\ 4)}, [2]_{\cong (\mathrm{mod}\ 4)}, [3]_{\cong (\mathrm{mod}\ 4)}\right\}$ is a partition of $\mathbb{Z}$.

Given a set X with an equivalence relation $\sim$, we obtain a new set $X/\sim$, the collection of all equivalence classes of elements in X with respect to $\sim$.

Definition A.3.2.16 — Quotient set Let $\sim$ be an equivalence relation on a set X. Then, the ***quotient of X with respect to $\sim$***, $X/\sim$, is defined by

$$X/\sim := \{[x]_\sim : x \in X\}\,. \tag{A.3.2.17}$$

The function $\mathrm{q} : X \to X/\sim$ defined by $\mathrm{q}(x) := [x]_\sim$ is the ***quotient function***.

R If one wants to define a function f on $X/\sim$, often times one will define $f([x]_\sim)$ in terms of x itself. This is dubious, however, as how do we know that our definition gives the same result if $x_1 \sim x_2$? (We can't have $f([x_1]_\sim) \neq f([x_2]_\sim)$ if $[x_1]_\sim = [x_2]_\sim$, now can we?) Thus, if ever we do want to make a definition like this we must first prove that our definition does not depend on the "representative" of the equivalence class $[x]_\sim$ we have chosen. More precisely, we must show that if $x_1 \sim x_2$, then $f(x_1) = f(x_2)$. If this is the case, we say that our definition f is ***well-defined***. (We elaborate on this below.)

Of course the quotient function is surjective. What's perhaps a bit more surprising is that *every* surjective function can be viewed as the quotient function with respect to some equivalence relation.

Exercise A.3.2.18 Let $\mathrm{q} : X \to Y$ be surjective and for $x_1, x_2 \in X$, define $x_1 \sim_\mathrm{q} x_2$ iff $x_1, x_2 \in \mathrm{q}^{-1}(y)$ for some $y \in Y$. Show that (i) $\sim_\mathrm{q}$ is an equivalence relation on X and (ii) that $\mathrm{q}(x) = [x]_{\sim_\mathrm{q}}$.

▪ **Example A.3.2.19 — Integers modulo m** This in turn is a continuation of Example A.3.2.14. For example, the quotient

set mod 5 is

$$\begin{aligned}&\mathbb{Z}/\cong \pmod 5\\ &= \left\{[0]_{\cong \pmod 5}, [1]_{\cong \pmod 5}, [2]_{\cong \pmod 5},\right.\\ &\qquad\left. [3]_{\cong \pmod 5}, [4]_{\cong \pmod 5}\right\}.\end{aligned} \tag{A.3.2.20}$$

It is quite common for us, after having defined the quotient set, to want to define operations on the quotient set itself. For example, we would like to be able to add integers modulo 24 (we do this when telling time). In this example, we could make the following definition.

$$[x]_{\cong \pmod{24}} + [y]_{\cong \pmod{24}} := [x+y]_{\cong \pmod{24}}. \tag{A.3.2.21}$$

This is okay, but before we proceed, we have to check that this definition is *well-defined*. That is, there is a potential problem here, and we have to check that this potential problem doesn't actually happen. I will try to explain what the potential problem is.

Suppose we want to add 3 and 5 modulo 7. On one hand, we could just do the obvious thing $3+5=8$. But because we are working with *equivalence classes*, I should just as well be able to add 10 and 5 and get the same answer. In this case, I get $10+5=15$. At first glance, it might seem we got different answers, but, alas, while 8 and 15 are not the same integer, they 'are' the same *equivalence class* modulo 7.

In symbols, if I take two integers x_1 and x_2 and add them, and you take two integers y_1 and y_2 *with* y_1 *equivalent to* x_1 *and* y_2 *equivalent to* x_2, it had better be the case that x_1+x_2 is equivalent to y_1+y_2. That is, the answer should not depend on the "representative" of the equivalence class we chose to do the addition with.

▪ **Example A.3.2.22 — Integers modulo m** This in turn is a continuation of Example A.3.2.19. Let $m \in \mathbb{Z}^+$, let $x_1, x_2 \in \mathbb{Z}$, and define

$$[x_1]_{\cong \pmod m} + [x_2]_{\cong \pmod m} := [x_1+x_2]_{\cong \pmod m}. \tag{A.3.2.23}$$

We check that this is well-defined. Suppose that $y_1 \cong x_1 \pmod m$ and $y_2 \cong x_2 \pmod m$. We must show that $x_1 + x_2 \cong$

$y_1 + y_2 \pmod{m}$. Because $y_k \cong x_k \pmod{m}$, we know that $y_k - x_k$ is divisible by m, and hence $(y_1 - x_1) + (y_2 - x_2) = (y_1 + y_2) - (x_1 + x_2)$ is divisible by m. But this is just the statement that $x_1 + x_2 \cong y_1 + y_2 \pmod{m}$, exactly what we wanted to prove.

Exercise A.3.2.24 Define multiplication modulo m and show that is is well-defined.

A.3.3 Preorders

Definition A.3.3.1 — Preorder A ***preorder*** on a set X is a relation $\leq$ on X that is reflexive and transitive. A set equipped with a preorder is a ***preordered set***.

R The notation $x_1 < x_2$ is shorthand for "$x_1 \leq x_2$ and $x_1 \neq x_2$".

R Note that an equivalence relation is just a very special type of preorder.

Exercise A.3.3.2 Find an example of

(i). a relation that is both reflexive and transitive (i.e. a preorder);
(ii). a relation that is reflexive but not transitive;
(iii). a relation that is not reflexive but transitive; and
(iv). a relation that is neither reflexive nor transitive.

The notion of an *interval* is obviously important in mathematics and you almost have certainly encountered them before in calculus. We give here the abstract definition (it of course turns out that this agrees with the definition you are familiar in case $X = \mathbb{R}$ with the usual order).

Definition A.3.3.3 — Interval Let $\langle X, \leq \rangle$ be a preordered set and let $I \subseteq X$. Then, I is an ***interval*** iff for all $x_1, x_2 \in I$ with $x_1 \leq x_2$, whenever $x_1 \leq x \leq x_2$, it follows that $x \in I$.

R In other words, I is an interval iff everything in-between two elements of I is also in I.

R As you are probably aware, the following notation is common.

$$[x_1, x_2] \coloneqq \{x \in X : x_1 \leq x \leq x_2\}$$
$$(x_1, x_2) \coloneqq \{x \in X : x_1 < x < x_2\}$$
$$[x_1, x_2) \coloneqq \{x \in X : x_1 \leq x < x_2\}$$
$$(x_1, x_2] \coloneqq \{x \in X : x_1 < x \leq x_2\}.$$

The first and second are called respectively ***closed intervals*** and ***open intervals***. Terminology for the third and fourth is less common, but you might call them respectively the ***half-closed-open intervals*** and ***half-open-closed intervals***.

Feel free to check that these sets are all in fact intervals.[a]

[a] Warning: Though there can be intervals not of this form—for example, $\{x \in \mathbb{Q} : 0 \leq x \leq \sqrt{2}\}$ is not of this form.

Definition A.3.3.5 — Monotone Let X and Y be preordered sets and let $f : X \to Y$ be a function. Then, f is ***nondecreasing*** iff $x_1 \leq x_2$ implies that $f(x_1) \leq f(x_2)$. If the second inequality is strict for distinct x_1 and x_2, i.e. if $x_1 < x_2$ implies $f(x_1) < f(x_2)$, then f is ***increasing***. If the inequality is in the other direction, i.e. if $x_1 \leq x_2$ implies $f(x_1) \geq f(x_2)$, then f is ***nonincreasing***. If it is both strict and reversed, i.e. if $x_1 < x_2$ implies $f(x_1) > f(x_2)$, then f is ***decreasing***. f is ***monotone*** iff it is either nondecreasing or nonincreasing and f is ***strictly monotone*** iff it is either increasing or decreasing.

R Note that the $\leq$ that appears in $x_1 \leq x_2$ is *different* than the $\leq$ that appears in $f(x_1) \leq f(x_2)$: the former is the preorder on X and the latter is the preorder on Y. We will often abuse notation in this manner.

In this course, we will almost always be dealing with preordered sets whose preorder is in addition antisymmetric (or are equivalence relations).

Definition A.3.3.6 — Partial-order A ***partial-order*** is an antisymmetric preorder. A set equipped with a partial-order is a ***partially-ordered set*** or a ***poset***.

There are two preorders that you can define on any set. They are not terribly useful, except perhaps for producing counter-examples.

▪ **Example A.3.3.7 — Discrete and indiscrete (orders** Let X be a set. Declare $x_1 \leq_D x_2$ iff $x_1 = x_2$. That is, $x \leq_D x$ is true, and nothing else.

Exercise A.3.3.8 Show that $\langle X, \leq_D \rangle$ is a partial-order.

R $\leq_D$ is the ***discrete-order*** on X.

Now declare $x_1 \leq_I x_2$ for all $x_1, x_2 \in X$. That is, $x_1 \leq_I x_2$ is *always* true.

Exercise A.3.3.9 Show that $\langle X, \leq_I \rangle$ is a total preorder that is not antisymmetric in general.

R In particular, this shows that there are total preorders which are not partial-orders (Definition A.3.3.6).

R $\leq_I$ is the ***indiscrete-order*** on X.

A much more useful collection of examples of partially-ordered sets is that are those exhibited as power-sets.

▪ **Example A.3.3.10 — Power set** The archetypal example of a partially-ordered set is given by the power set. Let X be a set and for $U, V \in 2^X$, define $U \leq V$ iff $U \subseteq V$.

Exercise A.3.3.11 Check that $\langle 2^X, \leq \rangle$ is in fact a partially-ordered set.

Exercise A.3.3.12 What is an example of a preorder that is not a partial-order?

While we will certainly be dealing with nontotal partially-ordered sets, totality of an ordering is another property we will commonly come across.

Definition A.3.3.13 — Total-order A ***total-order*** is a total partial-order. A set equipped with a total-order is a ***totally-ordered set***.

Exercise A.3.3.14 What is an example of a partially-ordered set that is not a totally-ordered set.

And finally we come to the notion of well-ordering, which is an incredibly important property of the natural numbers.

Definition A.3.3.15 — Well-order A ***well-order*** on a set X is a total-order that has the property that every nonempty subset of X has a smallest element. A set equipped with a well-order is a ***well-ordered set***.

In fact, we do not need to assume a priori that the order is a total-order. This follows simply from the fact that every nonempty subset has a smallest element.

Proposition A.3.3.16 Let X be a partially-ordered set that has the property that every nonempty subset of X has a smallest element. Then, X is totally-ordered (and hence well-ordered).

Proof. Let $x_1, x_2 \in X$. Then, the set $\{x_1, x_2\}$ has a smallest element. If this element is x_1, then $x_1 \preceq x_2$. If this element is x_2, then $x_2 \preceq x_1$. Thus, the order is total, and so X is totally-ordered. ■

Exercise A.3.3.17 What is an example of a totally-ordered set that is not a well-ordered set?

A.3.4 Well-founded induction

In the very beginning of this chapter when discussing proof techniques (Appendix A.2.2), we mentioned *well-founded induction*. It is time we return to this and make the statement precise.

Definition A.3.4.1 — Well-founded Let X be a set and let $\preceq$ be a relation on X. Then, $\langle X, \preceq \rangle$ is ***well-founded*** iff every nonempty subset of X has a minimal element.

The relationship between being well-ordered and well-founded is as follows.

Proposition A.3.4.2 Let X be a set and let $\preceq$ be a relation on X. Then, $\langle X, \preceq \rangle$ is a well-ordered set iff $\preceq$ is a well-founded total-order.

Proof. ($\Rightarrow$) Suppose that $\langle X, \preceq \rangle$ is a well-ordered set. Then, $\preceq$ is well-founded because minima are minimal. Let $x_1, x_2 \in X$. Then, $\{x_1, x_2\}$ is nonempty, and so has a minimum, say x_1. Then, $x_1 \preceq x_2$, and so $\preceq$ is total.

($\Leftarrow$) Suppose that $\preceq$ is a well-founded total-order. Let $S \subseteq X$ be nonempty. Then, S has a minimal element $s_0 \in S$. We wish

to show that s_0 is a minimum of S. So, let $s \in S$. We wish to show that $s_0 \preceq s$. By totality, either $s_0 \preceq s$ or $s \preceq s_0$. In the former case, we are done. In the latter case, by minimality, we have $s = s_0$. By reflexivity (total-orders are reflexive), this would imply $s_0 \preceq s$, and we are done. ■

We are ultimately interested in well-foundedness itself because of its relevance to the most powerful form of induction (I know of).

Theorem A.3.4.3 — Well-founded Induction. Let X be a set, let $\preceq$ be a well-founded relation on X, and let $\mathcal{P}: X \to \{0, 1\}$. Then, if $\mathcal{P}(y) = 1$ for all $y \preceq x$, $y \neq x$, implies that $\mathcal{P}(x) = 1$, it follows that $\mathcal{P}(x) = 1$ for all $x \in X$.

R Of course, we are thinking of $\mathcal{P}(x)$ as a statement that may or may not be true for a given x, and $\mathcal{P}(x) = 1$ corresponds to it being true and $\mathcal{P}(x) = 0$ corresponds to it being false.

R Note how this gives us 'normal' induction in case $X := \mathbb{N}$ and $\preceq := \leq$. Indeed, it similarly generalizes transfinite induction (whatever that is).

Proof. Suppose that $\mathcal{P}(y) = 1$ for all $y \preceq x$, $y \neq x$, implies that $\mathcal{P}(x) = 1$. Define $S := \{x \in X : \mathcal{P}(x) = 0\}$. We wish to show that S is empty. We proceed by contradiction: suppose that S is nonempty. Then, S has a minimal element $s_0 \in S$. Let $y \in X$ be such that $y \preceq s_0$ and $y \neq s_0$. If $y \in S$, then by minimality, we would have $y = s_0$, which is not the case. Thus, $y \notin S$, and hence $\mathcal{P}(y) = 1$. Thus, by hypotheses, $\mathcal{P}(s) = 1$: a contradiction. ■

A.3.5 Zorn's Lemma

We end this subsection with an incredibly important result known as *Zorn's Lemma*. At the moment, it's importance might not seem obvious, and perhaps one must see it in action in order to appreciate its significance. For the time being at least, let me say this: if ever

you are trying to produce something maximal by adding things to a set one-by-one (e.g. if you are trying to construct a basis by picking linearly-independent vectors one-by-one), but you are running into trouble because, somehow, this process will never stop, not even if you 'go on forever': give Zorn's Lemma a try.

Definition A.3.5.1 — Upper-bound and lower-bound Let $\langle X, \leq \rangle$ be a preordered set, let $S \subseteq X$, and let $x \in X$. Then, x is an ***upper-bound*** iff $s \leq x$ for all $s \in S$. x is a ***lower-bound*** iff $x \leq s$ for all $s \in S$.

Definition A.3.5.2 — Maximum and minimum Let $\langle X, \leq \rangle$ be a preordered set and let $x \in X$. Then, x is a ***maximum*** of X iff x is an upper-bound of all of X. x is a ***minimum*** of X iff x is a lower-bound of all of X.

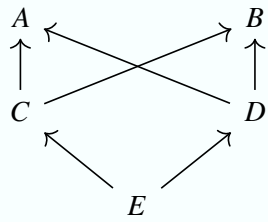
Definition A.3.5.3 — Maximal and minimal Let $\langle X, \leq \rangle$ be a preordered set, let $S \subseteq X$, and let $x \in S$. Then, x is ***maximal*** in S iff whenever $y \in S$ and $y \geq x$, it follows that $x = y$. x is ***minimal*** in S iff whenever $y \in S$ and $y \leq x$ it follows that $x = y$.

R In other words, maximal means that there is no element in S strictly greater than x (and similarly for minimal). Contrast this with maxi*mum* and mini*mum*: if x is a maximum of S it means that $y \leq x$ for all $y \in S$ (and analogously for minimum).

R Note that, in a *partially*-ordered set anyways, maximum elements are always maximal (see Exercise A.3.5.6, but not conversely (and similarly for minimum and minimal) (see Example A.3.5.4).

▪ **Example A.3.5.4 — Maximum vs. maximal** To understand the difference between maximal and maximum, consider

the following diagram.[a]



(A.3.5.5)

Then, A and B are both *maximal*, because nothing is strictly larger than them. On the other hand, neither of them are *maximum* (and in fact, there is no maximum), because neither of them is larger than everything (A is not larger than B and B is not larger than A). Of course, the difference between minimal and minimum is exactly analogous.

[a] This diagram is meant to define a poset in which $E \leq C, E \leq D, C \leq A$, $C \leq B$, $D \leq A$, and $D \leq B$ (of course, these aren't the only relations—for example, we also mean to imply that $C \leq C$, that $E \leq A$, etc.).

Exercise A.3.5.6 Let X be a *partially*-ordered set and let $S \subseteq X$.

(i). Show that every maximum of S is maximal in S.
(ii). Show that S has at most one maximum element.
(iii). Come up with an example of X and S where S has two distinct maximal elements.

Definition A.3.5.7 — Downward-closed and upward-closed Let X be a preordered set and let $S \subseteq X$. Then, S is ***downward-closed*** in X iff whenever $x \leq s \in S$ it follows that $x \in S$. S is ***upward-closed*** in X iff whenever $x \geq s \in S$ it follows that $x \in S$.

Proposition A.3.5.8 Let X be a well-ordered set and let $S \subset X$ be downward-closed in X. Then, there is some $s_0 \in X$ such that $S = \{x \in X : x < s_0\}$.

Proof. As S is a proper subset of X, S^{C} is nonempty. As X is well-ordered, it follows that S^{C} has a smallest element s_0. We claim that $S = \{x \in X : x < s_0\}$. First of all, let $x \in X$ and suppose that $x < s_0$. If it were *not* the case that $x \in S$, then s_0 would no longer be the smallest element in S^{C}. Hence, we must have that $x \in S$. Conversely, let $x \in S$. By totality, either $x \leq s_0$ or $s_0 \leq x$. As $x \in S$ and $s_0 \in S^{\mathsf{C}}$, we cannot have that $x = s_0$, so in fact, in the former case, we would have $x < s_0$, and we are done, so it suffices to show that $s_0 \leq x$ cannot happen. If $s_0 \leq x$, then because S is downward-closed in X and $x \in S$, it would follows that $s_0 \in S$: a contradiction. Therefore, it cannot be the case that $s_0 \leq x$. ∎

Theorem A.3.5.9 — Zorn's Lemma. Let X be a partially-ordered set. Then, if every well-ordered subset has an upper-bound, then X has a maximal element.

Proof. [a] STEP 1: MAKE HYPOTHESES

Suppose that every well-ordered subset has an upper bound. We proceed by contradiction: suppose that X has no maximal element.

STEP 2: SHOW THAT EVERY WELL-ORDERED SUBSET HAS AN UPPER-BOUND *NOT* CONTAINED IN IT

Let $S \subseteq X$ be a well-ordered subset, and let u be some upper-bound of S. If there were no element in X strictly greater than u, then u would be a maximal element of X. Thus, there is some $u' > u$. It cannot be the case that $u' \in S$ because then we would have $u' \leq u$ because u is an upper-bound of S. But then the fact that $u' \leq u$ and $u \leq u'$ would imply that $u = u'$: a

contradiction. Thus, $u' \notin S$, and so constitutes an upper-bound not contained in S.

STEP 3: DEFINE $u(S)$
For each well-ordered subset $S \subseteq X$, denote by $u(S)$ some upper-bound of S not contained in S.

STEP 4: DEFINE THE NOTION OF A u-SET
We will say that a well-ordered subset $S \subseteq X$ is a u-set iff $x_0 = u(\{x \in S : x < x_0\})$ for all $x_0 \in S$.

STEP 5: SHOW THAT FOR u-SETS S AND T, EITHER S IS DOWNWARD-CLOSED IN S OR T IS DOWNWARD CLOSED IN S
Define

$$D := \bigcup_{\substack{A \subseteq X \\ A \text{ is downward-closed in } S \\ A \text{ is downward-closed in } T}} A. \tag{A.3.5.10}$$

That is, D is the union of all sets that are downward-closed in both S and T.

We first check that D itself is downward-closed in both S and T. Let $d \in D$, let $s \in S$, and suppose that $s \leq d$. As $d \in D$, it follows that $d \in A$ for some $A \subseteq X$ downward-closed in both S and T. As A is in particular downward-closed in S, it follows that $s \in D$, and so D is downward-closed in S. Similarly it is downward-closed in T.

If $D = S$, then $S = D$ is downward-closed in T, and we are done. Likewise if $D = T$. Thus, we may as well assume that D is a proper subset of both S and T. Then, by Proposition A.3.5.8, there are $s_0 \in S$ and $t_0 \in T$ such that $\{s \in S : s < s_0\} = D = \{t \in T : t < t_0\}$. Because S and T are u-sets, it follows that

$$s_0 = u(\{s \in S : s < s_0\}) = u(\{t \in T : t < t_0\}) = t_0.$$

Define $D \cup \{s_0\} =: D' := D \cup \{t_0\}$. Let $d \in D'$, let $s \in S$, and suppose that $s \leq d$. Either $d = s_0$ or $d \in D$. In the latter case, $d < s_0$. Either way, $d \leq s_0$, and so we have that $s \leq d \leq s_0$, and so either $s = s_0$ or $s < s_0$; either way, $s \in D'$. The conclusion is that D' is downward-closed in S. It is similarly downward-closed in T. By the definition of D, we must have that $D' \subseteq D$: a contradiction. Thus, it could not have been the case that D was a proper subset of both S and T.

STEP 6: DEFINE U

Define

$$U := \bigcup_{\substack{S \subseteq X \\ S \text{ is a } u\text{-set}}} S. \tag{A.3.5.11}$$

We show that U is a u-set in the next step. Here, we argue that this is sufficient to complete the proof.

Define $U' := U \cup \{u(U)\}$. We wish to check that U' is likewise a u-set. First note that U' is still a well-ordered subset of X. Now let $x_0 \in U'$. We wish to show that $x_0 = u(\{x \in U' : x < x_0\})$. Note that $\{x \in U' : x < x_0\} = \{x \in U : x < x_0\}$. Hence, because U is a u-set, $u(\{x \in U' : x < x_0\}) = x_0$, as desired.

Thus, as U' is a u-set, from the definition of U, we will have $U' \subseteq U$: a contradiction, which will complete the proof. Thus, it does indeed suffice to show that U is a u-set.

STEP 7: FINISH THE PROOF BY SHOWING THAT U IS A u-SET

We first need to check that U is well-ordered. Let $A \subseteq U$ be nonempty. For $S \subseteq X$ a u-set, define $A_S := A \cap S$. For each A_S that is nonempty, denote by a_S the smallest element in A_S (which exists as S is in particular well-ordered). Let $T \subseteq X$ be some other u-set. Then, by Step 5, without loss of generality, S is downward-closed in T. In particular, $S \subseteq T$ so that $a_S \in T$. Hence, $a_T \leq a_S$. Then, because S is downward-closed in T,

$a_T \in S$, and hence $a_T \leq a_S$, and hence $a_T = a_S$. We claim that this unique element is a smallest element of A.

To see this, let $a \in A$. a is then in particular an element of U, and there is some u-set S such that $a \in S$. Then, $a \in A_S \coloneqq A \cap A$, and hence $a_S \leq a$.

Let $u_0 \in U$. All that remains to be shown is that $u_0 = u(\{x \in U : x < u_0\})$. To do this, we first show that every u-set is downward-closed in U.

Let $S \subseteq X$ be a u-set, let $s \in S$, let $x \in U$, and suppose that $x \leq s$. As $x \in U$, there is some u-set T such that $x \in T$. Then, by Step 5 again, either S is downward-closed in T or T is downward-closed in S. If the former case, then we have that $x \in S$ because $x \leq s$. On the other hand, in the latter case, we have that $x \in S$ because $x \in T \subseteq S$.

Now we finally return to showing that $u_0 = u(\{x \in U : x < u_0\})$. By definition of U, $u_0 \in S$ for some u-set S, and therefore, $u_0 = u(\{x \in S : x < u_0\})$. Therefore, it suffices to show that if $x \in U$ is less than u_0, then it is in S (because then $\{x \in S : x < u_0\} = \{x \in U : x < u_0\}$) u. This, however, follows from the fact that S is downward-closed in U. ■

[a] Proof adapted from [Gra07].

A.4 Sets with algebraic structure

Definition A.4.1 — Binary operation A *binary operation* $\cdot$ on a set X is a function $\cdot : X \times X \to X$. It is customary to write $x_1 \cdot x_2 \coloneqq \cdot(x_1, x_2)$ for binary operations.

R Sometimes people say that *closure* is an axiom. This is not necessary. That a binary operation on X takes values *in* X implicitly says that the operation is closed. That doesn't mean that you never have to check closure, however. For example, in order to verify that the even integers $2\mathbb{Z}$ are a subrng (see Definition A.4.13) of $\mathbb{Z}$, you do have to check

closure—you need to check this in order that $+ : 2\mathbb{Z} \times 2\mathbb{Z} \to 2\mathbb{Z}$ be a binary operation on $2\mathbb{Z}$ (and similarly for $\cdot$).

Definition A.4.2 Let $\cdot$ be a binary relation on a set X.

(i). (Associative) $\cdot$ is ***associative*** iff $(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3)$ for all $x_1, x_2, x_3 \in X$.

(ii). (Commutative) $\cdot$ is ***commutative*** if $x_1 \cdot x_2 = x_2 \cdot x_1$ for all $x_1, x_2 \in X$.

(iii). (Identity) An ***identity*** of $\cdot$ is an element $1 \in X$ such that $1 \cdot x = x = x \cdot 1$ for all $x \in X$.

(iv). (Inverse) If $\cdot$ has an identity and $x \in X$, then an ***inverse*** of x is an element $x^{-1} \in X$ such that $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.

We first consider sets equipped just a single binary operation.

Definition A.4.3 — Magma A ***magma*** is a set equipped with a binary operation.

Exercise A.4.4 Let $\langle X, \cdot \rangle$ be a magma and let $x_1, x_2, x_3 \in X$. Show that $x_1 = x_2$ implies $x_1 \cdot x_3 = x_2 \cdot x_3$.

R My hint is that the solution is so trivial that it is easy to overlook.

R This is what justifies the 'trick' (if you can call it that) of doing the same thing to both sides of an equation that is so common in algebra.

R Note that the converse is not true in general. That is, we can have $x_1 \cdot x_2 = x_1 \cdot x_3$ with $x_2 \neq x_3$.

Definition A.4.5 — Semigroup A ***semigroup*** is a magma $\langle X, \cdot \rangle$ such that $\cdot$ is associative.

Definition A.4.6 — Monoid A ***monoid*** $\langle X, \cdot, 1\rangle$ is a semigroup $\langle X, \cdot\rangle$ equipped with an identity $1 \in X$.

Exercise A.4.7 — Identities are unique Let X be a monoid and let $1, 1' \in X$ be such that $1 \cdot x = x = x \cdot 1$ and $1' \cdot x = x = x \cdot 1'$ for all $x \in X$. Show that $1 = 1'$.

Definition A.4.8 — Group A ***group*** is a monoid $\langle X, \cdot, 1\rangle$ equipped with a function $-^{-1} : X \to X$ so that x^{-1} is an inverse of x for all $x \in X$.

R Usually this is just stated as "X has inverses.". This isn't wrong, but this way of thinking about things doesn't generalize to universal algebra or category theory quite as well. The way to think about this is that, inverses, like the binary operation (as well as the identity) is *additional structure*. This is in contrast to the axiom of associativity which should be thought of as a *property* satisfied by an *already existing* structure (the binary operation).

R Usually we write $\langle X, \cdot, 1, -^{-1}\rangle$ to denote a group X with binary operation $\cdot$ with identity 1 and with the inverse of $x \in X$ being given by x^{-1}. However, especially if the group is commutative, it is also common to write $\langle X, +, 0, -\rangle$ to denote the same thing. In this case, what we previously would have written as x^3, would now be written as $3x$. It is important to realize that, even though the symbols being used are different, the axioms they are required to satisfy are exactly the same—the change in notation serves no other purpose other than to be suggestive.

Exercise A.4.9 — Inverses are unique Let X be a group, let $x \in X$, and let $y, z \in X$ both be inverses of x. Show that $y = z$.

Exercise A.4.10 Let $\langle X, \cdot, 1, -^{-1} \rangle$ be a group and let $x_1, x_2, x_3 \in X$. Show that if $x_1 \cdot x_2 = x_1 \cdot x_3$, then $x_2 = x_3$.

R Thus, the converse to Exercise A.4.4 holds in the case of a group.

Definition A.4.11 — Homomorphism (of magmas) Let X and Y be magmas and let $f : X \to Y$ be a function. Then, f is a ***homomorphism*** iff $f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2)$ for all $x_1, x_2 \in X$.

R Informally, we say that "f *preserves*" the binary operation.

R Note that, once again, the $\cdot$ in $f(x_1 \cdot x_2)$ is *not* the same as the $\cdot$ in $f(x_1) \cdot f(x_2)$. Confer the remark following the definition of a nondecreasing function, Definition A.3.3.5.

R There are similar definitions for monoids and groups, with extra conditions because of the extra structure. For monoids,[a] we additionally require that $\phi(1) = 1$. For groups, in turn additionally require that $\phi(x^{-1}) = \phi(x)^{-1}$. This is why we might say "homomorphism of monoids" instead of just "homomorphism"—we are clarifying that we are additionally requiring this extra condition.

[a] And more generally any magma with identity.

We now move on to the study of sets equipped with *two* binary operations.

Definition A.4.12 — Rg A ***rg*** is a set equipped with two binary operations $\langle X, +, \cdot \rangle$ such that

(i). $\langle X, + \rangle$ is a commutative monoid,
(ii). $\langle X, \cdot \rangle$ is a semigroup, and

(iii). $\cdot$ ***distributes*** over $+$, that is, $x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3$ and $(x_1 + x_2) \cdot x_3 = x_1 \cdot x_3 + x_2 \cdot x_3$ for all $x_1, x_2, x_3 \in X$.

R In other words, writing out what it means for $\langle X, + \rangle$ to be a commutative monoid and for $\langle X, \cdot \rangle$ to be a a semigroup, these three properties are equivalent to

(i). $+$ is associative,
(ii). $+$ is commutative,
(iii). $+$ has an identity,
(iv). $\cdot$ is associative,
(v). $\cdot$ distributes over $+$.

R For $x \in X$ and $m \in \mathbb{Z}^+$, we write $m \cdot x := \underbrace{x + \cdots + x}_{m}$.

Note that we do *not* make this definition for $m = 0 \in \mathbb{N}$. An empty-sum is *always* 0 (by definition), but $0 \cdot x$ need not be 0 in a general rg.

R Whenever we say that a rg is commutative, we mean that the *multiplication* is commutative (this should be obvious—addition is always commutative). Instead of saying referring to things as "commutative rgs" etc. we will often shorten this to "crg" etc..

As commutativity is such a nice property to have, elements which commute with everything have a special name: $x \in X$ is ***central*** iff $x \cdot y = y \cdot x$ for all $y \in X$.

R I have actually never seen the term rg used before. That being said, I haven't seen *any* term to describe such an algebraic object before. Nevertheless, I have seen both the terms rig and rng before (see below), and, well, given those terms, "rg" is pretty much the only reasonable term to give to such an algebraic object. We don't have a need to work with rgs directly, but we will work with both rigs and rngs, and so it is nice to have an object of which both rigs and rngs are special cases.

Definition A.4.13 — Rng A ***rng*** is a rg such that $\langle X, +, 0, - \rangle$ is a commutative group, that is, a rg that has additive inverses.

Exercise A.4.14 Let $\langle X, +, 0-, \cdot \rangle$ be a rng and let $x_1, x_2 \in X$. Prove the following properties.

(i). $0 \cdot x_1 = 0$ for all $x_1 \in X$.
(ii). $(-x_1) \cdot x_2 = -(x_1 \cdot x_2)$ for all $x_1, x_2 \in X$.

▪ **Example A.4.15 — A rg that is not a rng** The even natural numbers $2\mathbb{N}$ with their usual addition and multiplication is also an example of a rg that is not a rng.

Definition A.4.16 — Rig A ***rig*** is a rg such that $\langle X, \cdot, 1 \rangle$ is a monoid, that is, a rg that has a multiplicative identity.

R In a rig R, we write

$$R^\times := \{r \in R : r \text{ has a multiplicative inverse.}\}. \quad \text{(A.4.17)}$$

$R^\times$ is a group with respect to the ring multiplication and is known as the ***group of units*** in R.

R Just as the empty sum is defined to be 0 in a rg (see the remark in Definition A.4.12), the empty product is defined to be 1 in a rig.[a]

R I believe it is more common to refer to rigs as *semirings*. I dislike this terminology because it suggests an analogy with semigroups, of which there is none. The term rig is also arguably more descriptive—even if you didn't know what the term meant, you might have a good chance of guessing, especially if you had seen the term rng before.

[a] Of course, similar conventions apply for all types of algebraic objects (in particular, for monoids), but we shall not keep repeating this.

Definition A.4.18 — Characteristic Let $\langle X, +, 0, \cdot, 1\rangle$ be a rig. Then, either (i) there is some $m \in \mathbb{Z}^+$ such that $m \cdot 1 = 0 \in X$ or (ii) there is no such m. In the former case, the smallest positive integer such that $\underbrace{1 + \cdots + 1}_{m} = 0 \in X$ is the ***characteristic***, and in the latter case the ***characteristic*** is 0. We denote the characteristic by $\mathrm{Char}(X)$.

R For example, the characteristic of $\mathbb{Z}/m\mathbb{Z}$ is m, whereas the characteristic of $\mathbb{Z}$ is 0.

▪ **Example A.4.19 — A rg that is not a rig** The even natural numbers $2\mathbb{N}$ with their usual addition and multiplication is a rg that is not a rig.

Definition A.4.20 — Ring A ***ring*** is a rg that is both a rig and a rng.

R The motivation for the terminology is as follows. Historically, the term "ring" was the first to be used. It is not uncommon for authors to use the term ring to mean both our definition and our definition minus the requirement of having a multiplicative identity. To remove this ambiguity in terminology, we take the term "ring" to imply the existence of the identity and the removal of the "i" from the word is the term used for objects which do not necessarily have an identity. Similarly, thinking of the "n" in "ring" as standing for "negatives", a rig is just a ring that does not necessarily posses additive inverses.

R Note that it follows from Exercise A.4.14 that $-1 \cdot x = -x$ for all $x \in X$, X a ring.

Exercise A.4.21 Let X be a ring and suppose that $0 = 1$. Show that $X = \{0\}$.

R This is called the ***zero cring***.

Definition A.4.22 — Integral A rg $\langle X, +, 0, \cdot \rangle$ is ***integral*** iff it has the property that, whenever $x \cdot y = 0$, it follows that either $x = 0$ or $y = 0$.

R Usually the adjective "integral" is applied only to crings, in which case people refer to this as an ***integral domain*** instead of an integral cring. As the natural numbers have this property (i.e. $xy = 0 \Rightarrow x = 0$ or $y = 0$) I wanted an adjective that would describe rgs with this property and "integral" was an obvious choice because of common use of the term "integral domain".[a] It is then just more systematic to refer to them as integral crings instead of integral domains. This is usually not an issue because it is not very common to work with rigs or rgs.

[a] The adjective "integral" itself also appears in the context of schemes, and the usage there is consistent with the usage here (in a sense that will be obvious on the off-chance you know what a scheme is).

Definition A.4.23 — Division ring A ***division ring*** is a ring $\langle X, +, 0, -\cdot, 1 \rangle$ such that $\langle X \setminus \{0\}, \cdot, 1, -^{-1} \rangle$ is a group.

R In other words, a division ring is a ring in which every nonzero element has a multiplicative inverse.

R This condition makes just as much sense for rigs as it does for rings, however, to the best of my knowledge there is no accepted term for rigs in which every nonzero element has a multiplicative inverse (and as we shall have no need for such objects, we refrain from introducing a term ourselves).

R Sometimes people use the term ***skew-field*** instead of division ring.

Exercise A.4.24 Show that all division rings are integral.

Definition A.4.25 — Field A ***field*** is a commutative division ring.

Exercise A.4.26 Let F be a field with positive characteristic p. Show that p is prime.

Given any rg R, we can define another rg, the *opposite ring* of R, whose elements are the same but whose multiplication is in the 'opposite' order. Of course, this construction returns the same thing if R is commutative, but not in general. We don't elaborate too much on this because we don't make use of the construction very much, so you needn't worry if you don't immediate see it's use—remember, this appendix is primarily supposed to serve as a reference, to look definitions and facts up as you need them, not as a tool for learning per se.

Definition A.4.27 — Opposite rg Let X be a rg. Then, the ***opposite rg*** of X, $\langle X^{\mathrm{op}}, +^{\mathrm{op}}, 0^{\mathrm{op}}, -^{\mathrm{op}}, \cdot^{\mathrm{op}} \rangle$, is defined by

(I). $X^{\mathrm{op}} := X$;
(II). $x +^{\mathrm{op}} y := x + y$;
(III). $0^{\mathrm{op}} := 0$;
(IV). $-^{\mathrm{op}} x := -x$; and
(V). $x \cdot^{\mathrm{op}} y := y \cdot x$.

R In other words, everything is the same except for the multiplication, with the new multiplication being defined to be the old multiplication in the "opposite" order.

R Of course, if X is a rig, X^{op} is canonically a rig, and similarly for rngs and rings.

R Obviously, if X is commutative, then $X = X^{\mathrm{op}}$ (as rgs, not just sets).

Definition A.4.28 — Homomorphism (of rgs) Let $\langle X, +, \cdot \rangle$ and $\langle Y, +, \cdot \rangle$ be rgs and let $f : X \to Y$ be a function. Then, f is a ***homomorphism*** iff f is both a homomorphism (of magmas) from $\langle X, + \rangle$ to $\langle Y, + \rangle$ and from $\langle X, \cdot \rangle$ to $\langle Y, \cdot \rangle$.

R Explicitly, this means that

$$f(x + y) = f(x) + f(y), f(0) = 0 \quad \text{(A.4.29)}$$

and

$$f(xy) = f(x)f(y). \quad \text{(A.4.30)}$$

R Similarly as in the definition of monoid homomorphisms Definition A.4.11, we add corresponding extra conditions about preserving identities and inverses for rigs, rngs, and rings.[a]

[a] But *not* fields. This is why the definitions are stated in such a way that the additive inverses for rings are regarded as *structure*, whereas the multiplicative inverses for fields are regarded as *properties*—homomorphisms should preserve all "structure". This is a subtle and, for now, unimportant point, and so if this doesn't make sense, you can ignore it for the time being.

A.4.1 Quotient groups and quotient rngs

It is probably worth noting that this subsubsection is of relatively low priority. We present this information here essentially because it gives a more unified, systematic, sophisticated, and elegant way to view things presented in other places in the notes, but it is also not really strictly required to understand these examples.

If you have never seen quotient rngs before, it may help to keep in the back of your mind a concrete example as you work through the definitions. We recommend you keep in mind the example $R := \mathbb{Z}$ and $I := m\mathbb{Z}$ (all multiplies of m) for some $m \in \mathbb{Z}^+$. In this case, the quotient R/I is (supposed to be, and in fact will turn-out to be) the integers modulo m. While this is a quotient rng, it is also of course a quotient group (just forget about the multiplication), so this example may also help you think about quotient groups as well.

Before we get started with the precise mathematics, let's talk about the intuition.[28] At a naive level, if you ask yourself "How does one obtain $\mathbb{Z}/m\mathbb{Z}$ from $\mathbb{Z}$?", while I suppose you might come up with other answers, the 'correct' one is that "You obtain $\mathbb{Z}/m\mathbb{Z}$ from $\mathbb{Z}$ by 'setting $m = 0$'.". The intuition and motivation for quotient rings is *how to make precise the intuition of 'setting things equal to zero'*.

For reasons of 'consistency', you'll see that you can't *just* set $m = 0$. If you set $m = 0$, you must also set $m + m = 2m = 0$, and so on. Thus, if you want to set $m = 0$, in fact you must set all multiples of m equal to zero. In general, the sets of objects which are you 'allowed' to set equal to zero at once are called *ideals*. Thus, $\{m\}$ itself is not an ideal because it would be 'inconsistent' to only set $m = 0$. Instead, you take the 'ideal generated by m', which turns out to be $m\mathbb{Z}$, and set all elements of $m\mathbb{Z}$ equal to zero. If R is a rng and $I \subseteq R$ is an ideal, then R/I is the notation we use to represent the rng obtained from R by 'setting' every element of I equal to 0.

As we shall use quotient groups to define quotient rngs, we do them first. The first thing to notice is that every subgroup of a group induces an equivalence relation.

Proposition A.4.1.1 — Cosets (in groups) Let G be a group, let $H \subseteq G$, and define

$$g_1 \cong g_2 \,(\mathrm{mod}\, H) \text{ iff } g_2^{-1} g_1 \in H \text{ for } g_1, g_2 \in G. \quad \text{(A.4.1.2)}$$

Then, $\cong \pmod H$ is an equivalence relation iff H is a subgroup of G.

Furthermore, in the case this is an equivalence relation,

$$[g]_{\cong \,(\mathrm{mod}\, H)} = gH. \quad \text{(A.4.1.3)}$$

R To clarify, $[g]_{\cong \,(\mathrm{mod}\, H)}$ is the equivalence class of g with respect to $\cong \pmod H$ and $gH := \{gh : h \in H\}$.

[28] I think it's fair to say that quotient algebraic structures are among the most difficult things students encounter when first beginning algebra, and so it is worthwhile to take some extra time to step back and think about what one is actually trying to accomplish.

R The equivalence class of g with respect $\cong \pmod{H}$ is the ***left H-coset***. The set of all left H-cosets is denoted by $G/H := G/{\sim_{\cong \pmod{H}}} = \{gH : g \in G\}$.

R By changing the definition of the equivalent relation to "... iff $g_1 g_2^{-1} \in H$", then we obtain the corresponding definition of ***right H-cosets***, given explicitly by Hg. The set of all right H-cosets is denoted by $H\backslash G$.[a] Of course, in general if the binary operation is not commutative, then $gH \neq Hg$.

[a] This notation is technically ambiguous with the notation used for relative set complementation, however, in practice there will never be any confusion. Furthermore, if you pay extra special attention to the spacing, this uses the symbol \ `backslash` where set complementation uses the symbol \\.

Proof. ($\Rightarrow$) Suppose that $\cong \pmod{H}$ is an equivalence relation. Let $g_1, g_2 \in S$. As $g_i \cong g_i \pmod{H}$, we have that $g_i^{-1} g_i = 1 \in H$. Then, $1^{-1} g_i = g_i \in H$, and so $g_i \cong 1 \pmod{H}$. By symmetry, $1 \cong g_i \pmod{S}$, and so $g_i^{-1} 1 = g_i^{-1} \in H$. We then have that $g_1 \cong 1 \pmod{H}$ and $1 \cong g_2 \pmod{H}$, and hence, $g_1 \cong g_2 \pmod{H}$, and hence $g_2^{-1} g_1 \in H$. Thus, H is indeed a subgroup of G.

($\Leftarrow$) Suppose that H is a subgroup of G. Then, $1 \in H$, and so $g^{-1} g = 1 \in H$, and so $g \cong g \pmod{H}$. That is, $\cong \pmod{H}$ is reflexive. If $g_1 \cong g_2 \pmod{S}$, then $g_2^{-1} g_1 \in H$, then $g_1^{-1} g_2 = (g_2^{-1} g_1)^{-1} \in H^{-1} = H$, and so $g_2 \cong g_1 \pmod{H}$. Thus, $\cong \pmod{S}$ is symmetric. If $g_1 \cong g_2 \pmod{S}$ and $g_2 \cong g_3 \pmod{H}$, then $g_2^{-1} g_1, g_3^{-1} g_2 \in H$, and so $g_3^{-1} g_1 = (g_3^{-1} g_2)(g_2^{-1} g_1) \in HH \subseteq H$, and so $g_1 \cong g_3 \pmod{H}$. Thus, $\cong \pmod{H}$ is transitive, hence an equivalence relation.

We now prove the "Furthermore..." part. Certainly, as $(gh)^{-1} g = h^{-1} g^{-1} g = h^{-1} \in H$, $g \cong gh \pmod{H}$ for all $h \in$

H. On the other hand, if $g_1 \cong g_2 \pmod{H}$, then $g_2^{-1}g_1 \in H$, and so $g_2^{-1}g_1 = h$ for some $h \in H$, so that $g_1 = g_2 h$. Thus, $[g]_{\cong \pmod{H}} = gH$. ■

For a subgroup H of G, G/H will always be a set. However, in good cases, it will be more than just a set—it will be a group in its own right.

Definition A.4.1.4 — Ideals and quotient groups Let G be a group, let $H \subseteq G$ be a subgroup, and let $g_1, g_2 \in G$. Define

$$(g_1 H) \cdot (g_2 H) \coloneqq (g_1 g_2) H. \tag{A.4.1.5}$$

H is an ***ideal*** iff this is well-defined on the quotient set G/H. In this case, G/H is itself a group, the ***quotient group*** of G modulo H.

R Recall that (Proposition A.4.1.1) gH is the equivalent class of g modulo H, and so, in particular, these definitions involve picking representatives of equivalence classes. Thus, in order for these operations to make sense, they must be well-defined. In general, they will not be well-defined, and we call H an *ideal* precisely in the 'good' case where these operations make sense.

R In the spirit of Proposition A.4.1.1, you should really be thinking of H as a *subset* that has the property that $\cong \pmod{H}$ (defined by (A.4.1.2)) is an equivalence relation. Of course, this is perfectly equivalent to being a subgroup, but that's not the reason we care—we care because it gives us an equivalence relation. This distinction will be more important for rings.

R In the context of groups, it is *much* more common to refer to ideals as ***normal subgroups***. As always, we choose the terminology we do because it is more universally consistent, even if less common.

There is an easy condition to check that in order to determine whether a given subgroup is in fact an ideal that does not require checking the well-definedness directly.

Exercise A.4.1.6 Let G be a group and let $H \subseteq G$ be a subset. Show that H is an ideal iff (i) it is a subgroup and (ii) $gHg^{-1} \subseteq H$ for all $g \in G$.

And now we turn to quotient rngs, whose development is completely analogous.

Proposition A.4.1.7 — Cosets (in rngs) Let R be a group, let $S \subseteq R$, and define

$$r_1 \cong r_2 \,(\mathrm{mod}\, S) \text{ iff } -r_2 + r_1 \in S \text{ for } r_1, r_2 \in R. \quad \text{(A.4.1.8)}$$

Then, $\cong \,(\mathrm{mod}\, S)$ is an equivalence relation iff S is a subgroup of $\langle R, +, 0, - \rangle$.

Furthermore, in the case this is an equivalence relation,

$$[r]_{\cong\,(\mathrm{mod}\ S)} = r + S. \quad \text{(A.4.1.9)}$$

R To clarify, $[r]_{\cong\,(\mathrm{mod}\ S)}$ is the equivalence class of r with respect to $\cong \,(\mathrm{mod} S)$ and $r + S := \{r + s : s \in S\}$.

R The equivalence class of r with respect $\cong \,(\mathrm{mod} S)$ is the ***left S-coset***. The set of all left S-cosets is denoted by $R/S := R/{\sim_{\cong\,(\mathrm{mod}\ S)}} = \{r + S : r \in R\}$.

R By changing the definition of the equivalent relation to "... iff $r_1 - r_2 \in S$", then we obtain the corresponding definition of ***right S-cosets***, given explicitly by $S + r$. In this case, however, the binary operation in question $(+)$ is commutative, and so $r + S = S + r$, that is, the left and right cosets coincide, and so we can simply say ***coset***. In particular, there is no need to talk about the set of right S-cosets, which would have been denoted $S\backslash R$.

Proof. We leave this as an exercise.

Exercise A.4.1.10 Prove this yourself.

R Hint: Use the proof of Proposition A.4.1.1 as a guide.

■

You can check that $m\mathbb{Z}$ is indeed a subrng of $\mathbb{Z}$ and that $\mathbb{Z}/m\mathbb{Z}$ consists of just m cosets:

$$0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}, \tag{A.4.1.11}$$

though you are probably more familiar just writing this as

$$0 \,(\mathrm{mod} m), 1 \,(\mathrm{mod} m), \ldots, m-1 \,(\mathrm{mod} m). \tag{A.4.1.12}$$

Of course, however, $\mathbb{Z}/m\mathbb{Z}$ is more than just a set, it has a ring structure of its own, and in good cases, R/S will obtain a canonical ring structure of its own as well.

Definition A.4.1.13 — Ideals and quotient rngs Let R be a rng, let $S \subseteq \langle R, +, 0, - \rangle$ be a subgroup, and let $r_1, r_2 \in R$. Define

$$(r_1 + S) + (r_2 + S) \coloneqq (r_1 + r_2) + S \tag{A.4.1.14}$$

and

$$(r_1 + S) \cdot (r_2 + S) \coloneqq (r_1 \cdot r_2) + S. \tag{A.4.1.15}$$

S is an ***ideal*** iff both of these operations are well-defined. In this case, R/S is the ***quotient rng*** of R modulo S.

R I mentioned in a remark of the definition of quotient groups Definition A.4.1.4 that you should really be thinking of the condition there that "$H \subseteq G$ a subgroup" as the condition that $\cong \pmod{H}$ be well-defined. This shows its relevance here as, in

the spirit of Proposition A.4.1.7, the appropriate condition is *not* "$S \subseteq R$ a subrng" but instead that "$S \subseteq \langle R, 0, +, - \rangle$ be a subgroup". This is particularly important if you're working with rings, as in this case, the 'correct' definition of subring requires that subrings include 1, however, if an ideal I contains 1, then $I = R$.[a] Thus, if you write "$S \subseteq R$ a subring" instead of "$S \subseteq \langle R, +, 0, - \rangle$ a subgroup", your definition would imply that the only ideal in R is R itself![b]

[a] Because, by the absorption property, $r = r \cdot 1 \in I$ for all $r \in R$.

[b] In case it's not obvious, that would constitute a particularly shitty definition.

Just as before, we have an easy way of checking whether a given subring is in fact an ideal.

Exercise A.4.1.16 Let R be a rng and let $S \subseteq R$ be a subset. Show that S is an ideal iff (i) it is a subrng and (ii) $r \in R$ and $s \in S$ implies that $r \cdot s, s \cdot r \in S$.

R The second property is sometimes called "absorbing", because elements in the ideal 'absorb' things into the ideal when you multiply them.

▪ **Example A.4.1.17 — Integers modulo m** Let $m \in \mathbb{Z}^+$.

Exercise A.4.1.18 Show that $m\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Then, the ***integers modulo*** m are defined to be the quotient cring $\mathbb{Z}/m\mathbb{Z}$.

A.5 Cardinality, countability, and the natural numbers

The goal of this section is to define what is called the *cardinality* of a set. Intuitively, the cardinality of a set is the number of elements that set contains. The concept of cardinality will then allow us to define

the *natural numbers* (at least as a well-ordered set—we won't worry about the arithmetic of the natural numbers here), which in turn will allow us to define the important concept of *countability*.

A.5.1 Cardinality

The first step in defining the cardinality of sets is being able to decide when two sets have the same number of elements. So, suppose we are given two sets X and Y and that we would like to determine whether X and Y have the same number of elements. How would you do this?

Intuitively, you could start by trying to label all the elements in Y by elements of X, without repeating labels. If either (i) you ran out of labels before you finished labeling all elements in Y or (ii) you were forced to assign more than one label to an element of Y, then you could deduce that X and Y did *not* have the same number of elements. To make this precise, we think of this labeling as a function from X to Y. Then, the first case corresponds to this labeling function not being surjective and the second case corresponds to this labeling function not being injective.

The more precise intuition is then that the two sets X and Y have the same number of elements, that is, the same cardinality, iff there is a bijection $f\colon X \to Y$ between them: that f is an injection says that we don't use a label more than once (or equivalently that Y has at least as many elements as X) and that f is a surjection says that we label everything at least once (or equivalently that X has at least as many elements as Y). This yields the following definition.

Definition A.5.1.1 — Equinumerous Let X and Y be sets. Then, X and Y are ***equinumerous*** iff there is a bijection from X to Y.

Exercise A.5.1.2 Show that the relation of equinumerosity is an equivalence relation on the collection of sets.

So we've determined what it means for two sets to have the same cardinality, but what actually *is* a cardinality? The trick is to identify a cardinal with the collection of all sets which have that cardinality.

Definition A.5.1.3 — Cardinal number A *cardinal number* is an element of

$$\aleph := \mathrm{Obj}(\mathbf{Set})/\cong := \{[X]_{\cong} : X \in \mathrm{Obj}(\mathbf{Set})\}, \quad \text{(A.5.1.4)}$$

where $\cong$ is the equivalence relation of equinumerosity.

R In other words, a cardinal is an equivalence class of sets, the equivalence relation being equinumerosity. Furthermore, for X a set, we write $|X| := [X]_{\cong_{\mathbf{Set}}}$.

The next objective we would like to achieve is to be able to compare cardinals. As cardinal numbers are supposed to be a 'size' of some sort, we should have a notion of what it means for one cardinal to be larger than another. Of course, there is such a notion, and the relation so defined turns out to be a *well-order*. Once we define the natural numbers, it will then follow automatically that it restricts to a well-order on $\mathbb{N}$—see Corollary A.5.2.10.

As for what the definition of that well-order should be, recall our explanation of thinking of a function $f\colon X \to Y$ as 'labeling elements of Y with elements of X'—see the beginning of Appendix A.5.1 Cardinality. We argued that our definition of 'same number of elements' should have the properties that (i) every element of Y is labeled and (ii) no element of Y is labeled more than once. Similarly, our definition of "Y has at least as many element of X" should have the property that are not forced to label an element of Y more than once (i.e. that f is injective), but not necessarily that every element of Y is labeled.

Definition A.5.1.5 Let $m, n \in \aleph$ and let M and N be sets such that $m = |M|$ and $n = |N|$. Then, we define $m \leq n$ iff there is an injective map from M to N.

Exercise A.5.1.6 Check that $\leq$ is well-defined.

You might be thinking "Ah, that makes sense. But why use injective? Couldn't we also say that $|X| \geq |Y|$ iff there is a *surjective* function $X \to Y$?". Unfortunately, this is only *almost* correct.

Exercise A.5.1.7

(i). Show that if X and Y are nonempty sets, then $|X| \leq |Y|$ iff there is a surjective function from Y to X.

(ii). On the other hand, show how this might fail without the assumption of nonemptiness.

Proposition A.5.1.8 $\langle \aleph, \leq \rangle$ is a preordered set.

Proof. Recall that being a preorder just means that $\leq$ is reflexive and transitive (see Definition A.3.3.1).

Let $m, n, o \in \mathbb{N}$ and let M, N, O be sets such that $m = |M|$, $n = |N|$, $o = |O|$. The identity map from M to M is an injection (and, in fact, a bijection), which shows that $m = |M| \leq |M| = m$, so that $\leq$ is reflexive.

To show transitivity, suppose that $m \leq n$ and $n \leq o$. Then, there is an injection $f : M \to N$ and an injection from $g : N \to O$. Then, $g \circ f : M \to O$ is an injection (this is part of Exercise A.3.28), and so we have $m = |M| \leq |O| = o$, so that $\leq$ is transitive, and hence a preorder. ∎

That $\leq$ is a preorder is relatively easy. The next step, showing that it is a partial-order, is considerably more difficult, and even has a name.

Theorem A.5.1.9 — Bernstein-Cantor-Schröder Theorem. $\langle \aleph, \leq \rangle$ is a partially-ordered set.

R This theorem is usually stated as "If there is an injection from X to Y and there is an injection from Y to X, then there is a bijection from X to Y.".

R This theorem is *incredibly* useful for showing that two sets have the same cardinality—it's often much

easier to construct an injection in each direction than it is to construct a single bijection—and it would do you well to not forget it.

Proof. [a] STEP 1: RECALL WHAT IT MEANS TO BE A PARTIAL-ORDER

Recall that being a partial-order just means that $\leq$ is an antisymmetric preorder. We have just shown that $\leq$ is a preorder (see Definition A.3.3.6), so all that remains to be seen is that $\leq$ is antisymmetric.

STEP 2: DETERMINE WHAT EXPLICITLY WE NEED TO SHOW

Let $m, n \in \aleph$ and let M, N be sets such that $m = |M|$ and $n = |N|$. Suppose that $m \leq n$ and $n \leq m$. By definition, this means that there is an injection $f : M \to N$ and an injection $g : N \to M$. We would like to show that $m = n$. By definition, this means we must show that there is a bijection from M to N.

STEP 3: NOTE THE EXISTENCE OF LEFT-INVERSE TO BOTH f AND g

If M is empty, then as N injects into M, N must also be empty, and we are done. Likewise, if N is empty, we are also done. Thus, we may as well assume that M and N are both nonempty. We can now use the result of Equation (A.3.26) which says that both f and g have left inverses.[b] Denote these inverses by $f^{-1} : N \to M$ and $g^{-1} : M \to N$ respectively, so that

$$f^{-1} \circ f = \mathrm{id}_M \text{ and } g^{-1} \circ g = \mathrm{id}_N .^{c} \tag{A.5.1.10}$$

STEP 4: DEFINE C_x

Fix an element $x \in M$ and define

$$C_x \coloneqq \Big\{\ldots, g^{-1}\left(f^{-1}\left(g^{-1}(x)\right)\right), f^{-1}\left(g^{-1}(x)\right), g^{-1}(x), x, f(x), g\left(f(x)\right), f\left(g\left(f(x)\right)\right), \ldots\Big\} \subseteq M \sqcup N.^{d}$$

Note that C_x is 'closed' under application of f, g, f^{-1}, and g^{-1}, in the sense that, if $x' \in C_x$ and $f(x')$ makes sense (i.e. if $x' \in M$), then $f(x') \in C_x$, and similarly for g, f^{-1}, and g^{-1}.

STEP 5: SHOW THAT $\{C_x : x \in M\}$ FORMS A PARTITION OF $M \sqcup N$

We now claim that the collection $\{C_x : x \in M\}$ forms a partition of $M \sqcup N$ (recall that this means that any two given C_xs are either identical or disjoint—see Definition A.3.2.9). If C_{x_1} is disjoint from C_{x_2} we are done, so instead suppose that there is some element x_0 that is in both C_{x_1} and C_{x_2}. First, let us do the case in which $x_0 \in M$. From the definition of C_x, we then must have that

$$[g \circ f]^k(x_1) = x_0 = [g \circ f]^l(x_2) \tag{A.5.1.11}$$

for some $k, l \in \mathbb{Z}$. Without loss of generality, suppose that $k \leq l$. Then, applying $f^{-1} \circ g^{-1}$ to both sides of this equation k times,[e] we find that

$$x_1 = [g \circ f]^{l-k}(x_2). \tag{A.5.1.12}$$

In other words, $x_1 \in C_{x_2}$. Not only this, but $f(x_1) \in C_{x_2}$ as well because $f(x_1) = f\left([g \circ f]^{l-k}(x_2)\right)$. Similarly, $g^{-1}(x_1) \in C_{x_2}$, and so on. It follows that $C_{x_1} \subseteq C_{x_2}$. Switching $1 \leftrightarrow 2$ and applying the same arguments gives us $C_{x_2} \subseteq C_{x_1}$, and hence $C_{x_1} = C_{x_2}$. Thus, indeed, $\{C_x : x \in M\}$ forms a partition of $M \sqcup N$. In particular, it follows that

$$C_x = C_{x'} \text{ for all } x' \in C_x. \tag{A.5.1.13}$$

STEP 6: DEFINE X_1, X_2, Y_1, Y_2

Now define

$$A := \bigcup_{\substack{x \in M \text{ s.t.} \\ C_x \cap N \subseteq f(M)}} C_x \tag{A.5.1.14}$$

as well as

$$X_1 := M \cap A, \qquad Y_1 := N \cap A, \tag{A.5.1.15a}$$
$$X_2 := M \cap A^{\mathsf{C}}, \qquad Y_2 := N \cap A^{\mathsf{C}}. \tag{A.5.1.15b}$$

Note that, as $\{C_x : x \in M\}$ is a partition of $M \sqcup N$, we have that

$$A^{\mathsf{C}} = \bigcup_{\substack{x \in M \text{ s.t.} \\ C_x \cap N \not\subseteq f(M)}} C_x. \tag{A.5.1.16}$$

Step 7: Show that $f|_{X_1} : X_1 \to Y_1$ is a bijection
We claim that $f|_{X_1} : X_1 \to Y_1$ is a bijection. First of all, note the it $x \in X_1$, then in fact $f(x) \in Y_1$, so that this statement indeed does make sense. Of course, it is injective because f is. To show surjectivity, let $y \in Y_1 := N \cap A$. From the definition of A (A.5.1.14), we see that $y \in C_x \cap N$ for some C_x with $C_x \cap N \subseteq f(M)$, so that $y = f(x')$ for some $x' \in M$. We still need to show that $x' \in X_1$. However, we have that $x' = f^{-1}(y)$, and so as $y \in C_x$, we have that $x' = f^{-1}(y) \in C_x$ as well. We already had that $C_x \cap N \subseteq f(M)$, so that indeed $x' \in A$, and hence $x' \in X_1$. Thus, $f|_{X_1} : X_1 \to Y_1$ is a bijection.

Step 8: Show that $g|_{Y_2} : Y_2 \to X_2$ is a bijection
We now show that $g|_{Y_2} : Y_2 \to X_2$ is a bijection. Once again, all we must show is surjectivity, so let $x \in X_2 = M \cap A^{\mathsf{C}}$. From the definition of A (A.5.1.14), it thus cannot be the case that $C_x \cap N$ is contained in $f(M)$, so that there is some $y \in C_x \cap N$ such that $y \notin f(M)$. By virtue of (A.5.1.13), we have that $C_x = C_y$, and in particular $x \in C_y$. From the definition of C_y, it follows that either (i) $x = y$, (ii) x is in the image of f^{-1}, or (iii) x is in the image of g (the other possibilities are excluded because $x \in M$). Of course it cannot be the case that $x = y$ because $x \in M$ and $y \in N$. Likewise, it cannot be the case that x is in the image of f^{-1} because $x \in A^{\mathsf{C}}$. Thus, we must

have that $x = g(y')$ for some $y' \in N$. Once again, we still must show that $y' \in Y_2$. However, we have that $y' = g^{-1}(x)$, so that $y' \in C_x$. Furthermore, as $C_x \cap N$ is not contained in $f(M)$, from (A.5.1.16) it follows that $C_x \subseteq A^{\mathsf{C}}$. Thus, $y' \in C_x \subseteq A^{\mathsf{C}}$, and so $y' \in Y_2$. Thus, $g|_{Y_2} : Y_2 \to X_2$ is a bijection.

Step 9: Construct the bijection from M to N
Finally, we can define the bijection from M to N. We define $h\colon M \to N$ by

$$h(x) := \begin{cases} f(x) & \text{if } x \in X_1 \\ g^{-1}(x) & \text{if } x \in X_2. \end{cases} \tag{A.5.1.17}$$

Note that $\{X_1, X_2\}$ is a partition of M and $\{Y_1, Y_2\}$ is a partition of N. To show injectivity, suppose that $h(x_1) = h(x_2)$. If this element is in Y_1, then because $f|_{X_1} : X_1 \to Y_1$ is a bijection, it follows that both $x_1, x_2 \in X_1$, so that $f(x_1) = h(x_1) = h(x_2) = f(x_2)$, and hence that $x_1 = x_2$. Similarly if this element is contained in Y_2. To show surjectivity, let $y \in N$. First assume that $y \in Y_1$. Then, $f^{-1}(y) \in X_1$, so that $h\left(f^{-1}(y)\right) = y$. Similarly, if $y \in Y_2$, then $h\left(g(y)\right) = y$. Thus, h is surjective, and hence bijective. ■

R I think perhaps the mathematical precision here has obfuscated the core idea of the proof. Briefly, the basic idea is as follows. Once we have defined the chains C_xs, they 'break-up' M and N into 'chunks' in such a way that it suffices to construct a bijection separately on each chunk (that is, they form a *partition*). If the elements of C_x in the codomain are actually contained in the image of f, then f itself can serve as the bijection on that "chunk"—otherwise, we can use g.

[a] Proof adapted from [Abb02, pg. 29].

[b] To use this, we first needed to have that M and N are nonempty.

[c] Note that it is *not* necessarily the case that $f \circ f^{-1} = \mathrm{id}_N$ (and similarly for g). This certainly constitutes an abuse of notation, as we should really

be reserving the notation f^{-1} for a *two*-sided inverse, but as this makes the proof quite a bit more readable, we ignore such pedantry for the time being.

[d] The "C" is for "chain".

[e] If k happens to be negative, it is understood that we instead apply $g \circ f$ $-k$ times.

Finally, we check that $\leq$ is a well-order on $\aleph$.

Theorem A.5.1.18. $\langle \aleph, \leq \rangle$ is well-ordered.

Proof. [a] STEP 1: CONCLUDE THAT IT SUFFICES TO SHOW THAT EVERY NONEMPTY SUBSET HAS A SMALLEST ELEMENT

By Proposition A.3.3.16, we do not need to check totality explicitly, and so it suffices to show that every nonempty subset of $\aleph$ has a smallest element.

STEP 2: DEFINE $\mathcal{T}$ AS A PREORDERED SET

So, let $S \subseteq \aleph$ be a nonempty collection of cardinals and for each $m \in S$ write $m = |M_m|$ for some set M_m. Define

$$M := \prod_{m \in S} M_m \tag{A.5.1.19}$$

and

$$\mathcal{T} := \{T \subseteq M : T \in \mathrm{Obj}(\mathbf{Set});\ \text{for all } x, y \in T, \text{ if } x \neq y \text{ it follows that } x_m \neq y_m \text{ for all } m \in S.\}.$$

Order $\mathcal{T}$ by inclusion.

STEP 3: VERIFY THAT $\mathcal{T}$ SATISFIES THE HYPOTHESES OF ZORN'S LEMMA

We wish to apply Zorn's Lemma (Theorem A.3.5.9) to $\mathcal{T}$. To do that of course, we must first verify the hypotheses of Zorn's

Lemma. $\mathcal{T}$ is a partially-ordered set by Exercise A.3.3.11. Let $\mathcal{W} \subseteq \mathcal{T}$ be a well-ordered subset and define

$$W := \bigcup_{T \in \mathcal{W}} T. \tag{A.5.1.20}$$

It is certainly the case that $T \subseteq W$ for all $T \in \mathcal{W}$. In order to verify that W is indeed an upper-bound of $\mathcal{W}$ in $\mathcal{T}$, however, we need to check that W is actually an element of $\mathcal{T}$. So, let $x, y \in W$ be distinct. Then, there are $T_1, T_2 \in \mathcal{W}$ such that $x \in T_1$ and $y \in T_2$. Because $\mathcal{W}$ is in particular totally-ordered, we may without loss of generality assume that $T_1 \subseteq T_2$. In this case, both $x, y \in T_2$. As $T_2 \in \mathcal{T}$, it then follows that $x_m \neq x_m$ for all $m \in S$. It then follows in turn that $W \in \mathcal{T}$.

Step 4: Conclude the existence of a maximal element

The hypotheses of Zorn's Lemma being verified, we deduce that there is a maximal element $T_0 \in \mathcal{T}$.

Step 5: Show that there is some projection whose restriction to the maximal element is surjective

Let $\pi_m : M \to M_m$ be the canonical projection. We claim that there is some $m_0 \in S$ such that $\pi_{m_0}(T_0) = M_{m_0}$. To show this, we proceed by contradiction: suppose that for all $m \in M$ there is some element $x_m \in M_m \setminus \pi_m(T_0)$. Then, $T_0 \cup \{x\} \in \mathcal{T}$ is strictly larger than T_0: a contradiction of maximality. Therefore, there is some $m_0 \in S$ such that $\pi_{m_0}(T_0) = M_{m_0}$.

Step 6: Construct an injection from M_{m_0} to M_m for all $m \in S$

The defining condition of $\mathcal{T}$ is simply the statement that $\pi_m|_T : T \to M_m$ is injective for all $T \in \mathcal{T}$. In particular, by the previous step, $\pi_{m_0}\big|_{T_0} : T_0 \to M_{m_0}$ is a bijection. And

therefore, the composition $\pi_m \circ \pi_{m_0}\big|_{T_0}^{-1} : M_{m_0} \to M_m$ is an injection from M_{m_0} to M. Therefore,

$$m_0 = \left|M_{m_0}\right| \leq |M_m| = m \tag{A.5.1.21}$$

for all $m \in S$. That is, m_0 is the smallest element of S, and so $\aleph$ is well-ordered. ■

[a] Proof adapted from [Hön].

A.5.2 The natural numbers

The key idea used to define the natural numbers is that the natural numbers should be precisely those cardinals which are finite. We thus must now answer the question "What does it mean to be 'finite'?". This is actually a tad bit tricky.

Of course, we don't have a precise definition yet, but everyone has an intuitive idea of what it means to be infinite. So, consider an 'infinite set' X. Now remove one element $x_0 \in X$ to form the set $U := X \setminus \{x_0\}$. For any reasonable definition of "infinite", removing a single element from an infinite set should not change the fact that it is infinite, and so U should still be infinite. In fact, more should be true. Not only should U still be infinite, but it should still have the same cardinality as X.[29] It is this idea that we take as the defining property of being infinite.

Definition A.5.2.1 — Finite and infinite Let X be a set. Then, X is ***infinite*** iff there is a bijection from X to a proper subset of X. X is ***finite*** iff it is not infinite.

R The keyword here is *proper*—there is a bijection from every set X to some subset of X, namely $X \subseteq X$ itself.

[29] We will see in the next chapter that there are infinite sets which are not of the same cardinality. That is, in this sense, there is more than one type of infinity.

Before getting to the natural numbers themselves, let's discuss a couple of interesting properties about infinite sets.

Proposition A.5.2.2 Let X be a set and define

$$\mathscr{F}_X := \{S \subseteq X : S \text{ is finite.}\}\,. \tag{A.5.2.3}$$

Then, if X is infinite, then $|X| = |\mathscr{F}_X|$.

R In words, for infinite sets, the cardinality of the set itself is the same as the cardinality of its collection of finite subsets.

Proof. We leave this as an exercise.

Exercise A.5.2.4 Prove this yourself.

■

Proposition A.5.2.5 Let $\mathscr{F}$ be an infinite collection of finite sets. Then,

$$\left|\bigcup_{F\in\mathscr{F}} F\right| = |\mathscr{F}|. \tag{A.5.2.6}$$

R In words, if κ is an infinite cardinal, the union of κ many finite sets still has cardinality κ.

Proof. We leave this as an exercise.

Exercise A.5.2.7 Prove this yourself.

■

And now finally:

Definition A.5.2.8 — Natural numbers The ***natural numbers***, $\mathbb{N}$, are defined as

$$\mathbb{N} := \{|X| : X \in \text{Obj}(\mathbf{Set}) \text{ is finite.}\} . \tag{A.5.2.9}$$

In words, the natural numbers are precisely the cardinals of finite sets.

R Some people take the natural numbers to not include 0. This is a bit silly for a couple of reasons. First of all, if you think of the natural numbers as cardinals, as we are doing here, then 0 has to be a natural number as it is the cardinality of the empty-set. Furthermore, as we shall see in the next subsection, it makes the algebraic structure of $\mathbb{N}$ slightly nicer because 0 acts as an additive identity. Indeed, I am not even aware of a term to describe the sort of algebraic object $\mathbb{N}$ would be if it did not contain 0. Finally, regardless of your convention, you already have a symbol to denote $\{1, 2, 3, \ldots\}$, namely $\mathbb{Z}^+$:[a] having the symbol $\mathbb{N}$ denote the same is an inefficient use of notation.

[a] Of course, at this point in the next, we technically don't know what any of these symbols mean. For the purposes of motivating a convention, however, I have no qualms about pretending you are not completely ignorant.

As a corollary of Theorem A.5.1.18, we immediately have the following.

Corollary A.5.2.10 $\langle \mathbb{N}, \leq \rangle$ is a well-ordered set.

A.5.3 Countability

The cardinality of the natural numbers is special: it turns out that the cardinality of the natural numbers is the smallest infinite cardinal.

Proposition A.5.3.1 Let κ be an infinite cardinal. Then, $|\mathbb{N}| \leq \kappa$.

R Phrased differently ,note that the contrapositive easily implies the following.

If κ is a cardinal with $\kappa \leq |\mathbb{N}|$, then either $\kappa = |\mathbb{N}|$ or κ is finite.

Proof. Let K be any set such that $|K| = \kappa$. Recall that (Definition A.5.1.5) to show that $|\mathbb{N}| \leq \kappa$ requires that we produce an injection from $\mathbb{N}$ into K. We construct an injection $f : \mathbb{N} \to K$ inductively. Let $k_0 \in K$ be arbitrary and let us define $f(0) := k_0$. If $K \setminus \{k_0\}$ were empty, then K would not be infinite, therefore there must be some $k_1 \in K$ distinct from k_0, so that we may define $f(1) := k_1$. Continuing this process, suppose we have defined f on $0, \ldots, n \in \mathbb{N}$, and wish to define $f(n+1)$. If $K \setminus \{f(0), \ldots, f(n)\}$ were empty, then K would be finite. Thus, there must be some $k_{n+1} \in K$ distinct from $f(0), \ldots, f(n)$. We may then define $f(n+1) := k_{n+1}$. The function produced must be injective because, by construction, $f(m)$ is distinct from $f(n)$ for all $n < m$. Hence, $|\mathbb{N}| \leq \kappa$. ■

Thus, the cardinality of the natural numbers is the smallest infinite cardinality. We give a name to this cardinality.

Definition A.5.3.2 — Countability Let X be a set. Then, X is ***countably-infinite*** iff $|X| = |\mathbb{N}|$. X is ***countable*** iff either X is countably-infinite or X is finite. We write $\aleph_0 := |\mathbb{N}|$.

R It is not uncommon for people to use the term "countable" to mean what we call "countably-infinite". They would would then just say "countable or finite" in cases that we would say "countable".

Our first order of business is to decide what other sets besides the natural numbers are countably-infinite.

Proposition A.5.3.3 The even natural numbers, $2\mathbb{N}$, are countably-infinite.

Proof. On one hand, $2\mathbb{N} \subseteq \mathbb{N}$, so that $|2\mathbb{N}| \leq \aleph_0$. On the other hand, $2\mathbb{N}$ is infinite, and as we just showed that $\aleph_0$ is the smallest infinite cardinal, we must have that $\aleph_0 \leq |2\mathbb{N}|$. Therefore, by antisymmetry (Bernstein-Cantor-Schröder Theorem, Theorem A.5.1.9) of $\leq$, we have that $|2\mathbb{N}| = \aleph_0$. ■

Exercise A.5.3.4 Construct an explicit bijection from $\mathbb{N}$ to $2\mathbb{N}$.

This is the first explicit example we have seen of some perhaps not-so-intuitive behavior of cardinality. On one hand, our intuition might tell us that there are half as many even natural numbers as there are natural numbers, yet, on the other hand, we have just proven (in two different ways, if you did the exercise) that $2\mathbb{N}$ and $\mathbb{N}$ have the same number of elements! This of course is not the only example of this sort of weird behavior. The next exercise shows that this is actually quite general.

Exercise A.5.3.5 Let X and Y be countably-infinite sets. Show that $X \sqcup Y$ is countably-infinite.

R Note that this generalizes—see Exercise A.5.3.7.

Thus, it is literally the case that $2\aleph_0 = \aleph_0$. A simple corollary of this is that $\mathbb{Z}$ is countably-infinite.

Exercise A.5.3.6 Show that $|\mathbb{Z}| = \aleph_0$.

You (hopefully) just showed that $2\aleph_0 = \aleph_0$, but what about $\aleph_0^2$?

Exercise A.5.3.7 Let $\mathscr{X}$ be a countable indexed collection of countable sets. Show that

$$\bigsqcup_{X \in \mathscr{X}} X \tag{A.5.3.8}$$

is countable.

Proposition A.5.3.9 $\aleph_0^2 = \aleph_0$.

Proof. For $m \in \mathbb{N}$, define

$$X_m := \{\langle i, j\rangle \in \mathbb{N} \times \mathbb{N} : i + j = m\} \tag{A.5.3.10}$$

Note that each X_m is finite and also that

$$\mathbb{N} \times \mathbb{N} = \bigsqcup_{m \in \mathbb{N}} X_m. \tag{A.5.3.11}$$

Therefore, by the previous exercise, $|\mathbb{N} \times \mathbb{N}| =: \aleph_0^2$ is countable, i.e., $\aleph_0^2 \leq \aleph_0$. As $\aleph_0$ is not finite, we must thus have that $\aleph_0^2 = \aleph_0$ (Proposition A.5.3.1). ∎

Exercise A.5.3.12 Use Bernstein-Cantor-Schröder and the previous proposition to show that $|\mathbb{Q}| = \aleph_0$.

This result might seem a bit crazy at first. I mean, just 'look' at the number line, right? There's like bajillions more rationals than naturals. Surely it can't be the case there there are no more rationals than natural numbers, can it? Well, yes, in fact that can be, and in fact is, precisely the case—despite what your silly intuition might be telling you, there are no more rational numbers than there are natural numbers.

So, we've now done both $\mathbb{Z}$ and $\mathbb{Q}$, but what about $\mathbb{R}$? At first, you might have declared it obvious that there are more real numbers than natural numbers, but perhaps the result about $\mathbb{Q}$ has now given you some doubt. In fact, it *does* turn out that there are more real numbers than there are natural numbers. They key idea used to prove this is the following important famous result.

Theorem A.5.3.13 — Cantor's Cardinality Theorem. Let X be a set. Then, $|X| < |2^X|$.

R There is a good chance you may have heard of the term ***Cantor's Diagonal Argument***. The argument

here is a generalization of that (it's also 'cleaner'), and so we don't present the Diagonal Argument itself.

R We don't have need to give the details of how to show that $|\mathbb{R}| > |\mathbb{N}|$—these are better saved for an analysis course—but we can at least explain the vague idea. Of course, it suffices to show that $|[0,1)| > |\mathbb{N}|$. To do that, you think of elements in $[0,1)$ as being defined in terms of their binary expansions, which allows you to associate to every element of $[0,1)$ a sequence of 0s and 1s. Such a sequence in turn corresponds to a subset of $\mathbb{N}$—see Exercise A.3.31—and this then reduces the problem to show that $\left|2^{\mathbb{N}}\right| > |\mathbb{N}|$, but this is precisely the conclusion of Cantor's Cardinality Theorem!

Proof. We must show two things: (i) $|X| \leq |2^X|$ and (ii) $|X| \neq |2^X|$.

The first, by definition, requires that we construct an injection from X to 2^X. This, however, is quite easy. We may define a function $X \to 2^X$ by $x \mapsto \{x\}$. This is of course an injection.

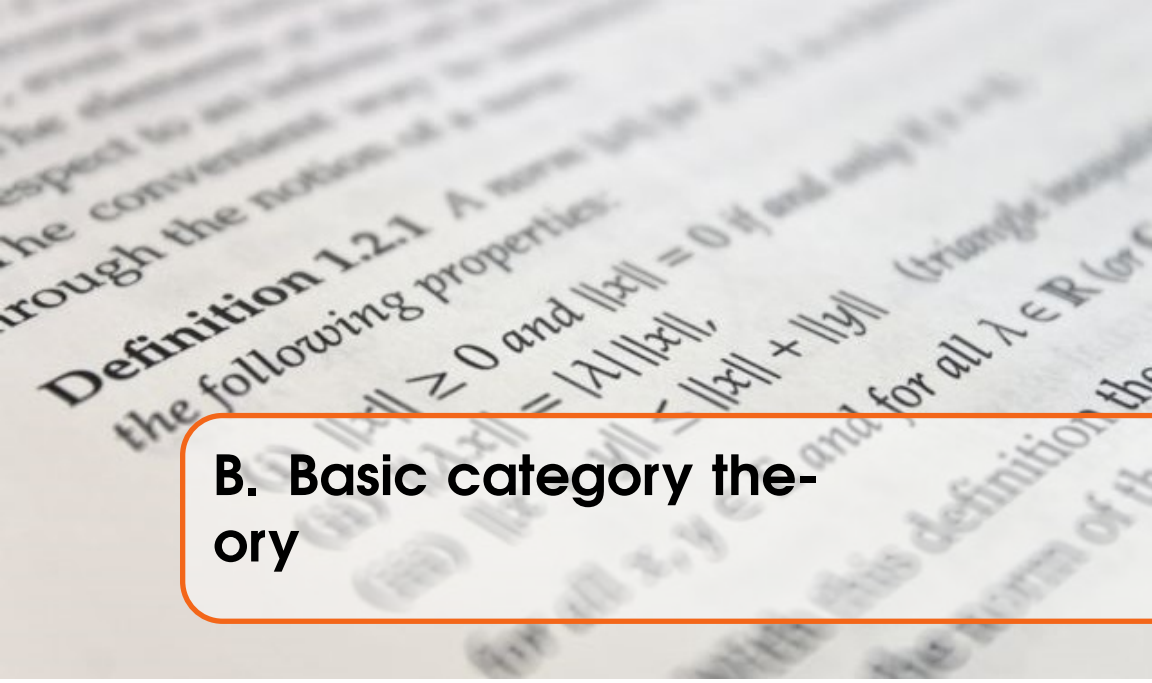
The harder part is showing that $|X| \neq |2^X|$. To show this, we must show that there is *no* surjection from X to 2^X. So, let $f\colon X \to 2^X$ be a function. We show that f cannot be surjective. To do this, we construct a subset of X that cannot be in the image of f.

We define

$$S := \{x \in X : x \notin f(x)\}\,. \tag{A.5.3.14}$$

We would like to show that S is not in the image of f. We proceed by contradiction: suppose that $S = f(x_0)$ for some $x_0 \in X$. Now, we must have that either $x_0 \in S$ or $x_0 \notin S$. If the former were true, then we would have that $x_0 \notin f(x_0) = S$: a contradiction. On the other hand, in the latter case, we would have $x \in f(x_0) = S$: a contradiction. Thus, as neither of these possibilities can be true, there cannot be any $x_0 \in X$ such that

$f(x_0) = S$. Thus, S is not in the image of f, and so f is not surjective. ■



B. Basic category theory

First of all, a disclaimer: it is probably not best pedagogically speaking to start with even the very basics of category theory. While in principle anyone who has the prerequisites for these notes knows everything they need to know to understand category theory, it may be difficult to understand the motivation for things without a collection of examples to work with in the back of your mind. Thus, if anything in this section does not make sense the first time you read through it, you should not worry—it will only be a problem if you do not understand ideas here as they occur in the text. In fact, it is probably perfectly okay to completely skip this section and reference back to it as needed. In any case, our main motivation for introducing category theory in a subject like this is simply that we would like to have more systematic language and notation.

B.1 What is a category?

In mathematics, we study many different types of objects: sets, preordered sets, monoids, rngs, vector spaces, topological spaces, schemes, etc..[1] In all of these cases, however, we are not only

[1] No, you are not expected to know what all of these are.

concerned with the objects themselves, but also with maps between them that 'preserve' the relevant structure. In the case of a set, there is no extra structure to preserve, and so the relevant maps are *all* the functions. In contrast, however, for vector spaces, we will see that the relevant maps are not all the functions, but instead all *linear* functions. The idea then is to come up with a definition that deals with both the objects and the relevant maps, or morphisms, simultaneously. This is the motivating idea of the definition of a category.

Definition B.1.1 — Category A ***category*** $\mathbf{C}$ is

(I). a collection $\mathrm{Obj}(\mathbf{C})$, the ***objects*** of $\mathbf{C}$; together with
(II). for each $A, B \in \mathrm{Obj}(\mathbf{C})$, a collection $\mathrm{Mor}_{\mathbf{C}}(A, B)$, the ***morphisms*** from A to B in $\mathbf{C}$;[a]
(III). for each $A, B, C \in \mathrm{Obj}(\mathbf{C})$, a function $\circ : \mathrm{Mor}_{\mathbf{C}}(B, C) \times \mathrm{Mor}_{\mathbf{C}}(A, B) \to \mathrm{Mor}_{\mathbf{C}}(A, C)$ called ***composition***;
(IV). and for each $A \in \mathrm{Obj}(\mathbf{C})$ a distinguished element $\mathrm{id}_A \in \mathrm{Mor}_{\mathbf{C}}(A, A)$, the ***identity*** of A;

such that

(i). $\circ$ is 'associative', that is, $f \circ (g \circ h) = (f \circ g) \circ h$ for all morphisms f, g, h for which these composition make sense,[b] and
(ii). $f \circ \mathrm{id}_A = f = \mathrm{id}_A \circ f$ for all $A \in \mathrm{Obj}(\mathbf{C})$.

R We write

$$\mathrm{Mor}_{\mathbf{C}} := \bigsqcup_{A,B \in \mathrm{Obj}(\mathbf{C})} \mathrm{Mor}_{\mathbf{C}}(A, B) \qquad \text{(B.1.2)}$$

for the collection of all morphisms in $\mathbf{C}$.

R The term ***map*** is often used synonymously with the term "morphism", though perhaps in a more casual manner. For example, it is not uncommon to see people say "linear map" instead of "map of vector spaces" or "map in the category of vector spaces".

R If the category $\mathbf{C}$ is clear from context, we may simply write $\mathrm{Mor}(A, B)$.

R We mentioned above that the morphisms relevant to vector spaces are the linear functions. Of course, nothing about the definition of a category *requires* this be the case—you could just as well consider the category whose objects are vector spaces and whose morphisms are *all* functions—it just turns out that these weird examples aren't particularly useful.

[a] No, we do not require that $\mathrm{Mor}_{\mathbf{C}}(A, B)$ be a (small) set. (This comment is really intended for those who have seen this definition elsewhere—often times authors fix a universe U, whose elements are referred to as the *small sets*, and in the definition of a category they require that the morphisms form small sets—we make no such requirement.)

[b] In case you're wondering, the quotes around "associative" are used because usually the word "associative" refers to a property that a binary operation has. A binary operation on a set S is, by definition, a function from $X \times X$ into X. Composition however in general is a function from $X \times Y$ into Z for $X := \mathrm{Mor}_{\mathbf{C}}(B, C)$, $Y := \mathrm{Mor}_{\mathbf{C}}(A, B)$ and $Z := \mathrm{Mor}_{\mathbf{C}}(A, C)$, and hence not a binary operation.

The intuition here is that the objects $\mathrm{Obj}(\mathbf{C})$ are the objects you are interested in studying (for example, vector spaces), and for objects $A, B \in \mathrm{Obj}(\mathbf{C})$, the morphisms $\mathrm{Mor}_{\mathbf{C}}(A, B)$ are the maps relevant to the study of the objects in $\mathbf{C}$ (for example, linear functions from A to B). For us, it will usually be the case that every element of $\mathrm{Obj}(\mathbf{C})$ is a set equipped with extra structure (e.g. a binary operation) and the morphisms are just the functions that 'preserve' this structure (e.g. homomorphisms). In fact, there is a term for such categories—see Definition B.1.7.

At the moment, this might seem a bit abstract because of the lack of examples. As you continue through the main text, you will encounter more examples of categories, which will likely elucidate this abstract definition. However, even already we have a couple basic examples of categories.

▪ **Example B.1.3 — The category of sets** The category of sets is the category **Set**

(i). whose collection of objects Obj(**Set**) is the collection of all sets,[a];
(ii). with morphism set $\mathrm{Mor}_{\mathbf{Set}}(X, Y)$ precisely the set of all functions from X to Y;
(iii). whose composition is given by ordinary function composition; and
(iv). whose the identities are given by the identity functions.

[a] See Appendix A.1 for clarification as to what we actually mean by the phrase "all sets".

We also have another example at our disposal, namely the category of preordered sets.

▪ **Example B.1.4 — The category of preordered sets** The category of preordered sets is the category **Pre**

(i). whose collection of objects Obj(**Pre**) is the collection of all preordered sets;
(ii). with morphism set $\mathrm{Mor}_{\mathbf{Pre}}(X, Y)$ precisely the set of all nondecreasing functions from X to Y;
(iii). whose composition is given by ordinary function composition; and
(iv). whose identities are given by the identity functions.

The idea here is that the only structure on a preordered set is the preorder, and that the precise notion of what it means to 'preserve' this structure is to be nondecreasing. Of course, we could everywhere replace the word "preorder" (or its obvious derivatives) with "partial-order" or "total-order" and everything would make just as much sense. Upon doing so, we would obtain the category of partially-ordered sets and the category of totally-ordered sets respectively.

We also have the category of magmas.

▪ **Example B.1.5 — The category of magmas** The category of magmas is the category **Mag**

(i). whose collection of objects Obj(**Mag**) is the collection of all magmas;
(ii). with morphism set $\mathrm{Mor}_{\mathbf{Mag}}(X, Y)$ precisely the set of all homomorphisms from X to Y;
(iii). whose composition is given by ordinary function composition; and
(iv). whose identities are given by the identity functions.

Similarly, the idea here is that the only structure here is that of the binary operation (and possibly an identity element) and that it is the homomorphisms which preserve this structure. Of course, we could everywhere here replace the word "magma" with "semigroup", "monoid", "group", etc. and everything would make just as much sense. Upon doing so, we would obtain the categories of semigroups, the category of monoids, and the category of groups respectively.

Finally we have the category of rgs.

▪ **Example B.1.6 — The category of rgs** The category of rgs is the category **Rg**

(i). whose collection of objects Obj(**Rg**) is the collection of all rgs;
(ii). with morphism set $\mathrm{Mor}_{\mathbf{Rg}}(X, Y)$ is precisely the set of all homomorphisms from X to Y;
(iii). whose composition is given by ordinary function composition; and
(iv). and whose identities are given by the identity functions.

R The same as before, we could have everywhere replaced the word "rg" with "rig", "rng", or "ring". These categories are denoted **Rig**, **Rng**, and **Ring** respectively.

As mentioned previously, it should almost always be the case that the examples of categories we encounter are of this form, that is, in which the objects are "sets equipped with extra structure" and the

morphisms are "functions which 'preserve' this structure". The term for such categories is *concrete*.

Definition B.1.7 — Concrete category Let $\mathbf{C}$ be a category. Then, $\mathbf{C}$ is ***concrete*** iff for all $A, B \in \mathrm{Obj}(\mathbf{C})$, $\mathrm{Mor}_{\mathbf{C}}(A, B) \subseteq \mathrm{Mor}_{\mathbf{Set}}(A, B)$.

R When defining categories, if the category happens to be concrete, we shall omit an explicit statement of the composition and identity, and instead will simply say that the category is concrete (e.g. "The category of XYZ is the concrete category $\mathbf{C}$...").

R Warning: Strictly speaking, this doesn't actually make sense as A and B are not actually sets. Implicit in this is that we are additionally given a way of regarding objects of $\mathbf{C}$ as sets. For example, in the case of the category of vector spaces, we regard a vector space as a set simply by "forgetting" the addition and scaling operations. To better understand this, it might help to see an example of a nonconcrete category—see the following example.

While not terribly important for us, as you might now be wondering "What could a nonconcrete category possibly look like?", we present the following example.

▪ **Example B.1.8 — A category that is not concrete** Let $\langle X, \leq \rangle$ be a preordered set and define $\mathbf{C}_X$ to be the category

(i). with collection of objects $\mathrm{Obj}(\mathbf{C}_X) := X$;
(ii). with morphism set $\mathrm{Mor}_{\mathbf{C}_X}(x, y)$ taken to be a singleton iff $x \leq y$ and empty otherwise—in the case that $x \leq y$, let us write $x \to y$ for the unique element of $\mathrm{Mor}_{\mathbf{C}_X}(x, y)$;
(iii). with composition defined by $(y \to z) \circ (x \to y) := x \to z$; and
(iv). with identity $\mathrm{id}_x := x \to x$.

Exercise B.1.9 Check that $\mathbf{C}_X$ is in fact a category.

R Note how the axiom of reflexivity corresponds to the identities and the axiom of transitivity corresponds to composition.

B.2 Some basic concepts

The real reason we introduce the definition of a category in notes like these is that it allows us to introduce consistent notation and terminology throughout the text. Had we forgone even the very basics of categories, we would still be able to do the same mathematics, but the notation and terminology would be much more ad hoc.

Definition B.2.1 — Domain and codomain Let $f\colon A \to B$ be a morphism in a category. Then, the ***domain*** of f is A and the ***codomain*** of f is B.

R Of course, these terms generalize the notions of domain and codomain for sets.

Definition B.2.2 — Endomorphism Let $\mathbf{C}$ be a category and let $A \in \mathrm{Obj}(\mathbf{C})$. Then, an ***endomorphism*** is a morphism $f \in \mathrm{Mor}_{\mathbf{C}}(A, A)$. We write $\mathrm{End}_{\mathbf{C}}(A) \coloneqq \mathrm{Mor}_{\mathbf{C}}(A, A)$ for the collection of endomorphisms on A.

R In other words, "endomorphism" is just a fancy name for a morphism with the same domain and codomain.

Definition B.2.3 — Isomorphism Let $f\colon A \to B$ be a morphism in a category. Then, f is an ***isomorphism*** iff it is invertible, i.e., iff there is a morphism $g\colon B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. In this case, g is an ***inverse*** of

f. The collection of all isomorphisms from A to B is denoted by $\mathrm{Iso}_{\mathbf{C}}(A, B)$.

Exercise B.2.4 Let $f\colon A \to B$ be a morphism in a category and let $g, h\colon B \to A$ be two inverses of f. Show that $g = h$.

R As a result of this exercise, we may denote *the* inverse of f by f^{-1}.[a]

[a] If inverses were not unique, then the notation f^{-1} would be ambiguous: what inverse would we be referring to?

Exercise B.2.5 Show that a morphism in **Set** is an isomorphism iff it is bijective.

Exercise B.2.6 Show that a morphism in **Mag** is an isomorphism iff (i) it is bijective, (ii) it is a homomorphism, and (iii) its inverse is a homomorphism.

Exercise B.2.7 Show that the inverse of a bijective homomorphism of magmas is itself a homomorphism.

R Thus, if you want to show a function is an isomorphism of magmas, in fact you only need to check (i) and (ii) of the previous exercise, because then you get (iii) for free. (Of course, essentially the very same thing happens in **Rg** as well.)

Definition B.2.8 — Isomorphic Let $A, B \in \mathrm{Obj}(\mathbf{C})$ be objects in a category. Then, A and B are ***isomorphic*** iff there is an isomorphism from A to B. In this case, we write $A \cong_{\mathbf{C}} B$, or just $A \cong B$ if the category $\mathbf{C}$ is clear from context.

Exercise B.2.9 Let $\mathbf{C}$ be a category. Show that $\cong_{\mathbf{C}}$ is an equivalence relation on $\mathrm{Obj}(\mathbf{C})$.

Definition B.2.10 — Automorphisms Let $\mathbf{C}$ be a category and let $A \in \mathrm{Obj}(\mathbf{C})$. Then, an ***automorphism*** $f\colon A \to A$ is a morphism which is both an endomorphism and an isomorphism. We write $\mathrm{Aut}_{\mathbf{C}}(A) := \mathrm{Iso}_{\mathbf{C}}(A, A)$ for the collection of automorphisms of A.

R The automorphisms of A are often thought of as the *symmetries* of A.

The following result can be seen as a reason why the concepts of monoid and group are so ubiquitous in mathematics.

Proposition B.2.11 Let $\mathbf{C}$ be a category and let $A \in \mathrm{Obj}(\mathbf{C})$. Then,

(i). $\langle \mathrm{End}_{\mathbf{C}}(A), \circ, \mathrm{id}_A \rangle$ is a monoid; and
(ii). $\langle \mathrm{Aut}_{\mathbf{C}}(A), \circ, \mathrm{id}_A, -^{-1} \rangle$ is a group.

Proof. We leave this as an exercise.

Exercise B.2.12 Prove this yourself.

■

Finally, we end this section with a concrete example of isomorphism.

▪ **Example B.2.13** The category we work in is **Grp**. Thus, we are going to present an example of two different groups which are isomorphic in **Grp**.

On one hand, we have $\langle \mathbb{Z}/2\mathbb{Z}, +, 0, - \rangle$, which if you have been reading along in the appendix, should be relatively familiar to you by now.[a]. Regardless, however, we list the

addition table for $\mathbb{Z}/2\mathbb{Z}$ for absolute concreteness.

$+$	0	1
0	0	1
1	1	0

(B.2.14)

On the other hand, let's define a group you haven't seen before, $C_2 \coloneqq \{1, -1\}$ with binary operation defined by

$\cdot$	1	-1
1	1	-1
-1	-1	1

. (B.2.15)

(Feel free to check that this does indeed satisfy the axioms of a group (in fact, commutative group) if you like, but this is not so crucial .)

Now, the key to notice is the following: aside from a relabeling of symbols, *the tables in* (B.2.14) *and* (B.2.15) *are identical*. Explicitly, the relabeling is $0 \mapsto 1$, $1 \mapsto -1$, and $+ \mapsto \cdot$. The precise way of saying this is: the function $\phi\colon \mathbb{Z}/2\mathbb{Z} \to C_2$ defined by $\phi(0) \coloneqq 1$ and $\phi(1) \coloneqq -1$ *is an isomorphism in* **Grp** (or, to say the same thing in slightly different language, *is an isomorphism of groups*).

While not always literally true, depending on your category, I think at an intuitive level it is safe to think of two objects that are isomorphic as being 'the same' up to a relabeling of the elements. This is why, in mathematics, it is very common to not distinguish between objects which are isomorphic. This would be like making a distinction between the two equations $x^2 + 5x - 3 = 0$ and $y^2 + 5y - 3 = 0$ in elementary algebra: the name of the variable in question doesn't have any serious effect on the mathematics—it's just a name.

[a] Note that, we can regard $\mathbb{Z}/2\mathbb{Z}$ as a ring, explicitly $\langle \mathbb{Z}/2\mathbb{Z}, +, 0, -, \cdot \rangle$, but we don't. We're *forgetting* about the extra binary operation, and upon doing so, we obtain the group $\langle \mathbb{Z}/2\mathbb{Z}, +, 0, - \rangle$.

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

We end this subsection with relatively tricky concepts, that of *embedding* and *quotient*. Roughly speaking, you might say that "embedding" is the categorical generalization of the concept of a subset. In a general category with objects A and B, the statement $A \subseteq B$ just doesn't make sense—we need A and B to be sets to even posit the question "Is A a subset of B?". But even in concrete categories, where $A \subseteq B$ *does* make sense, simply being a subset of an object is the 'wrong' notion—see Example B.2.17. The basic idea which we want to make precise then is that, in addition to A being a subset of B, the structure on A is somehow the structure 'inherited' from B.

The first thing to realize is that if we are to be categorical about things (by which I mean that the *morphisms* are to play a central role), is that we shouldn't try to generalize the concept of "subset" to objects, but rather, to morphisms. That is to say, the objective should be to figure out what it means for a *morphism* to be an embedding. So, let $f\colon A \to B$ be a morphism in a concrete category.[2] In order to be an embedding, f has to be at the very least an embedding of the underlying sets, that is, f should be injective. We need more than this however: if C is another object 'contained' in A, by which I mean there is a morphism $g\colon C \to A$, then, just as I can consider a subset of a subset as a subset,[3] if f is to be an embedding, I should be able to consider C directly as being 'contained' in B, that is, $f \circ g$ should be a morphism as well. This is made precise with the following definition (as well as the 'dual' concept of *quotient*).

Definition B.2.16 — Embedding and quotient Let $\mathbf{C}$ be a concrete category, let $A, B \in \mathrm{Obj}(\mathbf{C})$, and let $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$.

[2] We take our category to be concrete because, to the best of my knowledge, there is no definition of embedding/quotient that is satisfactory for all (not-necessarily-concrete) categories.

[3] That is, if X is a subset of Y and Y is a subset of Z, then of course I can consider X as a subset of Z as well.

(i). f is an ***embedding*** iff f is injective and whenever a function $g\colon C \to A$ is such $f \circ g \in \mathrm{Mor}_{\mathbf{C}}(C, B)$ (with $C \in \mathrm{Obj}(\mathbf{C})$), it follows that $g \in \mathrm{Mor}_{\mathbf{C}}(C, A)$.

(ii). f is a ***quotient*** iff f is surjective and whenever a function $g\colon B \to C$ is such that $g \circ f \in \mathrm{Mor}_{\mathbf{C}}(A, C)$ (with $C \in \mathrm{Obj}(\mathbf{C})$), it follows that $g \in \mathrm{Mor}_{\mathbf{C}}(B, C)$.

Now that we have the precise definition in hand, we can *prove* that being an injective morphism is not enough.

▪ **Example B.2.17 — A nondecreasing injective function that is not an embedding** Define $X := \{A, B\}$ equipped with the trivial partial-order[a] and define $Y := \{1, 2\}$ with the only nontrivial relation being $1 \leq 2$.

Define $f\colon X \to Y$ by $f(A) := 1$ and $f(B) := 2$. If $x_1 \leq x_2$ in X, then in fact we must have that $x_1 = x_2$ (because it's the trivial order), and so of course $f(x_1) \leq f(x_2)$ (in fact, we have equality. Thus, f is nondecreasing. It is also certainly injective (in fact, bijective).

We wish to show that f is not an embedding. Define $g\colon Y \to X$ by $g(A) := 1$ and $g(B) := 2$. Then, $f \circ g = \mathrm{id}_Y$ is certainly nondecreasing (i.e. a morphism in **Pre**), but yet g is not nondecreasing. Hence, f is not an embedding.

R Though you may be able to follow the proof, it's also important to understand why f *shouldn't* be an embedding. That is to say, while it may be true that our definition has the property that f is not an embedding, furthermore, any definition we might have come up with should have this property. The reason is that, if you consider X as a subset of Y (via f), then the order on Y would dictate that $A \leq B$ (because $f(A) \leq f(B)$), which is not the case. In this case, the 'structure' on X is *not* that inherited from Y via f.

[a] That is, $A \leq A$, $B \leq B$, and nothing else.

On the other hand, we do have the following.

Exercise B.2.18 Let **C** be either the category **Set**, **Rg**, or **Mag**.

(i). Show that a morphism in **C** is an embedding iff it is injective.

(ii). Show that a morphism in **C** is a quotient iff it is surjective.

Exercise B.2.19

(i). Show that a morphism f in **Pre** is an embedding iff it is injective and has the property that $f(x_1) \leq f(x_2)$ iff $x_1 \leq x_2$.

(ii). Show that a morphism f in **Pre** is a quotient iff it is surjective and has the property that $f(x_1) \leq f(x_2)$ iff $x_1 \leq x_2$.

B.3 Functors and natural-transformations

B.3.1 Functors

The motivating idea behind the definition of a category is we wanted a definition that would contain the data of both the objects under study and the *morphisms* which 'preserve' the relevant structure.[4] We've just now introduced a new type of object, namely, a category, and so now what might ask "What is the 'right' notion of morphisms between categories?". Well, looking back at the definition (Definition B.1.1), we see that there are four pieces of data (I) the objects, (II) the morphisms, (III) the composition, and (IV) the identity morphisms. One thus comes up with the following definition of a 'morphism of categories', what is called a *functor*.

[4]Of course, any choice of morphisms can work so long as they satisfy the axioms, but most of the examples we're interested in the morphisms will be taken to be the ones which "preserve" the structure, and furthermore, when dealing with general abstract categories, I find this to be my guiding intuition.

Definition B.3.1.1 — Functor Let $\mathbf{C}$ and $\mathbf{D}$ be categories. A ***functor*** is

(I). a function $\mathbf{f}\colon \mathrm{Obj}(\mathbf{C}) \to \mathrm{Obj}(\mathbf{D})$; together with
(II). for every $A, B \in \mathrm{Obj}(\mathbf{C})$, a function[a]

$$\mathbf{f}\colon \mathrm{Mor}_{\mathbf{C}}(A, B) \to \mathrm{Mor}_{\mathbf{D}}(\mathbf{f}(A), \mathbf{f}(B)) \qquad \text{(B.3.1.2)}$$

such that

(i). $\mathbf{f}(g \circ f) = \mathbf{f}(g) \circ \mathbf{f}(f)$ for all composable morphisms $f, g \in \mathrm{Mor}_{\mathbf{C}}$; and
(ii). $\mathbf{f}(\mathrm{id}_A) = \mathrm{id}_{\mathbf{f}(A)}$ for all $A \in \mathrm{Obj}(\mathbf{C})$.

R Thus, a functor between two categories maps the objects to objects and the morphisms to the morphisms, and does so in such a way so as to "preserve" composition and the identities.

[a] Of course, this function depends on A and B, but by abuse of notation we omit this dependence.

▪ **Example B.3.1.3 — The category of categories** The category of categories is the category $\mathbf{Cat}$

(i). whose collection of objects $\mathrm{Obj}(\mathbf{Cat})$ is the collection of all categories;
(ii). with morphism set $\mathrm{Mor}_{\mathbf{Cat}}(\mathbf{C}, \mathbf{D})$ precisely the set of all functors from $\mathbf{C}$ to $\mathbf{D}$;
(iii). whose composition is given by ordinary function composition of both the functions on objects and morphisms;
(iv). and whose identities are given by the functors for which both the functions on objects and morphisms is the identity function.

R Okay, so I won't blame you if you think this is total nonsense. "Category of categories"? That's just asking for some sort of paradox. The answer to this of course is that we're being sloppy.

You'll recall during our discussion of Russell's Paradox (around (A.1.1)), we explained that our method of resolving the paradox was to fix some set U, the "universe", that satisfied certain properties which made it reasonable to do "all of mathematics" inside U. Russel's Paradox was then resolved by concluding that the set in question simply was just not an element of U.

Something nearly identity is going on here. Implicitly, we pick a smallest "universe" we wish to work in U_0. Then, whenever we say something like "the category of all rgs", it is implicit that all those rgs are coming from U_0. Doing this will usually result in categories that are themselves not contained in U_0, but rather, a larger universe U_1. Then, when we form "the category of all categories", it is implicit that all our categories are coming from U_1. And again, the resulting category will not be in U_1. But so what. 99% of the time, that doesn't matter. Yes, yes, technically we should be saying "The category of all categories in U_1.", but you can see how that would get really annoying really fast, and as it will never matter for us, we are sloppy.[a]

[a] And also give this remark because we feel guilty about being sloppy.

When I think of functors intuitively, I think of them as some sort of mathematical "constructions", something that takes in objects of **C** and spits out objects of **D**. For example, the entire subject of algebraic topology originated as studying "constructions" that associate algebraic objects (like groups) to "geometric" objects (like topological spaces). Unfortunately, our limited background gives us a limited supply of examples, but we do have some things.

▪ **Example B.3.1.4 — The power-set functor** Consider the functor **Set** $\to$ **Pos** from the category of sets to the category of partially-ordered sets defined by

$$\mathrm{Obj}(\mathbf{Set}) \ni X \mapsto \langle 2^X, \subseteq \rangle \in \mathrm{Obj}(\mathbf{Pos}) \qquad \text{(B.3.1.5a)}$$

$$\mathrm{Mor}_{\mathbf{Set}}(X, Y) \ni f \mapsto f \in \mathrm{Mor}_{\mathbf{Pos}}(2^X, 2^Y), \qquad \text{(B.3.1.5b)}$$

where $f \in \mathrm{Mor}_{\mathbf{Pos}}(2^X, 2^Y)$ is the function that sends $S \subseteq X$ to $f(Y) \subseteq Y$.

Exercise B.3.1.6 Check that this defines a functor.

The next example we would like to consider is the *dual-space* functor $V \mapsto V^\dagger$ on the category of vector spaces. Unfortunately, however, we run into a bit of a problem when trying to do this naively. This functor on objects acts as $V \mapsto V^\dagger$, and so naturally on morphisms this functor acts as $T \mapsto T^\dagger$. The definition of a functor, however, requires that, if $T \in \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V, W)$, then $T^\dagger \in \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V^\dagger, W^\dagger)$. But it's not. $T^\dagger$ is not a map from $V^\dagger$ to $W^\dagger$, but rather, a map from $W^\dagger$ to $V^\dagger$. We get around this little hiccup by defining the *opposite category*.

Definition B.3.1.7 — Opposite category Let $\mathbf{C}$ be a category. Then, the ***opposite category*** of $\mathbf{C}$, $\mathbf{C}^{\mathrm{op}}$, is defined by

(I). $\mathrm{Obj}(\mathbf{C}^{\mathrm{op}}) := \mathrm{Obj}(\mathbf{C})$;
(II). for $A, B \in \mathrm{Obj}(\mathbf{C}^{\mathrm{op}})$,

$$\mathrm{Mor}_{\mathbf{C}^{\mathrm{op}}}(A, B) := \mathrm{Mor}_{\mathbf{C}^{\mathrm{op}}}(B, A); \tag{B.3.1.8}$$

(III). for $f, g \in \mathrm{Mor}_{\mathbf{C}^{\mathrm{op}}}$ composable,

$$f \circ_{\mathrm{op}} g := g \circ f; \tag{B.3.1.9}$$

and
(IV). for $A \in \mathrm{Obj}(\mathbf{C}^{\mathrm{op}})$, $\mathrm{id}_A := \mathrm{id}_A$.

R In brief, $\mathbf{C}^{\mathrm{op}}$ has the same objects as $\mathbf{C}$, but the morphisms go in the *opposite* direction.

Such a construction might seem a bit silly, but it allows us to make the following convenient definition.

Definition B.3.1.10 — Cofunctor Let $\mathbf{C}$ and $\mathbf{D}$ be categories. Then, a ***cofunctor*** from $\mathbf{C}$ to $\mathbf{D}$ is a functor $\mathbf{C}^{\mathrm{op}} \to \mathbf{D}$.

R We will often write things like "Let $\mathbf{f}\colon \mathbf{C} \to \mathbf{D}$ be a cofunctor. . . ". Strictly speaking, the domain category is $\mathbf{C}$, not $\mathbf{C}^{\mathrm{op}}$, but this notation is convenient for what will eventually be obvious reasons.

R This is more commonly referred to as a ***contravariant functor*** (in which case an 'ordinary' functor is called a ***covariant functor*** for contrast). I actually think this is pretty terrible terminology as in pretty much every other context in mathematics something with the prefix "co" is the "dual" thing, not the 'primary' thing.

Proposition B.3.1.11 Let $\mathbf{C}$ and $\mathbf{D}$ be categories, let $\mathbf{f}\colon \mathrm{Obj}(\mathbf{C}) \to \mathrm{Obj}(\mathbf{D})$ be a function, and for every $A, B \in \mathrm{Obj}(\mathbf{C})$ let $\mathbf{f}\colon \mathrm{Mor}_{\mathbf{C}}(A, B) \to \mathrm{Mor}_{\mathbf{D}}(\mathbf{f}(B), \mathbf{f}(A))$ be a function. Then, this defines a cofunctor iff

(i). $\mathbf{f}(g \circ f) = \mathbf{f}(f) \circ \mathbf{f}(g)$ for all composable morphisms $f, g \in \mathrm{Mor}_{\mathbf{C}}$; and
(ii). $\mathbf{f}(\mathrm{id}_A) = \mathrm{id}_{\mathbf{f}(A)}$.

R Note that this is exactly the same as the definition of a functor (Definition B.3.1.1), except here the requirement is $\mathbf{f}(g \circ f) = \mathbf{f}(f) \circ \mathbf{f}(g)$ (instead of $\mathbf{f}(g \circ f) = \mathbf{f}(g) \circ \mathbf{f}(f)$). In this sense, cofunctors are just functors which 'flip' the order of composition.

Proof. We leave this as an exercise.

Exercise B.3.1.12 Prove the result.

■

With this language in hand, we can now return to what is probably the most relevant example for us.

▪ **Example B.3.1.13 — Dual-space** Let $\mathbb{K}$ be a cring and consider the *co*functor $\mathbb{K}$-**Mod** $\to$ $\mathbb{K}$-**Mod** defined by

$$\mathrm{Obj}(\mathbb{K}\text{-}\mathbf{Mod}) \ni V \mapsto V^\dagger \in \mathrm{Obj}(\mathbb{K}\text{-}\mathbf{Mod})$$
$$\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(V,W) \ni T \mapsto T^\dagger \in \mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Mod}}(W^\dagger, V^\dagger)$$

Exercise B.3.1.15 Check that this defines a functor.

B.3.2 Natural-transformations

We can compose the dual-space functor with itself to obtain the "double-dual-space" functor $V \mapsto [V^\dagger]^\dagger$. Recall that (Theorem 5.2.1.11), for every $\mathbb{K}$-module V, we actually have a linear-transformation $V \to [V^\dagger]^\dagger$, and in fact, this is an isomorphism in the context of finite-dimensional vector spaces.

On the other hand, if V is a finite-dimensional vector space, then so is $V^\dagger$. Furthermore, they have the same dimension, and hence are isomorphic.[5] The isomorphisms $V \cong V^\dagger$ and $V \cong [V^\dagger]^\dagger$ are fundamentally different, however. The latter is what is called a *natural isomorphism*. To see more clearly how these isomorphisms are different, let us recall more explicitly what they are.

First of all, the map $V \to [V^\dagger]^\dagger$ is given by

$$v \mapsto \langle \cdot, v \rangle. \tag{B.3.2.1}$$

On the other hand, the isomorphism $V \to V^\dagger$ is more complicated. Let $\{b_1, \ldots, b_d\}$ be a basis for V, so that the dual basis $\{b_1^\dagger, \ldots, b_d^\dagger\}$ is a basis for $V^\dagger$. Then,

$$V \ni \alpha_1 \cdot b_1 + \cdots + \alpha_d \cdot b_d \mapsto \alpha_1 \cdot b_1^\dagger + \cdots + \alpha_d \cdot b_d^\dagger \in V^\dagger \tag{B.3.2.2}$$

is an isomorphism. The significant thing to note here is that the definition of this morphism *depended on an arbitrary choice* of a basis for V.

[5] Because they are both isomorphic to $\mathbb{K}^d$ by taking coordinates (after choosing bases).

Thus, in order to define the morphism $V \to V^\dagger$ for every vector space V, you'll have to pick a basis for every single vector space, and there is no single "natural" way to do so. The isomorphisms that I happen to use are almost certainly going to be different than the ones you choose to use. On the other hand, there is *no choice* when it comes to the isomorphism $V \to [V^\dagger]^\dagger$. Intuitively, this isomorphism doesn't depend on V, the same definition works for every vector space, whereas the isomorphisms $V \to V^\dagger$ do depend on V.

The precise notion which distinguishes these two is that of a *natural transformation*: $V \to [V^\dagger]^\dagger$ will be a natural isomorphism, whereas $V \to V^\dagger$ will not be.

Definition B.3.2.3 — Natural-transformation Let $\mathbf{C}$ and $\mathbf{D}$ be functors, and let $\mathbf{f}, \mathbf{g} \colon \mathbf{C} \to \mathbf{D}$ be functors. Then, a ***natural transformation*** from $\mathbf{f}$ to $\mathbf{g}$ is, for every $A \in \mathrm{Obj}(\mathbf{C})$, a morphism $\eta_A \colon \mathbf{f}(A) \to \mathbf{f}(B)$, such that

$$\begin{array}{ccc} \mathbf{f}(A) & \xrightarrow{\mathbf{f}(f)} & \mathbf{f}(B) \\ {\scriptstyle \eta_A}\downarrow & & \downarrow{\scriptstyle \eta_B} \\ \mathbf{g}(A) & \xrightarrow[\mathbf{g}(f)]{} & \mathbf{g}(B) \end{array} \tag{B.3.2.4}$$

commutes for every morphism $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$ and $A, B \in \mathrm{Obj}(\mathbf{C})$.

R A *diagram* in this sense of the word refers to a set of objects and morphisms between them indicated by drawing arrows for each morphism (from the domain to the codomain). A path from one object to another (in the direction indicated by the arrows) then corresponds to the composition of the corresponding morphisms. If you select any two objects in a given diagram, in general, there will be more than one path from the first to the second; the diagram is said to *commute* iff all corresponding compositions agree.

For example, in this case, the phrase "the following diagram commutes" should be understood as shorthand for the statement "$\mathbf{g}(f) \circ \eta_A = \eta_B \circ \mathbf{f}(f)$".

R The entire natural-transformation is usually just denoted "η", in which case η_A is referred to as the ***component*** of η at A.

R Admittedly, this definition is difficult to understand at first sight. For one thing, it's not clear how this captures "doesn't depend on A/B". I will do the best I can to explain.

The idea is that, if I can define the morphisms η_A in such a way that doesn't make use of anything special to this particular A, then it shouldn't matter whether I 'go to a different object' and then apply the morphism, or if I first apply the morphism and then "go to a different object". (Here, "going to a different object" corresponds to $\mathbf{f}(f)$ and $\mathbf{g}(f)$, and "the morphism" refers to η_A and η_B.)

It turns out that, in the following sense, natural-transformations should themselves be thought of as *morphisms of functors*.

Definition B.3.2.5 — Category of functors Let $\mathbf{C}$ and $\mathbf{D}$ be categories. Then, the ***category of functors*** from $\mathbf{C}$ to $\mathbf{D}$, $\mathrm{Mor}_{\mathbf{Cat}}(\mathbf{C}, \mathbf{D})$, is defined by

(I). $\mathrm{Obj}\left(\mathrm{Mor}_{\mathbf{Cat}}(\mathbf{C}, \mathbf{D})\right) := \mathrm{Mor}_{\mathbf{Cat}}(\mathbf{C}, \mathbf{D})$;
(II). $\mathrm{Mor}_{\mathrm{Mor}_{\mathbf{Cat}}(\mathbf{C},\mathbf{D})}(\mathbf{f}, \mathbf{g})$ is the collection of natural-transformations from $\mathbf{f}$ to $\mathbf{g}$;
(III). composition of natural-transformations is defined componentwise; and
(IV). $[\mathrm{id}_{\mathbf{f}}]_A := \mathrm{id}_A$.

R Thus, the objects are functors, the morphisms are the natural-transformations, composition is done the way you would expect (componentwise), and the identity on $\mathbf{f} \in \mathrm{Obj}\left(\mathrm{Mor}_{\mathbf{Cat}}(\mathbf{C}, \mathbf{D})\right)$ is the natural-transformation whose component as the object $A \in \mathbf{C}$ is id_A.

R We are abusing notation and using $\mathrm{Mor}_{\mathbf{Cat}}(\mathbf{C}, \mathbf{D})$ to denote the collection of functors from $\mathbf{C}$ to $\mathbf{D}$ as well as the corresponding category.

As in every category, we have a notion of isomorphism. In the case of categories of functors, the following term is used.

Definition B.3.2.6 — Natural-isomorphism Let $\eta\colon \mathbf{f} \to \mathbf{g}$ be a natural-transformation of functors $\mathbf{f}, \mathbf{g}\colon \mathbf{C} \to \mathbf{D}$. Then, η is a ***natural-isomorphism*** iff η is an isomorphism in $\mathrm{Mor}_{\mathbf{Cat}}(\mathbf{C}, \mathbf{G})$.

R If we're thinking of functors as some sort of mathematical 'constructions' (e.g. taking the dual of a vector space), then, intuitively speaking, saying that "$\mathbf{f}$ is naturally-isomorphic to $\mathbf{g}$" is saying more than just "$\mathbf{f}(A)$ is isomorphic to $\mathbf{g}(A)$ for all $A \in \mathrm{Obj}(\mathbf{C})$", but rather that the entire "constructions" $A \mapsto \mathbf{f}(A)$ and $A \mapsto \mathbf{g}(A)$ are isomorphic.

Fortunately, this is equivalent to what you would hope.

Proposition B.3.2.7 Let $\eta\colon \mathbf{f} \to \mathbf{g}$ be a natural-transformation of functors $\mathbf{f}, \mathbf{g}\colon \mathbf{C} \to \mathbf{D}$. Then, η is a natural-isomorphism iff $\eta_A\colon \mathbf{f}(A) \to \mathbf{g}(A)$ is an isomorphism for all $A \in \mathrm{Obj}(\mathbf{C})$.

Proof. We leave this as an exercise.

Exercise B.3.2.8 Prove the result.

■

We now finally return to the example of primary interest.

▪ **Example B.3.2.9 —** $V \to [V^\dagger]^\dagger$ Let $\mathbb{K}$ be a cring and consider the linear-transformation $\eta_V\colon V \to [V^\dagger]^\dagger$ defined by $v \mapsto \langle \cdot, v\rangle$.

Exercise B.3.2.10 Show that this is a natural-transformation.

Thus, by Theorem 5.2.1.11, it is in fact a natural-isomorphism in the category of finite-dimensional vector spaces.

C. Results from ring theory

Linear algebra is the study of vector spaces, which themselves are just $\mathbb{F}$-modules for $\mathbb{F}$ a division ring. Thus, it should be expected, and is in fact the case, that some basic results about ring theory are used throughout the main text. In order to avoid interrupting the flow with long tangents on not linear algebra, we have relegated most of these results to this appendix.

C.1 Prerequisites

In this section, we present a miscellany of results used in the sections to come. You might consider skipping it for now and coming back as the results are referenced.

Definition C.1.1 — Kernel (of a ring homomorphism) Let $\phi\colon R \to S$ be a ring homomorphism. Then, the ***kernel***, $\mathrm{Ker}(\phi)$, is defined by

$$\mathrm{Ker}(\phi) \coloneqq \{x \in R : \phi(x) = 0\}. \tag{C.1.2}$$

Proposition C.1.3 Let $\phi\colon R \to S$ be a ring homomorphism. Then, $\mathrm{Ker}(\phi) \subseteq R$ is an ideal.

R Warning: Unlike the case of modules, it is *not* the case in general that $\mathrm{Im}(\phi) \subseteq S$ is an ideal. That said, see the following result.

Proof. We leave this as an exercise.

Exercise C.1.4 Prove the result.

■

Proposition C.1.5 Let $\phi\colon R \to S$ be a ring homomorphism. Then,

(i). the preimage under ϕ of a subring of S is a subring of ϕ;
(ii). the preimage under ϕ of an ideal of S is an ideal of R;
(iii). the image under ϕ of a subring of R is a subring of S; and
(iv). the image under ϕ of every ideal of R is an ideal of S iff ϕ is surjective.Then, $\mathrm{Im}(\phi) \subseteq S$ is a subring.

Proof. We leave this as an exercise.

Exercise C.1.6 Prove the result.

■

Exercise C.1.7 Give an example of a ring homomorphism $\phi\colon R \to S$ for which $\phi(S) \subseteq R$ is *not* an ideal.

By and large, we're going to only be working with *two-sided* ideals. A "two-sided ideal" is just an ideal in the sense you (hopefully) learned back in Definition A.4.1.13. The "two-sided" is used for emphasis to distinguish between *left* and *right* sided ideals.

Definition C.1.8 — Left and right ideals Let R be a ring and let $I \subseteq R$. Then, I is a ***left (resp. right) ideal*** iff it is a submodule of R regarded as a left (resp. right) module over itself.

R See Example 1.1.17 to recall exactly what we are referring to when we regard a ring as a module over itself. It's not hard—for example, when we say that "$\mathbb{R}$ is a one-dimensional vector space over itself" we're thinking of $\mathbb{R}$ as a module over itself.

Proposition C.1.9 Let R be a ring and let $I \subseteq R$.

(i). I is a left ideal iff (i) it is a subrng and (ii) $r \in R$ and $i \in I$ implies that $r \cdot i \in I$.

(ii). I is a right ideal iff (ii) it is a subrng and (ii) $r \in R$ and $i \in I$ implies that $i \cdot r \in I$.

R Warning: Note that it is not a subring! Indeed, you should check that ideals (of any type) contain the multiplicative identity iff they are all of R.

R Note that this is an exact analogue of what we say in the two-sided case (Exercise A.4.1.16)—in addition to being a subrng, you have respectively left and right "absorption" properties.

Proof. We leave this as an exercise.

Exercise C.1.10 Prove the result.

R Hint: This is no more difficult than just applying the submodule criterion (Proposition 1.2.1.2) to the left (resp. right) module R.

■

Proposition C.1.11 — Product of ideals Let R be a ring and let $I, J \subseteq R$ be ideals. Then, the ***product*** of I and J, IJ, defined by

$$IJ := \left\{ \sum_{k=1}^{m} x_k y_k : m \in \mathbb{N}, x_k \in I, y_k \in J \right\}, \qquad \text{(C.1.12)}$$

is an ideal.

R For $n \in \mathbb{N}$, we define

$$I^n := \underbrace{I \cdots I}_{n} \qquad \text{(C.1.13)}$$

(as well as $I^0 := R$). Note how this is *not* the same as $\left\{ \sum_{k=1}^{m} x_k^n : m \in \mathbb{N}, x_k \in I \right\}$, which is in general smaller.

R For noncommutative rings, there are also notions of left and right ideals,[a] in which case one might refer to what we have been simply calling "ideals" as "two-sided ideals" for emphasis. While certainly some of the things we do could be adapted for the one-sided versions, throughout, "ideal" should be interpreted as meaning "two-sided ideal".

[a] Well, the notions exist in the commutative case as well, but there all three notions coincide.

Proof. We leave this as an exercise.

Exercise C.1.14 Prove the result.

■

Proposition C.1.15 — Generated ideal Let $\mathbb{K}$ be a ring and let $S \subseteq \mathbb{K}$ be a subset. Then, there is a unique ideal (S), the ideal ***generated*** by S, such that

(i). $S \subseteq (S)$; and
(ii). if I is any other ideal containing S, it follows that $S \subseteq (S)$.

Furthermore, explicitly,

$$(S) = \left\{ \sum_{s \in S} x_s s y_s : x_s, y_s \in \mathbb{K} \right\} =: \mathbb{K}S\mathbb{K}. \tag{C.1.16}$$

R If $S =: \{s_1, \ldots, s_m\}$ is finite, people typically write

$$(s_1, \ldots, s_m) := (()S). \tag{C.1.17}$$

Proof. We leave this as an exercise.

Exercise C.1.18 Prove the result.

■

Theorem C.1.19 — Krull's Theorem. Let R be a ring and let $I \subseteq R$ be a proper ideal. Then, there is a maximal ideal $M \subseteq R$ containing I.

Proof. We leave this as an exercise.

Exercise C.1.20 Prove the result.

R Hint: Zorn's Lemma.

■

Definition C.1.21 — Principal ideal ring Let R be a ring. Then, R is a ***left (resp. right, resp. two-sided) principal ideal***

ring iff every nonzero left (resp. right, resp. two-sided) ideal is generated by a single element.

R It is much more common to see this condition stated only in the case where it is already assumed that R is an integral domain, in which case people say ***principal ideal domain***. Without question, this term is far more common than "principal ideal ring", though of course it would be inappropriate if R isn't actually an integral domain.

R "Principal ideal domain" is often abbreviated to ***PID***. It thus seems appropriate to abbreviate "principal ideal ring" to ***PIR***.

R The primary example we have in mind are polynomial rings—see Proposition C.3.2.8.

R The zero ideal is generated by the empty-set, which of course doesn't have a single element, it has no elements—that's what "empty" means.

Proposition C.1.22 Let R be a ring. Then, if R is a left or right PIR, then R is a two-sided PIR.

Proof. Suppose that R is a left or right PIR. Without loss of generality, suppose that R is a left PIR. Let $I \subseteq R$ be a two-sided ideal. Then, I is in particular a left ideal, and so as R is a left PIR, there is some $x \in R$ such that $I = Rx$. However, as I is two-sided, $RxR = IR = I$, and hence x generates I as a two-sided ideal as well. ■

C.2 Ideals and their quotients

The primary goal of this section is to prove the "dictionary" Theorem C.2.4.1 that establishes a correspondence between properties of ideals I and properties of their quotients R/I. We begin with a

discussion of relatively intuitive properties one might like a ring to have (one of which we have already encountered). For reasons that won't be particularly apparent to us given our limited discussion, these properties, while more intuitive, are arguably not the 'correct' notion in the noncommutative setting. We thus introduce variants of these properties more suited to the noncommutative setting and check that they agree with the first definition if the ring is commutative. To state these definitions, however, we must first define the corresponding properties of ideals. Finally, we prove the dictionary itself.

C.2.1 Some properties of rings

As mentioned previously, all of the definitions given here come with the tiny caveat that they are arguably not the best definition, at least for noncommutative rings.

We have already defined what it means for a ring to be a *division ring* (Definition A.4.23) and to be *integral* (Definition A.4.22). We reproduce the definitions here both for convenience and to stress it's relationship to the properties of reduced (Definition C.2.1.3) and hyper-connected (Definition C.2.1.4).

Definition C.2.1.1 — Division ring Let R be a ring. Then, R is a ***division ring*** iff every element of R has a multiplicative inverse.

Definition C.2.1.2 — Integral ring Let R be a ring. Then, R is ***integral*** iff $xy = 0$ implies $x = 0$ or $y = 0$.

Definition C.2.1.3 — Reduced ring Let R be a ring. Then, R is ***reduced*** iff $x^m = 0$, $m \in \mathbb{N}$, implies $x = 0$.

R In other words, R is reduced iff the only nilpotent element is 0.

Definition C.2.1.4 — Hyper-connected ring Let R be a ring. Then, R is ***hyper-connected*** iff whenever $xy = 0$ and

one of these elements is nonzero it follows that the other element is nilpotent.

R The name comes from the fact that the Zariski topology on the spectrum is hyper-connected[a] iff R is hyper-connected (for R commutative).

[a] Or *irreducible*, in algebraic geometer parlance.

Proposition C.2.1.5 Let R be a ring.

(i). If R is a division ring, then it is integral.
(ii). R is integral iff it is reduced and hyper-connected.

R One can interpret this as saying that a ring can fail to be integral in one of two ways: it can have nonzero nilpotents or it can fail to be hyper-connected. The definition of hyper-connected given above is superficially quite unintuitive. I tend to think of it as "That property you need together with reducedness to guarantee the ring be integral.".

Proof. We leave this as an exercise.

Exercise C.2.1.6 Prove the result.

■

C.2.2 Some properties of ideals

Definition C.2.2.1 — Maximal ideal Let R be a ring and let $I \subseteq R$ be a proper ideal. Then, I is ***maximal*** iff I is maximal among all proper ideals with respect to the partial-order of inclusion.

Definition C.2.2.2 — Prime ideal Let R be a ring and let $I \subseteq R$ be a proper ideal. Then, I is ***prime*** iff $JK \subseteq I$, $J, K \subseteq R$ ideals, implies $J \subseteq I$ or $K \subseteq I$.

R The name comes from the fact that $\mathbb{Z}p \subseteq \mathbb{Z}$ is a prime ideal iff $p \in \mathbb{Z}$ is prime in the classical sense of the word ($p = 0$ being an exception—$0 \subseteq \mathbb{Z}$ is a prime ideal but $0 \in \mathbb{Z}$ is not usually considered a prime integer).

R You can remember that R itself is excluded from being prime because it is excluded from being maximal (if it weren't, then it would be the only maximal ideal). Indeed, $I = R$ is excluded from this entire list of classes of ideals, and so making the exclusion in all definitions (instead of just one) is convenient.

Definition C.2.2.3 — Radical ideal Let R be a ring and let $I \subseteq R$ be a proper ideal. Then, I is ***radical*** iff $J^m \subseteq I$, $J \subseteq R$ an ideal and $m \in \mathbb{N}$, implies $J \subseteq I$.

R The name comes from the following result.

R Warning: Some authors instead refer to this concept as that of a ***semiprime ideal***. For such authors, an ideal I is "radical" iff $x^m \in I$ implies $x \in I$. The two definitions agree in case R is commutative, and as far as I can tell, the definition we have given above is the one that is better-behaved in the noncommutative setting, and so it is the one we make use of.[a]

[a] Of course, we could have just called it "semiprime", but I prefer "radical" as this is the more common of the two terms, at least outside of a strictly noncommutative setting.

Theorem C.2.2.4 — Radical of an ideal. Let R be a ring and let $I \subseteq R$ be a proper ideal. Then, there is a unique radical ideal, the ***radical***, $\sqrt{I}$, such that

(i). $I \subseteq \sqrt{I}$ and
(ii). if $J \subseteq R$ is another radical ideal that contains I, then $\sqrt{I} \subseteq J$.

Furthermore, explicitly, we have

$$\sqrt{I} = \bigcap_{\substack{P \subseteq R \text{ prime} \\ I \subseteq P}} P. \tag{C.2.2.5}$$

Proof. We leave this as an exercise.

Exercise C.2.2.6 Prove the result.

R Hint: See [T Y91, Theorem 10.7].

■

Definition C.2.2.7 — Primary ideal Let R be a ring and let $I \subseteq R$ be a proper ideal. Then, I is ***primary*** iff $JK \subseteq I$, $J, K \subseteq R$ ideals, implies that either one of J, K is contained in I or one of J, K is contained in $\sqrt{I}$.

Proposition C.2.2.8 Let R be a ring and let $I \subseteq R$ be an ideal.

(i). If I is maximal, then it is prime.
(ii). I is prime iff it is radical and primary.

Proof. (i) Suppose that I is maximal. Let $J, K \subseteq R$ be ideals such that $JK \subseteq I$. If $J \subseteq I$, we're done. Otherwise, there is some $j \in J \setminus I$. Then, $RjR + I$ is an ideal that properly contains I, and so by maximality, $R = RjR + I$. In particular, there are $a, b \in R$ and $i \in I$ such that $1 = ajb + i$. Let $k \in K$. Then, $k = ajbk + ik \in JK + I \subseteq I + I \subseteq I$. Thus, $K \subseteq I$, and so I is prime.

(ii) ($\Rightarrow$) Suppose that I is prime. We first check that I is radical. So, let $J \subseteq R$ be an ideal and suppose that $J^m \subseteq I$ for some $m \in \mathbb{N}$. We can't have $m = 0$ as I is proper. If $m = 1$, we're done. Otherwise, we can write

$$I \supseteq J^m := JJ^{m-1}, \tag{C.2.2.9}$$

whence we deduce that either $J \subseteq I$ or $J^{m-1} \subseteq I$. In the former case, we are done. In the latter case, we have $J^{m-1} \subseteq I$. Continuing inductively, we eventually find that $J \subseteq I$, and so I is radical. We now check that I is primary. So, let $J, K \subseteq R$ be ideals and suppose that $JK \subseteq I$. If $J \subseteq I$, we're done. Otherwise, $K \subseteq I \subseteq \sqrt{I}$, and we are again done.

($\Leftarrow$) Suppose that I is radical and primary. Let $J, K \subseteq R$ be ideals and suppose that $JK \subseteq I$. If one of J, K is contained in I, we're done. Otherwise, as I is primary, one of J, K is contained in $\sqrt{I}$. Without loss of generality, suppose that $J \subseteq \sqrt{I}$. However, as I is radical, $\sqrt{I} = I$, and hence $J \subseteq I$. Thus, I is prime. ■

Theorem C.2.2.10. Let R be a ring and let I be an ideal. Then, $R \supseteq J \mapsto J/I \subseteq R/I$ is a bijection from the set of ideals of R that contain I and the set of ideals of R/I. Furthermore,

(i). J is maximal iff J/I is maximal;
(ii). J is prime iff J/I is prime;
(iii). J is radical iff J/I is radical; and
(iv). J is primary iff J/I is primary.

Proof. We leave this as an exercise.

Exercise C.2.2.11 Prove the result.

■

C.2.3 Their noncommutative variants

Though we call them the "noncommutative variants", of course they make just as much sense in commutative rings. However, for commutative rings, they coincide (Theorem C.2.3.7) with the more intuitive concepts defined in Appendix C.2.1, and so in that context it's usually preferable to work with the previous definitions.

Definition C.2.3.1 — Simple ring Let R be a nonzero ring. Then, R is ***simple*** iff the only ideals of R are 0 and R itself.

R Warning: This definition is exactly analogous to the definition of a simple module (Definition C.5.1). *However*, there is a notion of semisimple ring and it is *not* analogous to the definition of a semisimple module (Definition C.5.8). Because mathematicians are literally cancer when it comes to developing systematic terminology, the term "semisimple ring" refers to a ring that is semisimple when regarded as a left (equivalently, right) module over itself.

Definition C.2.3.2 — Prime ring Let R be a nonzero ring. Then, R is ***prime*** iff $IJ = 0$, $I, J \subseteq R$ ideals, implies $I = 0$ or $J = 0$.

R Note that this is just the statement that the zero ideal is prime.

Definition C.2.3.3 — Radical ring Let R be a nonzero ring. Then, R is ***radical*** iff $I^m = 0$, $I \subseteq R$ an ideal and $m \in \mathbb{N}$, implies $I = 0$.

R Note that this is just the statement that the zero ideal is radical.

R Warning: Some authors refer to this concept as that of a ***semiprime ring***, essentially because such authors will instead use the term "semiprime ideal" in place of "radical ideal"—see the remark in Definition C.2.2.3.

Definition C.2.3.4 — Primary ring Let R be a nonzero ring. Then, R is ***primary*** iff $IJ = 0$, $I, J \subseteq R$ ideals, implies that either one of I, J is 0 or one of I, J is contained in $\sqrt{0}$.

R Note that this is just the statement that the zero ideal is primary.

R Warning: This terminology seems nonstandard, and in fact, upon looking it up, it seems to conflict with a usage of the term I had never seen before. Oh well.

Proposition C.2.3.5 Let R be a ring.

(i). If R is simple, then it is prime.
(ii). R is prime iff it is radical and primary.

Proof. We leave this as an exercise.

Exercise C.2.3.6 Prove the result.

■

We now check that this definitions do indeed agree with the previous ones in the case that R is commutative.

Theorem C.2.3.7. Let $\mathbb{K}$ be a cring.

(i). $\mathbb{K}$ is simple iff it is a division ring.[a]
(ii). $\mathbb{K}$ is prime iff it is integral.
(iii). $\mathbb{K}$ is radical iff it is reduced.
(iv). $\mathbb{K}$ is primary iff it hyper-connected.

[a] Or, equivalently, a field.

Proof. (i) ($\Rightarrow$) Suppose that $\mathbb{K}$ is simple. Let $x \in \mathbb{K}$ be nonzero. $\mathbb{K}x \subseteq \mathbb{K}$ is then a nonzero ideal, and hence $\mathbb{K}x = \mathbb{K}$. Thus, there is some $y \in \mathbb{K}$ such that $yx = 1$.

($\Leftarrow$) Suppose that $\mathbb{K}$ is a division ring. Let $I \subseteq \mathbb{K}$ be a nonzero ideal. Let $i \in I$ be nonzero. $1 = ii^{-1} \in I$, and so $x = 1x \in I$ for all $x \in \mathbb{K}$, and hence $I = \mathbb{K}$.

(iii) ($\Rightarrow$) Suppose that $\mathbb{K}$ is radical. Let $x \in \mathbb{K}$ and suppose that $x^m = 0$ for some $m \in \mathbb{N}$. It follows that $(\mathbb{K}x)^m = 0$, and so $\mathbb{K}x = 0$, and in particular $x = 0$.

($\Leftarrow$) Suppose that $\mathbb{K}$ is reduced. Let $I \subseteq \mathbb{K}$ be an ideal and suppose that $I^m = 0$ for some $m \in \mathbb{N}$. Let $i \in I$. Them, $i^m = 0$ as $i^m \in I^m$, and so $i = 0$.

(iv) ($\Rightarrow$) Suppose that $\mathbb{K}$ is primary. Let $x, y \in \mathbb{K}$ and suppose that $xy = 0$. It follows that $(\mathbb{K}x)(\mathbb{K}y) = 0$. If $(\mathbb{K}x) = 0$, then in particular $x = 0$, and we're done. Otherwise, we must have that $(\mathbb{K}y)^m = 0$ for some $m \in \mathbb{N}$, and again, in particular, $y^m = 0$.

($\Leftarrow$) Suppose that $\mathbb{K}$ is hyper-connected. Let $I, J \subseteq \mathbb{K}$ be ideals and suppose that $IJ = 0$. If $I = 0$, we're done, so suppose this is not the case. Then, there is some nonzero $i \in I$. For every $j \in J$, we have that $ij = 0$, and so as $i \neq 0$, there is some $m_j \in \mathbb{N}$ such that $j^{m_j} = 0$. Thus, $j \in \sqrt{0}$, and hence $J \subseteq \sqrt{0}$.

(ii) $\mathbb{K}$ is prime iff it is radical and primary (Proposition C.2.3.5) iff it is reduced and hyper-connected (by the previous parts) iff it is integral (Proposition C.2.1.5). ■

C.2.4 The dictionary

We now finish with the ultimate goal of this section.

Theorem C.2.4.1. Let R be a ring and let $I \subseteq R$ be an ideal.

(i). I is maximal iff R/I is simple.
(ii). I is prime iff R/I is prime
(iii). I is radical iff R/I is radical.

(iv). I is primary iff R/I is primary.

R In particular, if $\mathbb{K}$ is commutative, by Theorem C.2.3.7, we have

(i). I is maximal iff $\mathbb{K}I$ is a field.
(ii). I is prime iff $\mathbb{K}/I$ is integral.
(iii). I is radical iff $\mathbb{K}/I$ is reduced.
(iv). I is primary iff $\mathbb{K}/I$ is hyper-connected.

Proof. (i) ($\Rightarrow$) Suppose that I is maximal. Every ideal of R/I is of the form J/I for an ideal $J \subseteq I$ containing I. As I is maximal, there are only two such ideals, I and R. Hence, the only ideals of R/I are $I/I = 0$ and R/I itself. Thus, R/I is simple.

($\Leftarrow$) Suppose that R/I is simple. Let $J \supseteq I$ be a proper ideal. $J/I \subseteq R/I$ is an ideal, and so as R/I is simple, either $J/I = 0$ or $J/I = R/I$. The latter cannot happen as J is proper, and so $J/I = 0$, that is, $J = I$. Hence, I is maximal.

(ii) ($\Rightarrow$) Suppose that I is prime. Let $J/I, K/I \subseteq R/I$ be ideals such that $(J/I)(K/I) = 0$. It follows that $JK \subseteq I$, and hence as I is prime, without loss of generality, $J \subseteq I$, so that $J/I = 0$.

($\Leftarrow$) Suppose that R/I is prime. Let $J, K \subseteq R$ be ideals such that $JK \subseteq I$. It follows that $(J/I)(K/I) = 0$, and hence as R/I is prime, without loss of generality, $J/I = 0$, so that $J \subseteq I$.

(iii) ($\Rightarrow$) Suppose that I is radical. Let $J/I \subseteq R/I$ be an ideal such that $(J/I)^m = 0$ for some $m \in \mathbb{N}$. As $(J/I)^m = J^m/I$, it follows that $J^m = I$, and hence as I is radical, $J \subseteq I$, so that $J/I = 0$.

($\Leftarrow$) Suppose that R/I is radical. Let $J \subseteq R$ be an ideal such that $J^m \subseteq I$ for some $m \in \mathbb{N}$. As $J^m/I = (J/I)^m$, it follows that $(J/I)^m = 0$, and hence as R/I is radical, $J/I = 0$, so that $J \subseteq I$.

(iv) ($\Rightarrow$) Suppose that I is primary. Let $J/I, K/I \subseteq R/I$ be ideals such that $(J/I)(K/I) = 0$. It follows that $JK \subseteq I$, and hence as I is primary, either one of J, K is contained in I or one of J, K is contained in $\sqrt{I}$. In the former case, without loss of generality, suppose that $J \subseteq I$, in which case $J/I = 0$ and we are done. Otherwise, without loss of generality, $J \subseteq \sqrt{I}$, so that $J/I \subseteq \sqrt{0}$.

($\Leftarrow$) Suppose that R/I is primary. Let $J, K \subseteq R$ be ideals such that $JK \subseteq I$. It follows that $(J/I)(K/I) = 0$, and hence as R/I is primary, either one of $J/I, K/I$ is 0 or one of $J/I, K/I$ is contained in $\sqrt{0}$. In the former case, without loss of generality, suppose that $J/I = 0$, in which case $J \subseteq I$ and we are done. Otherwise, without loss of generality, $J/I \subseteq \sqrt{0}$, so that $J \subseteq \sqrt{I}$. ■

C.2.5 Summary

While this might seem like a lot, I claim that it can all be organized quite nicely. First of all, we have three things: properties of ideals, the corresponding properties of their quotient rings, and the 'simpler' properties these are equivalent to in the commutative case. Secondly, we also have implications among these properties. In the table below, the properties in the first row imply the properties in the second row, and the properties in the second row are equivalent to the combination of the corresponding properties in the third and fourth rows.

Ideal I	Quotient R/I	R/I for R comm.
Maximal	Simple	Field
Prime	Prime	Integral
Radical	Radical	Reduced
Primary	Primary	Hyper-connected

To clarify, an ideal I has the property in the left-hand column iff R/I has the property in the middle column. Likewise, for crings, the properties in the middle column are equivalent to the properties in the right-hand column.

We also covered the result (Theorem C.2.2.10) that states that ideals in R/I correspond exactly to ideals in R which contain I, and

that all the properties discussed are preserved in both directions by this correspondence.

C.3 The integral closure

Let's take a step back for a moment and forget we know pretty much everything we know about mathematics. In fact, let's temporarily forget everything except the natural numbers, $\mathbb{N}$. So, we have the natural numbers in hand, and we write down an equation $x + m = n$, and then we try to solve it (because that's what mathematicians do, yeah?). Sometimes we can: if $x + 3 = 5$, then $x = 2$. But eventually we run into a problem: if $x + 3 = 1$, what should x be?

Uh oh. For a moment there, you think you just broke math. But now I come along, the clever man that I am, and I tell you about this super cool idea called the "integers". Basically, you can solve all equations like this just by taking $\mathbb{N}$ and 'adding in' all the solutions to the equations you can't solve. Want to solve $x + 5 = 0$ you say? Great, I present unto you -5. "What's -5 you ask?". "It's the solution to the equation $x + 5 = 0$", I reply. You now have the integers, $\mathbb{Z}$.

It's that easy. Want to solve an equation? Cheat. Pretend you have a solution, give it a name, add it to your set, et voilà: you can now solve your equation.

Life goes on, things are good, you can solve your equations. But then one day someone decides to ask this super insanely difficult question: "If $2x = 1$, what is x?". You freak out, thinking you broke math again, but then recall my words of wisdom. And so your mind brings $\frac{1}{2}$ into existence, the solution to the equation $2x = 1$. After a bit more thought, you realize you can perform similar feats of wizardry and solve all equations of the form $mx = n$. You now have the rationals, $\mathbb{Q}$.

And now something mysterious happens. Something something limits. Something something least-upper bound property. Something something .... You now have the real numbers, $\mathbb{R}$.[1]

Again, life is going well, until one day a heretic decides to ask the question "If $x^2 + 1 = 0$, what is x?". Your fellow mathematicians

[1]Passing from $\mathbb{Q}$ to $\mathbb{R}$ is about solving a different sort of 'problem' that $\mathbb{Q}$ has that doesn't really have much to do with solving equations.

call this heretic out on his. . . heresy. . . , but you, recalling my wisdom from days long past, realize that you *can* solve such an equation: all you have to do is make up the solution!

And so, you take $\mathbb{R}$, add this new solution to the mix, which you have quite creatively decided to call "i", to obtain a new 'number system'. You now have the complex numbers, $\mathbb{C}$.

But something of a miracle has happened. You set out to solve a single equation, $x^2 + 1 = 0$, but by adding *just a single element*, you can now solve all polynomial equations! In fact, you can even solve polynomial equations with coefficients in this weird new number system you just cooked up.

This passage from $\mathbb{R}$ to $\mathbb{C}$ is one we would like to generalize in this section. Given a field $\mathbb{F}$, we would like to be able to solve polynomial equations in $\mathbb{F}$. Of course, you can't always do that, and so the plan is to 'enlarge' the field $\mathbb{F}$ to a new field $\mathbb{A}$ which contains all the solutions you needed.[2] This will be the *algebraic closure* of $\mathbb{A}$.

It turns out however, that, in full generality (so for rings and not just fields), there is something that is better-behaved, but yet agrees with the algebraic closure in the case the ring happens to be a field. This is the *integral closure*. The integral closure is the thing you obtain only by adding in roots to *monic* polynomials, that is, polynomials whose leading coefficient is 1.

We investigate both. A priori, the algebraic closure is the one we'd be interested in (so we can solve *all* polynomial equations, not just the monic ones), but a further investigation will reveal that the integral closure is the one you probably want to work with in general. That's not a terribly big deal for us, however, as, like I said, the two notions wind up agreeing in the primary case of interest.

In any case, let us begin.

[2]In general, doing this will be quite a bit more complicated than going from $\mathbb{R}$ to $\mathbb{C}$. That really was something of a miracle—it turns out that those fields which you can obtain an "algebraic closure" by adding just a single new element in this way have a name: they are the *real-closed fields*.

C.3.1 Associative algebras

Suppose we start with a field $\mathbb{F}$ which we enlarge to a field $\mathbb{A}$. $\mathbb{A}$ is of course a ring, but it also has the structure of a vector space: you can scale elements of $\mathbb{A}$ by elements of $\mathbb{F}$. This gives $\mathbb{A}$ the structure of what is called an *associative algebra*.

Intuitively, an associative algebra is like a module[3] where you are allowed to "multiply" the elements of the module. Equivalently, you might think of an associative algebra as a ring where you can scale elements. That is, an associative algebra is something with both the structure of a bimodule and a ring for which the two structures are mutually compatible.

Definition C.3.1.1 — $\mathbb{K}$-algebra Let $\mathbb{K}$ be a ring. Then, a ***$\mathbb{K}$-algebra*** is

(I). a ring $\langle A, +, 0, -, \cdot, 1\rangle$; together with
(II). functions $\cdot_L : \mathbb{K} \times A \to A$ and $\cdot_R : A \times \mathbb{K} \to A$;

such that

(i). $\langle A, +, 0, -, \mathbb{K}, \cdot_L, \cdot_R\rangle$ is a $\mathbb{K}$-$\mathbb{K}$-bimodule;
(ii).

$$\alpha \cdot_L (a_1 \cdot a_2) = (\alpha \cdot_L a_1) \cdot a_2; \tag{C.3.1.2}$$

(iii).

$$(a_1 \cdot a_2) \cdot_R \alpha = a_1 \cdot (a_2 \cdot_R \alpha); \tag{C.3.1.3}$$

(iv).

$$(a_1 \cdot_R \alpha) \cdot a_2 = a_1 \cdot (\alpha \cdot_L a_2) \tag{C.3.1.4}$$

and
(v).

$$\alpha \cdot_L a = a \cdot_R \alpha \tag{C.3.1.5}$$

if $a \in A$ is central;

[3] Actually, a bimodule (Definition 1.1.1.5).

for all $a_1, a_2 \in A$ and $\alpha \in \mathbb{K}$.

R Essentially what these axioms state is (i) "associativity" holds between elements of $\mathbb{K}$ and elements of A,[a], and (ii) central elements commute with scalars.

R An ***associative algebra*** is a $\mathbb{K}$-algebra for some $\mathbb{K}$. This term is thus used when you don't want to have to specify the ground ring. The "associative" here refers to the associativity of the ring multiplication. If you drop this hypothesis (in which case the definition becomes a bit more cumbersome to state because $\cdot$ is then no longer a ring multiplication), you obtain what is simply an ***algebra***. For example, Lie algebras are algebras that are generally not associative. Thus, the term "algebra" by itself should be avoided if one really means "associative algebra". On the other hand, if we say "$\mathbb{K}$-algebra", for us it is implicit that the algebra is associative.

R The reason we require the structure of a bimodule (instead of just a left or right module) is motivated by the fact that doing things this way gives us another standard equivalent definition—see Theorem C.3.1.8.

[a] Three axioms needed to deal with the three cases of the scalar appearing on the left, on the right, or in the middle. Note that the case of two scalars and one element of A is part of the definition of a bimodule.

Definition C.3.1.6 — $\mathbb{K}$-algebra homomorphism Let A and B be $\mathbb{K}$-modules and let $\phi\colon A \to B$ be a function. Then, ϕ is a ***$\mathbb{K}$-algebra homomorphism*** iff it both a ring homomorphism and $\mathbb{K}$-$\mathbb{K}$-linear.

▪ **Example C.3.1.7 — The category of $\mathbb{K}$-algebras** Let $\mathbb{K}$ be a ring. Then, the category of $\mathbb{K}$-algebras is the concrete category $\mathbb{K}$-**Alg**

(i). whose collection of objects Obj($\mathbb{K}$-**Alg**) is the collection of all $\mathbb{K}$-algebras; and
(ii). with morphism set $\mathrm{Mor}_{\mathbb{K}\text{-}\mathbf{Alg}}(A, B)$ precisely the set of all $\mathbb{K}$-algebra homomorphisms from A to B.

R Just as we have the category of left $\mathbb{K}$-algebras $\mathbb{K}$-**Alg**, we also have that category of right $\mathbb{K}$-algebras **Alg**-$\mathbb{K}$ defined similarly.

While, in my opinion anyways, "ring in which you can scale elements" is by far the more intuitive way to think about the concept, there is an equivalent formulation which some authors take as the definition.

Theorem C.3.1.8. Let $\mathbb{K}$ be a ring.

(i). Let A be a ring and let $\phi\colon \mathbb{K} \to A$ be a ring homomorphism. Then, $\langle A, \cdot_{L,\phi}, \cdot_{R,\phi}\rangle$ is a $\mathbb{K}$-algebra, where $\cdot_{L,\phi}\colon \mathbb{K} \times A \to A$ and $\cdot_{R,\phi}\colon A \times \mathbb{K} \to A$ are defined by

$$\alpha \cdot_{L,\phi} a := \phi(\alpha)a \text{ and } a \cdot_{R,\phi} \alpha := a\phi(\alpha). \quad \text{(C.3.1.9)}$$

(ii). Let $\langle A, \cdot_L, \cdot_R\rangle$ be a $\mathbb{K}$-$\mathbb{K}$-algebra. Then, $\phi\colon \mathbb{K} \to A$, defined by

$$\alpha \cdot_L 1 =: \phi_{\cdot_L,\cdot_R}(\alpha) := 1 \cdot_R \alpha, \quad \text{(C.3.1.10)}$$

is a ring homomorphism.

Furthermore, these two constructions are inverse to each other.

R Given a ring homomorphism $\phi\colon \mathbb{K} \to A$, ϕ will be referred to as the ***structure morphism*** of the corresponding $\mathbb{K}$-algebra structure on A.

R This result says that we could have equivalently defined a $\mathbb{K}$-algebra to be a ring homomorphism $\mathbb{K} \to A$ into some ring A. While I think this is an unintuitive way to think about things, it *is* important.[a] In particular, you should note that ring homomorphisms allow you to define $\mathbb{K}$-algebras in this way.

R In particular, if $\mathbb{K}$ and $\mathbb{L}$ are rings with $\mathbb{K} \subseteq \mathbb{L}$, then $\mathbb{L}$ obtains the structure of a $\mathbb{K}$-algebra via the inclusion map $\mathbb{K} \hookrightarrow \mathbb{L}$.

R This result is *roughly* analogous to our equivalent characterization of R-modules (Theorem 1.1.6).

[a] Indeed, I used this characterization to determine what axioms I wanted to use for the definition of a $\mathbb{K}$-algebra (in the noncommutative case, there is single standard definition).

Proof. (i) For the sake of brevity, we shall simply write $\cdot := \cdot_{L,\phi}$, and by abuse of notation, $\cdot := \cdot_{R,\phi}$ as well. We first check that this gives A the structure of a left $\mathbb{K}$-module. So, let $\alpha_1, \alpha_2 \in \mathbb{K}$ and $a \in A$. Then,

$$\begin{aligned}(\alpha_1\alpha_2) \cdot a &:= \phi(\alpha_1\alpha_2)a = \phi(\alpha_1)(\phi(\alpha_2)a) \\ &=: \alpha_1 \cdot (\alpha_2 \cdot a).\end{aligned} \tag{C.3.1.11}$$

We also have $1 \cdot a := \phi(1)a = 1a = a$. As for the distributivity axioms of a $\mathbb{K}$-module, we have

$$\begin{aligned}(\alpha_1 + \alpha_2) \cdot a &:= \phi(\alpha_1 + \alpha_2)a \\ &= (\phi(\alpha_1) + \phi(\alpha_2))\, a \\ &= \phi(\alpha_1)a + \phi(\alpha_2)a \\ &=: \alpha_1 \cdot a + \alpha_2 \cdot a\end{aligned} \tag{C.3.1.12}$$

and

$$\begin{aligned}\alpha \cdot (a_1 + a_2) &:= \phi(\alpha)(a_1 + a_2) = \phi(\alpha)a_1 + \phi(\alpha)a_2 \\ &=: \alpha \cdot a_1 + \alpha \cdot a_2.\end{aligned} \tag{C.3.1.13}$$

Thus, $\cdot$ does indeed give A the structure of a left $\mathbb{K}$-module. Similarly, it has the structure of a right $\mathbb{K}$-module. Finally, to see that A is in fact a $\mathbb{K}$-$\mathbb{K}$-bimodule, note that

$$(\alpha_1 \cdot a) \cdot \alpha_2 := {}^{a} := \phi(\alpha_1)a\phi(\alpha_2) =: \alpha_1 \cdot (a \cdot \alpha_2). \tag{C.3.1.14}$$

We next check (ii) of Definition C.3.1.1. So, let $\alpha \in \mathbb{K}$ and $a_1, a_2 \in A$. Then,

$$\alpha \cdot (a_1 a_2) \coloneqq \phi(\alpha)(a_1 a_2) = (\phi(\alpha) a_1) a_2 =: (\alpha \cdot a_1) a_2 \quad \text{(C.3.1.15)}$$

(iii) follows similarly. As for (iv), we see that

$$\begin{aligned}(a_1 \cdot \alpha) a_2 &\coloneqq (a_1 \phi(\alpha)) a_2 = {}^{b} a_1 (\phi(\alpha) a_2) \\ &=: a_1 (\alpha \cdot a_2).\end{aligned} \quad \text{(C.3.1.16)}$$

Finally, we check (v). So, let $\alpha_1, \alpha_2 \in \mathbb{K}$ and let $a \in A$ be central. Then,

$$\alpha \cdot a \coloneqq \phi(\alpha) a = a \phi(\alpha) \coloneqq a \cdot \alpha. \quad \text{(C.3.1.17)}$$

(ii) For the sake of brevity, we shall simply write $\phi \coloneqq \phi_{\cdot_L, \cdot_R}$. ϕ preserves addition because scaling distributes over addition in $\mathbb{K}$. As for multiplication, let $\alpha, \beta \in \mathbb{K}$. Then,

$$\begin{aligned}\phi(\alpha\beta) &\coloneqq (\alpha\beta) \cdot 1 = \alpha \cdot (\beta \cdot 1) =: \alpha \cdot \phi(\beta) \\ &= \alpha \cdot (1 \phi(\beta)) = (\alpha \cdot 1) \phi(\beta) =: \phi(\alpha) \phi(\beta).\end{aligned} \quad \text{(C.3.1.18)}$$

And of course, $\phi(1) \coloneqq 1 \cdot 1 = 1$.

It remains to check that these constructions are inverse to one another.

$$\begin{aligned}\alpha \cdot_{L, \phi_{\cdot_L, \cdot_R}} a &\coloneqq \phi_{\cdot_L, \cdot_R}(\alpha) a \coloneqq (\alpha \cdot_L 1) a \\ &= \alpha \cdot_L (1a) = \alpha \cdot_L a.\end{aligned} \quad \text{(C.3.1.19)}$$

Similarly for $\cdot_R$.

In the other direction,

$$\phi_{\cdot_{L,\phi}, \cdot_{R,\phi}}(\alpha) \coloneqq \alpha \cdot_{L,\phi} 1 \coloneqq \phi(\alpha) 1 = \phi(\alpha). \quad \text{(C.3.1.20)}$$

■

[a] This uses the associativity of the ring multiplication.
[b] Because the ring multiplication is associative.

Definition C.3.1.21 — Extension Let $\mathbb{K}$ be a ring. Then, an ***extension*** of $\mathbb{K}$ is a $\mathbb{K}$-algebra $\mathbb{L}$ such that $\mathbb{K} \subseteq \mathbb{L}$ and whose structure morphism is given by the inclusion $\mathbb{K} \hookrightarrow \mathbb{L}$.

▪ **Example C.3.1.22 — Rings are $\mathbb{Z}$-algebras** Let R be a ring.

Exercise C.3.1.23 Show that there is a *unique* ring homomorphism $\mathbb{Z} \to R$.

R thus obtains the structure of a $\mathbb{Z}$-algebra using the previous result. It turns out that scaling (on both the left and right) $r \in R$ by $m \in \mathbb{Z}^+$ is nothing more than r added to itself m times.

R Just as commutative groups are 'the same as' $\mathbb{Z}$-modules (Example 1.1.22), rings are 'the same as' $\mathbb{Z}$-algebras.

▪ **Example C.3.1.24**

(i). $\mathbb{R}$ is an infinite-dimensional $\mathbb{Q}$-algebra.
(ii). $\mathbb{C}$ is a 2-dimensional $\mathbb{R}$-algebra.
(iii). $\mathbb{H}$ is a 2-dimensional $\mathbb{C}$-algebra and a 4-dimensional $\mathbb{R}$-algebra.

Polynomials furnish another natural collection of $\mathbb{K}$-algebras.

C.3.2 Polynomials

Proposition C.3.2.1 — Polynomial algebra Let $\mathbb{K}$ be a ring. Define $\cdot : \mathbb{K}^\infty \times \mathbb{K}^\infty \to \mathbb{K}^\infty$ by

$$[a \cdot b]_k := \sum_{i+j=k} a_i b_j. \tag{C.3.2.2}$$

Then, $\mathbb{K}[x] := \langle \mathbb{K}^\infty, +, 0, -, \cdot, 1 \rangle$, the ***polynomial algebra*** in a single variable with coefficients in $\mathbb{K}$, is a $\mathbb{K}$-algebra, where

addition and both left and right scaling are defined componentwise, 0 is the sequence of all 0s, and $1 := \langle 1, 0, 0, \ldots \rangle$.

R We suggestively write

$$\begin{aligned} &a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + a_m x^m \\ &\quad := \langle a_0, a_1, \ldots, a_{m-1}, a_m, 0, 0, \ldots \rangle. \end{aligned} \tag{C.3.2.3}$$

With this notation, addition, multiplication, and scaling all work how you think they would with x commuting with everything.

R Elements of $\mathbb{K}[x]$ are ***polynomials*** (in a single variable with coefficients in $\mathbb{K}$).

R Warning: Elements in $\mathbb{K}[x]$ are *not* functions—see Equation (C.3.2.12). That said, it is not uncommon to use notation suggestive of such. For example, it is not uncommon to write $p(x) \in \mathbb{K}[x]$ for a polynomial. In fact, the polynomial is just p, but it can be useful to write $p(x)$ for the polynomial just as one writes $f(x)$ to denote a function, even though technically the function is just f.

R For $p(x) = a_0 + \cdots + a_m x^m \in \mathbb{K}[x]$, $a_m \neq 0$, the ***degree*** of p, $\deg(p)$, is defined by $\deg(p) := m$. a_m is the ***leading coefficient*** of p. a_0 is the ***constant term*** of p. p is ***monic*** iff the leading coefficient is 1.

R We also make use of that $\mathbb{K}$-algebra $[x]\mathbb{K}$. As a $\mathbb{K}$-algebra, $[x]\mathbb{K}$ is identical to $\mathbb{K}[x]$. However, notationally, elements in $[x]\mathbb{K}$ are written as

$$a_0 + x a_1 + \cdots + x^{m-1} a_{m-1} + x^m a_m. \tag{C.3.2.4}$$

This of course is just a matter of notation. What actually *does* change, however, are the corresponding evaluations maps—see Definition C.3.2.14.

R Recall (Example 1.1.18) that $\mathbb{K}^\infty$ is the set of all $\mathbb{K}$-valued sequences that are eventually 0.

Proof. We leave this as an exercise.

Exercise C.3.2.5 Prove the result.

■

One important fact is that you can "divide" polynomials with coefficients in a division ring.

Theorem C.3.2.6 — Division Algorithm. Let $\mathbb{F}$ be a division ring and let $f, g \in \mathbb{F}[x]$ with $g \neq 0$.

(i). There are unique $q, r \in \mathbb{F}[x]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.
(ii). There are unique $q, r \in \mathbb{F}[x]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.

R q is the *quotient* and r is the *remainder*.

Proof. We leave this as an exercise.

Exercise C.3.2.7 Prove the result.

■

As mentioned in the definition of the property (Definition C.1.21), polynomial rings furnish examples of PIDs.

Proposition C.3.2.8 — $\mathbb{F}[x]$-is a left and right PID Let $\mathbb{F}$ be a division ring. Then, $\mathbb{F}[x]$ is a left and right PIR.

R This is certainly not true if $\mathbb{F}$ is not a division ring. For example, the ideal (x, y) generated by $x, y \in [\mathbb{C}[x]][y]$ is not generated by a single element.[a]

R $\mathbb{F}[x]$ is of course integral, but we don't use the term principal ideal *domain* because that suggests commutativity.

[a] Can you prove this?

Proof. We prove that $\mathbb{F}[x]$ is a left PIR. That it is a right PIR is similar. So, let $I \subseteq \mathbb{F}[x]$ be a nonzero left ideal. Let $g \in I$ be nonzero of minimum degree. Let $f \in I$. By the Division Algorithm, there are unique $q, r \in \mathbb{F}[x]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$. As I is a left ideal, $qg \in I$, and hence $r = f - qg \in I$. However, as g was chosen to have minimum degree among nonzero elements of I and $\deg(r) < \deg(g)$, this implies that $r = 0$, that is, $f = qg \in (g)$. Hence, $I \subseteq (g)$, and so $I = (g)$. ■

Exercise C.3.2.9 Is it true that $\mathbb{F}[x]$ a left and right PID implies that $\mathbb{F}$ is necessarily a division ring?

Polynomial algebras have an important "universal property".

Theorem C.3.2.10. Let $\mathbb{K}$ be a ring and let A be a $\mathbb{K}$-algebra. Then, for every $a \in A$ central, there is a unique $\mathbb{K}$-algebra homomorphism $\phi\colon \mathbb{K}[x] \to A$ such that $\phi(x) = a$.

R Intuitively, a homomorphism $\mathbb{K}[x] \to A$ is completely determined by where it sends x (though you do have to ensure that you map it to a central element as x is itself central). This is not unlike how linear-transformations are completely determined by where they send the elements in a basis.

Proof. We leave this as an exercise.

Exercise C.3.2.11 Prove the result.

■

Not only is this useful in its own right, it suggests a convenient way to define polynomial algebras in multiple variables.

Theorem C.3.2.12 — Polynomial algebras in multiple variables. Let X be a set. Then, there is a unique $\mathbb{K}$-algebra, the ***polynomial algebra*** in the variables X with coefficients in $\mathbb{K}$, $\mathbb{K}[X]$, with $X \subseteq \mathbb{K}[X]$ that has the property that for every $\mathbb{K}$-algebra A and function $f\colon X \to A$ with central image there is a unique $\mathbb{K}$-algebra homomorphism $\phi\colon \mathbb{K}[X] \to A$ such that $\phi|_X = f$.

R Intuitively, this is the statement that any $\mathbb{K}$-algebra homomorphism $\mathbb{K}[X] \to A$ is determined solely by where you send the elements of X.

For example, for $X = \{x, y\}$, a $\mathbb{K}$-algebra homomorphism $\mathbb{K}[X] \to A$ is determined by a choice of two elements of A, say $a_x, a_y \in A$. This then determines the image of every polynomial. For example, the polynomial $3xy - 16x^2 + 3y$ is mapped to $3a_xa_y - 16a_x^2 + 3a_y$.

R For the purpose of (hopefully) increasing clarity, we are actually being sloppy here. When we say that $\mathbb{K}[X]$ is "unique", what we actually mean is that $\mathbb{K}[X]$ is "unique up to unique isomorphism" in the sense that, if A is some other $\mathbb{K}$-algebra with $X \subseteq A$ that satisfies this property, then there is a unique isomorphism (of $\mathbb{K}$-algebras) $\mathbb{A} \to A$.

Similarly, when we write $\mathbb{A} \subseteq A$, we don't *literally* mean that $\mathbb{A}$ is a subset of A, but rather, that there is a unique embedding of $\mathbb{K}$-algebras $\mathbb{A} \to A$.

R The single variable polynomial algebras are a special case of this: $\mathbb{K}[x] \coloneqq \mathbb{K}[\{x\}]$. Thus, we could have just started with this result as the definition of all polynomial algebras, but I think this might be a bit difficult to understand without seeing the single variable case first, and in particular, the "universal property" stated in Theorem C.3.2.10.

R In general, if $X =: \{x_1, \dots, x_m\}$ is a finite set, we write $\mathbb{K}[x_1, \dots, x_m] \coloneqq \mathbb{K}[X]$.

R So, for example, $-3x^3yz^2 + xy - 2y + x + 4z - 6 \in \mathbb{Z}[x, y, z]$.

R As with the single variable case, we have a corresponding $\mathbb{K}$-algebra of "right polynomials $[X]\mathbb{K}$ which, as a $\mathbb{K}$-algebra, is the same as $\mathbb{K}[X]$, but will be distinguished from $\mathbb{K}[X]$ by how the polynomials become polynomial functions—see Definition C.3.2.14.

Proof. We leave this as an exercise.

Exercise C.3.2.13 Prove the result.

■

Polynomials vs. polynomial functions

Given a polynomial $p \in \mathbb{K}[x]$, we obtain a corresponding function $\mathbb{K} \to \mathbb{K}$ defined by $x \mapsto p(x)$, where $p(x) \in \mathbb{K}$ is obtained by "plugging-in" the value $x \in \mathbb{K}$ into p and evaluating. For example, if $\mathbb{K} := \mathbb{R}$ and $p := 3x^2 - 5$, then $p(-2) := 3(-2) \cdot (-2) - 5 = 7$. The distinction between this function and the original polynomial is a subtle one. Elements of $\mathbb{K}[x]$ are merely "formal"[4] polynomials, and not functions themselves.

To see the difference between the concepts, take $\mathbb{K} := \mathbb{Z}/2\mathbb{Z}$ and consider the two polynomials $p := 0$ and $q := x + x^2 = x(x-1)$. These are manifestly different polynomials—the coefficients are different—but yet they both define the same function on $\mathbb{Z}/2\mathbb{Z}$ as $q(0) = 0 \cdot 1 = 0$ and $q(1) = 1 \cdot 0 = 0$.

We now make the distinction between a polynomial and a polynomial function precise by actually giving the definition of the latter.

[4] I'm not quite sure why this word is used. I think it's a bit misleading, but the word "formal" in this context essentially means that the thing is to be mindlessly manipulated as symbols and nothing more. For example, I can talk about the "formal" power series $1 + 2x + 3x^2 + 4x^3 + \cdots$ even though the resulting expression might not make sense when I plug in particular values of x—here, x is just a symbol, not a number.

Definition C.3.2.14 — Polynomial function Let $\mathbb{K}$ be a ring.

(i). A ***left polynomial function*** is a function $\mathbb{K} \to \mathbb{K}$ of the form $\alpha \mapsto p(\alpha)$ for $p \in \mathbb{K}[x]$.

(ii). A ***right polynomial function*** is a function $\mathbb{K} \to \mathbb{K}$ of the form $\alpha \mapsto p(\alpha)$ for $p \in [x]\mathbb{K}$.

R To clarify what is meant by $p(\alpha)$, write $p(x) = a_0 + \cdots + a_m x^m \in \mathbb{K}[x]$. Then,

$$p(\alpha) := a_0 + \cdots + a_m \alpha^m. \tag{C.3.2.15}$$

Similarly, for $p(x) = a_0 + \cdots + x^m a_m \in [x]\mathbb{K}$,

$$p(\alpha) := a_0 + \cdots + \alpha^m a_m. \tag{C.3.2.16}$$

We mentioned after Example 4.3.11 that, for a given linear operator, there is a polynomial, called the characteristic polynomial, of which all the eigenvalues are a root, and that essentially the reason that the matrix given in Example 4.3.11 was diagonalizable over $\mathbb{C}$ but not over $\mathbb{R}$ was because the characteristic polynomial in this case had complex but not real roots. This suggests that the property we want to impose on the ground division ring has something to do with roots of polynomials. So, before anything else, let's be absolutely clear what we mean by the term "root".

Convention C.3.2.17 — Two-sided In what follows, many definitions have left and right versions (because of the possible noncommutativity). We then have a corresponding ***two-sided*** version: ABC is two-sided XYZ iff ABC is left XYZ and right XYZ.

Furthermore, if we every drop these phrases, it should be understood that we are referring to the *two-sided* version (e.g. if we just say "XYZ" instead of "two-sided XYZ").

Definition C.3.2.18 — Relative root Let $\mathbb{L}$ be a $\mathbb{K}$-algebra and let $x_0 \in \mathbb{L}$.[a]

(i). For $p \in \mathbb{K}[x]$, x_0 is a ***right root*** of p iff $p(x_0) = 0$.
(ii). For $p \in [x]\mathbb{K}$, x_0 is a ***left root*** of p iff $(x_0)p = 0$.
(iii). For $\mathbb{K}[x] \ni p \in [x]\mathbb{K}$, x_0 is a ***two-sided root*** of p iff it is both a left and right root of p.

R "Relative" refers to the fact that we are only concerned with the roots of p that lie in $\mathbb{L}$, so this is "relative to $\mathbb{L}$"—see Definition C.3.3.43 for an "absolute version".

R Write $p(x) = a_0 + a_1 x + \cdots + a_m x^m$. Then,

$$p(x_0) \coloneqq a_0 + a_1 x_0 + \cdots + a_m x_0^m. \quad \text{(C.3.2.19)}$$

On the other hand, the corresponding polynomial in $[x]\mathbb{K}$ is $p(x) = a_0 + x a_1 + \cdots + x^m a_m$, in which case

$$(x_0)p \coloneqq a_0 + x_0 a_1 + \cdots + x_0^m a_m \quad \text{(C.3.2.20)}$$

Note that in general these are *not* the same.

That said, I find the notation $(x_0)p$ to be rather awkward and I shall avoid it unless strictly necessary (note how above I still wrote $p(x) = a + x a_1 + \cdots + x^m a_m$—I suppose it might be better to denote this by $(x)p$, but as I said, that looks very awkward to me).

R Thus, the definition was probably exactly what you thought it would be, but we gave it just to be absolutely sure that noncommutativity didn't change the definition in any serious way. Be warned, however: though it didn't change the definition, it *will* change the behavior of roots. For example, we no longer have $[pq](x_0) = p(x_0)q(x_0)$, and so we can no longer conclude that x_0 is a root of pq if it is a root of p. (It will be true that x_0 is a root of pq if it's a root of q, though hopefully this makes it clear we have to be more careful with our proof than you might have previously thought.)

R The reason to involve two rings ($\mathbb{L}$ and $\mathbb{K}$) instead of just one is because, for example, we would like to be able to say that $\mathrm{i} \in \mathbb{C}$ is a root of $x^2 + 1 \in \mathbb{R}[x]$ even though $\mathrm{i} \notin \mathbb{R}$.

[a] Recall that as $\mathbb{K}$-algebras, $\mathbb{K}[x] \cong [x]\mathbb{K}$, and so we may freely regard a polynomial in one as a polynomial in the other. These two algebras only differ in how we "plug-in" values, as explained in the remarks below.

Proposition C.3.2.21 Let $\mathbb{F}$ be a division ring and let $x_0 \in \mathbb{F}$.

(i). x_0 is a right root of $p \in \mathbb{F}[x]$ iff there is some $q \in \mathbb{F}[x]$ such that $p(x) = q(x)(x - x_0)$.

(ii). x_0 is a left root of $p \in [x]\mathbb{F}$ iff there is some $q \in [x]\mathbb{F}$ such that $p(x) = (x - x_0)q(x)$.

Proof. We leave this as an exercise.

Exercise C.3.2.22 Prove the result.

R Hint: See [T Y91, Proposition 16.2].

■

▪ **Example C.3.2.23 — A degree 2 polynomial with infinitely many roots** The polynomial $x^2 + 1$ has infinitely many roots in $\mathbb{H}$.[a]

Exercise C.3.2.24 Check this.

Exercise C.3.2.25 On the other hand, show that $x^2 + 1$ doesn't have *any* central roots.

R For fields, it is well-known (perhaps even to you) that a polynomial of degree m can have at most m roots. Thus, this phenomenon is perhaps quite startling: in what is arguably the simplest of all noncommutative

division rings, we have a polynomial of degree 2 with infinitely many roots![b] Instead, this classical result generalizes to the statement that the set of all roots of p belong to at most m *conjugacy classes* in D.[c] Furthermore, it *is* true that either (i) there are infinitely many roots or (ii) the number of roots is less than m. For example, even over the most noncommutative division rings, you can't find a degree 3 polynomial with 6 roots: the only possibilities are 0, 1, 2, 3, and infinitely many roots.

[a] Of course, it has none in $\mathbb{R}$ and 2 in $\mathbb{C}$.

[b] Of course, we can't do this with degree less than 2.

[c] You don't need to know what "conjugacy class" means. This is just a comment for those that already know and those that are curious enough to look up the details. By the way, this theorem has a name: it's called the *Gordon-Motzkin Theorem*.

C.3.3 Algebraic and integral

Definition C.3.3.1 — Algebraically closed Let $\mathbb{K}$ be a ring. Then, $\mathbb{K}$ is ***algebraically closed*** iff every nonconstant polynomial with coefficients in $\mathbb{K}$ can be written as a product of linear factors.

Definition C.3.3.2 — Integrally closed Let $\mathbb{K}$ be a ring. Then, $\mathbb{K}$ is ***integrally closed*** iff every nonconstant monic polynomial with coefficients in $\mathbb{K}$ can be written as a product of monic linear factors.

Meta-definition C.3.3.3 — Weakly algebraically closed Let $\mathbb{K}$ be a ring. Then, $\mathbb{K}$ is ***XYZ weakly algebraically closed*** iff every nonconstant $p \in \mathbb{K}[x]$ has an XYZ root in $\mathbb{K}$.

R Recall that (Convention C.3.2.17) XYZ can stand for either "right", "left", or "two-sided"—this applies throughout though we won't remind you again.[a]

R The reason why this is *right* weakly algebraically closed (and not left) is that the statement that $\alpha \in \mathbb{K}$ is a root of p is equivalent to the statement that $p(x) = q(x)(x - \alpha)$ for some $q \in \mathbb{K}[x]$[b]—see the following result Proposition C.3.2.21. Similarly for left weakly algebraically closed.

R Warning: $\mathbb{K}$ being (two-sided) algebraically closed is *not* the same as every nonconstant polynomial having a (two-sided) root. According to Convention C.3.2.17, $\mathbb{K}$ being (two-sided) algebraically closed means that it is both left algebraically closed and right algebraically closed. Thus, every nonconstant polynomial would have to have a right and a left root, but these roots don't necessarily have to coincide (that is, be a (two-sided) root).

R Of course, algebraically closed implies weakly algebraically closed.

[a] I imagine that would get slightly annoying. . .

[b] This is *not* in general equivalent to the statement that $p(x) = (x-\alpha)r(x)$ for some $r \in \mathbb{K}[x]$ if $\mathbb{K}$ is noncommutative.

Meta-definition C.3.3.4 — Weakly integrally closed Let $\mathbb{K}$ be a ring. Then, $\mathbb{K}$ is ***XYZ integrally closed*** iff every nonconstant monic $p \in \mathbb{K}[x]$ has a XYZ root in $\mathbb{K}$.

R Warning: Don't confuse this with the term "integrally closed-domain"![a]

R You should see Example C.3.3.16 to perhaps better understand the difference between the integrally closed and algebraically closed.

For me anyways, algebraically closed is the more intuitive of the two, but this is perhaps just because I was taught it much earlier. One reason for the introduction of "integrally closed" when one already has the notion of "algebraically closed" is that the former is in general more well-behaved than the latter.

For example, integral elements form a ring (Proposition C.3.3.22) whereas the algebraic elements do not necessarily (Example C.3.3.26).

R Note that in the common case of interest where $\mathbb{K}$ is a field, the notions of "integral" and "algebraic" are equivalent—see Meta-proposition C.3.3.15.

R Warning: $\mathbb{K}$ being (two-sided) integrally closed is *not* the same as every nonconstant monic polynomial having a (two-sided) root. According to Convention C.3.2.17, $\mathbb{K}$ being (two-sided) integrally closed means that it is both left integrally closed and right integrally closed. Thus, every nonconstant monic polynomial would have to have a right and a left root, but these roots don't necessarily have to coincide (that is, be a (two-sided) root).

R Of course, integrally closed implies weakly integrally closed.

[a] This means that it is an integral domain that is integrally closed in its field of fractions, as opposed to just "absolutely" integrally closed, not relative to another ring.

Proposition C.3.3.5 Let $\mathbb{K}$ be a ring. Then, the following are equivalent.

(i). $\mathbb{K}$ is integrally closed.
(ii). $\mathbb{K}$ is right weakly integrally closed.
(iii). $\mathbb{K}$ is left weakly integrally closed.
(iv). $\mathbb{K}$ is two-sided weakly integrally closed.

R Warning: The analogous result for "algebraic" should be false, though it is true if $\mathbb{K}$ is a field—see Proposition C.3.3.7.

R Hence, we need only use the term "integrally closed".

Proof. We leave this as an exercise.

Exercise C.3.3.6 Prove the result.

R Hint: The Stacks Project.

■

Proposition C.3.3.7 Let $\mathbb{F}$ be a field. Then, the following are equivalent.

(i). $\mathbb{F}$ is algebraically closed.
(ii). $\mathbb{F}$ is right weakly algebraically closed.
(iii). $\mathbb{F}$ is left weakly algebraically closed.
(iv). $\mathbb{F}$ is two-sided weakly algebraically closed.
(v). $\mathbb{F}$ is integrally closed.
(vi). $\mathbb{F}$ is right weakly integrally closed.
(vii). $\mathbb{F}$ is left weakly integrally closed.
(viii). $\mathbb{F}$ is two-sided weakly integrally closed.

Proof. We leave this as an exercise.

Exercise C.3.3.8 Prove the result.

■

Exercise C.3.3.9 Can you find a counter-example showing that Proposition C.3.3.5 fails when you replace "integrally" with "algebraically"?

▪ **Example C.3.3.10** Note that $\mathbb{C}$ is algebraically closed but $\mathbb{R}$ is not. $\mathbb{H}$ is also (left and right) algebraically closed.

Exercise C.3.3.11 Can you find an example of a division ring that is left algebraically closed but not right algebraically closed (or vice versa)?

Of course, not everything is algebraically closed or even integrally closed (for example, the real numbers). As being algebraically closed is such a useful property, it is of interest to 'enlarge' a given field to something that is algebraically closed. The basic idea is to take your field and just 'throw in' all solutions to polynomial equations, not unlike one obtains $\mathbb{Q}$ from $\mathbb{Z}$ by "throwing in" all solutions to equations of the form $mx = n$. The field obtained in this way is the *algebraic closure* of the original field. Before we make this intuition precise, however, we must first discuss some preliminaries.

Meta-definition C.3.3.12 — Algebraic element Let $\mathbb{L}$ be a $\mathbb{K}$-algebra and let $\alpha \in \mathbb{L}$. Then, α is ***XYZ algebraic*** over $\mathbb{K}$ iff there is a nonconstant polynomial $p \in \mathbb{K}[x]$ such that α is an XYZ root of p.

α is ***XYZ transcendental*** over $\mathbb{K}$ iff it is not XYZ algebraic over $\mathbb{K}$.

Meta-definition C.3.3.13 — Integral element Let $\mathbb{L}$ be a $\mathbb{K}$-algebra and let $\alpha \in \mathbb{L}$. Then, α is ***XYZ integral*** over $\mathbb{K}$ iff there is a nonconstant monic polynomial $p \in \mathbb{K}[x]$ such that α is an XYZ root of p.

▪ **Example C.3.3.14** $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ (it is a root of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$).

$\pi \in \mathbb{R}$ is not algebraic over $\mathbb{Q}$.[a]

[a] For example, by the Lindemann-Weierstrass Theorem, if you enjoy swatting your flies with sledgehammers (I know I do).

Meta-proposition C.3.3.15 — Integral=algebraic over division rings Let $\mathbb{F}$ be a division ring, let A be an $\mathbb{F}$-algebra,

and let $x \in A$. Then, x is XYZ integral over $\mathbb{F}$ iff it is XYZ algebraic over $\mathbb{F}$.

R Similarly, a division ring is XYZ integrally closed iff it is XYZ algebraically closed.

Proof. ($\Rightarrow$) Immediate from the definitions.

($\Leftarrow$) Suppose that x is right algebraic over $\mathbb{F}$. By definition, there is a nonconstant polynomial $p \in \mathbb{F}[x]$ such that $p(x) = 0$. Denote the leading coefficient of p by a_m. Multiplying $p(x) = 0$ on the left by a_m^{-1} shows that $[a_m^{-1}p](x) = 0$. As $a_m^{-1}p$ is monic, this shows that x is left-integral. ■

▪ **Example C.3.3.16 — Algebraic but not integral** $\frac{1}{2} \in \mathbb{Q}$ is algebraic but not integral over $\mathbb{Z}$: it is a root of the polynomial $2x - 1$, but it is not the root of any monic polynomial with integer coefficients.

Meta-definition C.3.3.17 — Algebraic $\mathbb{K}$-algebra Let $\mathbb{L}$ be a $\mathbb{K}$-algebra. Then, $\mathbb{L}$ is ***XYZ algebraic*** iff every element of $\mathbb{L}$ is XYZ algebraic over $\mathbb{K}$.

R We may instead say that $\mathbb{L}$ is ***algebraic*** over $\mathbb{K}$.

R If $\mathbb{L}$ is an extension of $\mathbb{K}$, then people will say that "L is an ***XYZ algebraic extension*** of $\mathbb{K}$" instead of that "$\mathbb{L}$ is an XYZ algebraic $\mathbb{K}$-algebra".

Meta-definition C.3.3.18 — Integral $\mathbb{K}$-algebra Let $\mathbb{L}$ be a $\mathbb{K}$-algebra. Then, $\mathbb{L}$ is ***XYZ integral*** iff every element of $\mathbb{L}$ is XYZ integral over $\mathbb{K}$.

R We may instead say that $\mathbb{L}$ is ***integral*** over $\mathbb{K}$.

R If $\mathbb{L}$ is an extension of $\mathbb{K}$, then people will say that "L is an ***XYZ integral extension*** of $\mathbb{K}$" instead of that "$\mathbb{L}$ is an XYZ integral $\mathbb{K}$-algebra".

Meta-definition C.3.3.19 — Algebraic closure Let $\mathbb{L}$ be a $\mathbb{K}$-algebra. Then, $\mathbb{L}$ is an ***XYZ algebraic closure*** of $\mathbb{K}$ iff it is algebraically closed and XYZ algebraic over $\mathbb{K}$.

Meta-definition C.3.3.20 — Integral closure Let $\mathbb{L}$ be a $\mathbb{K}$-algebra. Then, $\mathbb{L}$ is an ***XYZ integral closure*** of $\mathbb{K}$ iff it is integrally closed and XYZ integral over $\mathbb{K}$.

▪ **Example C.3.3.21**

(i). $\mathbb{H}$ is an algebraic extension of $\mathbb{C}$.
(ii). $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.
(iii). $\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$.

Proposition C.3.3.22 — Relative integral closure Let A be a commutative $\mathbb{K}$-algebra. Then,

$$\{x \in A : x \text{ is integral over } \mathbb{K}.\} \tag{C.3.3.23}$$

is an integral $\mathbb{K}$-subalgebra of A, the ***integral closure*** of $\mathbb{K}$ in A.

Furthermore,

(i). if A is integrally closed, then integral closure of $\mathbb{K}$ in A is integrally closed; and
(ii). if $\mathbb{K}$ and A are fields, then the integral closure of $\mathbb{K}$ in A is a field.

R Warning: The analogous result for algebraic fails—see Example C.3.3.26. Indeed, this is one motivation for preferring integral over algebraic. That said, it seems like it will hold for integral crings,[a] though we won't use this fact—see math.stackexchange.

R "Relative"refers to the fact that this is the integral closure of $\mathbb{K}$ *in* A—see Theorem C.3.3.39 for the "absolute" integral closure.

[a]Different meaning of the word "integral". In fact, just off the top of my head I can think of four different meanings of that word. Like I said, mathematicians are terrible when it comes developing sensible terminology.

Proof. We leave this as an exercise.

Exercise C.3.3.24 Prove the result.

■

Exercise C.3.3.25 Is the previous result true if A is noncommutative?

▪ **Example C.3.3.26 — The algebraic elements need not form a ring** We leave this as an exercise.

Exercise C.3.3.27 Find such a counter-example.

R Hint: See mathoverflow.

Theorem C.3.3.28 — Rings have weakly algebraically closed extensions. Let $\mathbb{K}$ be a (commutative) ring. Then, there exists a (commutative) weakly algebraically closed extension A of $\mathbb{K}$.

Furthermore, if $\mathbb{K}$ is field, then A itself taken to be a field.

R Note that A is integrally closed by Proposition C.3.3.5.

Proof. STEP 1: INTRODUCE NOTATION

Define

$$\mathcal{F} := \{f \in \mathbb{K}[x] : f \text{ nonconstant.}\}, \tag{C.3.3.29}$$

$$X := \left\{x_f : f \in \mathcal{F}\right\}, \tag{C.3.3.30}$$

and

$$\mathbb{L} := \mathbb{K}[X]. \tag{C.3.3.31}$$

Intuitively, we have a "variable" x_f for each monic $f \in \mathbb{K}[X]$ and $\mathbb{L}$ is the polynomial algebra in those variables. Now define

$$I := \left\{\sum_{f \in \mathcal{F}} g_f f(x_f) h_f : g_f, h_f \in \mathbb{L}\right\}, \tag{C.3.3.32}$$

the ideal "generated by" the $f(x_f)$s.

STEP 2: CONSTRUCT A $\mathbb{K}$-ALGEBRA THAT CONTAINS A ROOT FOR EVERY NONCONSTANT $f \in \mathbb{K}[x]$
Now define

$$\mathbb{K}_1 := \mathbb{L}/I. \tag{C.3.3.33}$$

$\mathbb{K}_1$ is a $\mathbb{K}$-algebra, and furthermore, it contains a root of every nonconstant $f \in \mathbb{K}[x]$, namely $x_f + I \in \mathbb{K}_1$.[a]

STEP 3: REPEAT THIS PROCESS INDUCTIVELY
Performing the same construction, we obtain a $\mathbb{K}_1$-algebra $\mathbb{K}_2$ that contains a root of every nonconstant $f \in \mathbb{K}_1[x]$. Note that $\mathbb{K}_2$ can also be considered a $\mathbb{K}$-algebra via the composite structure map $\mathbb{K} \to \mathbb{K}_1 \to \mathbb{K}_2$. Proceeding inductively, we

obtain a sequence of $\mathbb{K}$-algebra $\{\mathbb{K}_m : m \in \mathbb{N}\}$ such that $\mathbb{K}_{m+1}$ contains roots of every nonconstant $f \in \mathbb{K}[x]$.[b]

STEP 4: DEFINE THE WEAKLY ALGEBRAICALLY CLOSED $\mathbb{K}$-ALGEBRA

Now define[c]

$$\mathbb{K}_\infty := \bigcup_{m\in\mathbb{N}} \mathbb{K}_m. \tag{C.3.3.34}$$

STEP 5: CHECK THAT $\mathbb{K}_\infty$ IS INDEED WEAKLY ALGEBRAICALLY CLOSED

We claim that $\mathbb{K}_\infty$ is algebraically closed. So, let $f \in \mathbb{K}_\infty[x]$ be nonconstant. Then, as f has finitely many terms, there is some $m \in \mathbb{N}$ such that $f \in \mathbb{K}_m[x]$. But we know that f then has a root in $\mathbb{K}_{m+1}$, and hence in $\mathbb{K}_\infty$. Thus, $\mathbb{K}_\infty$ is algebraically closed.

STEP 6: CHECK THAT $\mathbb{K}_\infty$ IS COMMUTATIVE IF $\mathbb{K}$ IS

Looking at the above proof, we see that $\mathbb{L}$ is commutative if $\mathbb{K}$ is, and hence $\mathbb{K}_1$ is commutative if $\mathbb{K}$ is. Thus, each $\mathbb{K}_m$ is commutative if $\mathbb{K}$ is, and hence so is $\mathbb{K}_\infty$.

STEP 7: CHECK THAT $\mathbb{K}_\infty$ IS AN EXTENSION

We leave this as an exercise.

Exercise C.3.3.35 Finish this step.

STEP 8: CHECK THE EXTRA PROPERTIES IF $\mathbb{K}$ IS A FIELD

Suppose that $\mathbb{K}$ is a field. We show in this case that $1 \notin I$. If it were, we could write

$$g_1 f_1(x_{f_1}) + \cdots + g_m f_m(x_{f_m}) = 1 \tag{C.3.3.36}$$

for $g_k \in \mathbb{L}$. For convenience, let us write $x_k := x_{f_k}$, and enumerate any remaining variables that appear in any g_k as $x_{m+1}, \ldots, x_n$, so that this equation then reads

$$g_1(x_1, \ldots, x_n) f_1(x_1) + \cdots + g_m(x_1, \ldots, x_n) f_m(x_m) = 1.$$

Define $A_1 := \mathbb{K}[x]/I_1$, where $I_1 := \{a f_1(x) b : a, b \in \mathbb{K}\}$, the ideal "generated" by f_1. A_1 is a $\mathbb{K}$-algebra that contains a root of f_1 (namely $x + I_1 \in A_1$), and furthermore, the image of $1 \in \mathbb{K}$ under the quotient map $\mathbb{K} \to A_1$ is nonzero, for if it were, we would have $1 = a f_1(x) b$ for some $a, b \in \mathbb{K}$, in which case $f_1(x)$ would be a constant polynomial, a contradiction. We may now define $A_2 := A_1[x]/I_2$, where $I_2 := \{a f_2(x) b : a, b \in \mathbb{K}_1\}$. As before, A_2 is a $\mathbb{K}$-algebra that now contains roots of both f_1 and f_2, and furthermore, the image of $1 \in \mathbb{K}$ under the map $\mathbb{K} \to A_2$ is nonzero. Proceeding inductively, we obtain a $\mathbb{K}$-algebra A_m that contains roots of $f_1, \ldots, f_m$ and $1 \neq 0$ in A_m. Plugging in these roots for $x_1, \ldots, x_m$ respectively (and anything for the remaining variables), the above equation reduces to $0 = 1$ in A_m: a contradiction.[d] Thus, $1 \notin I$.

We just showed that $1 \notin I$, and so in particular $I \subseteq \mathbb{L}$ is a proper ideal. It is thus contained in a maximal ideal M, in which case let us replace our definition of $\mathbb{K}_1$ in (C.3.3.33) by

$$\mathbb{K}_1 := \mathbb{L}/M. \tag{C.3.3.37}$$

$\mathbb{K}_1$ now has all the properties it did before, except now it is additionally a field. Proceeding inductively, we find that each $\mathbb{K}_m$ is a field. Then, for $x \in \mathbb{K}_\infty$ nonzero, we have that $x \in \mathbb{K}_m$ for some $m \in \mathbb{N}$, in which case x has an inverse in $\mathbb{K}_m$, and hence in $\mathbb{K}_\infty$. Thus, $\mathbb{K}_\infty$ is likewise a field. ■

[a] This is a root because, as $f(x_f) \in I$ (from the definition of I), $f(x_f + I) = f(x_f) + I = 0$ in $\mathbb{L}/I$.

[b] Take $\mathbb{K}_0 := \mathbb{K}$.

[c] This definition doesn't literally make sense as we don't literally have that $\mathbb{K}_m \subseteq \mathbb{K}_{m+1}$. Instead, what is actually meant is the disjoint union of the $\mathbb{K}_m$s modulo the equivalence relation that identifies elements in $\mathbb{K}_m$ with their images in $\mathbb{K}_{m+1}$.

[d] If $\mathbb{K}$ were noncommutative, then these terms wouldn't just be of the form $g_k f_k$, but rather, $g_k f_k h_k$, and now, the result we get by plugging in the root α_k is not necessarily equal to $g_k(\alpha_k) f_k(\alpha_k) h_k(\alpha_k)$. This seems to break the proof for $\mathbb{K}$ noncommutative.

Exercise C.3.3.38 In the above result, if $\mathbb{K}$ is a division ring, can we still take A to be an extension of $\mathbb{K}$? Can we take A to be simple?

Theorem C.3.3.39 — Integral closure. Let $\mathbb{K}$ be a cring. Then, there is a unique commutative integral closure $\mathbb{A}_{\mathbb{K}}$ of $\mathbb{K}$ which is an extension of $\mathbb{K}$.

Furthermore, if $\mathbb{K}$ is a field, then $\mathbb{A}_{\mathbb{K}}$ itself is a field.

R While it is true (Theorem C.3.3.28) that any ring $\mathbb{K}$ has an algebraically closed $\mathbb{K}$-algebra, it is *not* true that rings, even commutative ones, have algebraic closures. Essentially this boils down to the fact that the algebraic elements need not form a ring (Example C.3.3.26), whereas the integral ones do (Proposition C.3.3.22).

R For the purpose of (hopefully) increasing clarity, we are actually being sloppy in a couple of places here. First of all, when we say "unique", what we actually mean is that $\mathbb{A}$ is "unique up to isomorphism"[a] in the sense that, if A is some other integrally closed $\mathbb{K}$-algebra that satisfies this property, then there is an isomorphism (of $\mathbb{K}$-algebras) $\mathbb{A} \to A$.

R In the important case $\mathbb{K}$ is a field, there is no distinction between integral and algebraic (Meta-proposition C.3.3.15), and so in this context people almost always just say "algebraic closure".

R Warning: As far as I know, the integral closure does not satisfy any universal property—see math.stackexchange. As such, while $\mathbb{A}_{\mathbb{K}}$ is unique up to isomorphism, it is not unique up to *unique* isomorphism.

For example, it's also true that there is only one, up to isomorphism, d-dimensional vector space over $\mathbb{R}$—would you carelessly make no distinction between $\mathbb{R}^d$ and $\mathbb{R}[x]_{d-1}$ as a result? Probably not most of the time. Keep this in mind any time you want to say "*the* integral closure"—it probably won't break anything, but, as I said, you should at least keep this in mind.

[a] But not unique isomorphism!

Proof. Step 1: Existence
By Theorem C.3.3.28, there is a commutative integrally closed $\mathbb{K}$-algebra A. Take A to be a field if $\mathbb{K}$ is. Define

$$\mathbb{A}_{\mathbb{K}} = \{x \in A : x \text{ is integral over } \mathbb{K}.\}. \tag{C.3.3.40}$$

By Proposition C.3.3.22, $\mathbb{A}_{\mathbb{K}}$ is still a commutative integrally closed $\mathbb{K}$-algebra, which is a field if $\mathbb{K}$ is. By construction, it is integral over $\mathbb{K}$, and hence an integral closure of $\mathbb{K}$.

Step 2: Uniqueness
We leave this as an exercise.

Exercise C.3.3.41 Prove the result.

R Hint: Show that any integral extension A of $\mathbb{K}$ embeds in $\mathbb{A}_{\mathbb{K}}$ by using Zorn's Lemma to find a map into $\mathbb{A}_{\mathbb{K}}$ with maximal domain—see math.stanford.edu.

■

Exercise C.3.3.42 Do noncommutative rings have (left/right) integral closures? What about noncommutative division rings in particular?

One of the most significant implications of the existence of an algebraic closure is that they permit us to make the following definitions.

Definition C.3.3.43 — Absolute root Let $\mathbb{F}$ be a field, let $\mathbb{A}_{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$, and let $p \in \mathbb{F}[x]$. Then, a ***root*** of p is a root of p in $\mathbb{A}_{\mathbb{F}}$.

R Warning: Note that this *does* technically depend on a choice of algebraic closure. Thus, if we ever use the word "root" in this sense, it should be implicitly understood that we chose an algebraic closure before hand. As algebraic closures are unique up to isomorphism, this seldom will make a difference (at least for us), but it's still good to keep in mind.

R Of course, $\mathbb{A}_{\mathbb{F}}$ exists by the previous result. Note that we need $\mathbb{F}$ to be a field, otherwise we are only guaranteed that only *monic* polynomials have roots.

Proposition C.3.3.44 — Generated field Let $\mathbb{F}$ be a field, let $\mathbb{A}$ be an algebraic closure of $\mathbb{F}$, and let $S \subseteq \mathbb{A}$. Then, there exists a unique subfield $\mathbb{F}(S)$ of $\mathbb{A}$, the subfield ***generated*** by S, such that

(i). $S \subseteq \mathbb{F}(S)$; and
(ii). if $\mathbb{K} \subseteq \mathbb{A}$ is any other subfield containing S, it follows that $\mathbb{F}(S) \subseteq \mathbb{K}$.

R If $S =: \{s_1, \ldots, s_m\}$ is finite, people typically write

$$\mathbb{F}(s_1, \ldots, s_m) := \mathbb{F}(S). \tag{C.3.3.45}$$

Proof. We leave this as an exercise.

Exercise C.3.3.46 Prove the result.

■

C.3.4 Summary

We started out with the objective of being able to solve polynomial equations over a given field. This gives us the concept of *algebraic closure* (Meta-definition C.3.3.19), though we found that the related concept of *integral closure* (Meta-definition C.3.3.20) was better-behaved in general (Proposition C.3.3.22 and Example C.3.3.26), and in any case agree with the algebraic closure for division rings (Meta-proposition C.3.3.15).

To talk about such things, we needed to discuss $\mathbb{K}$-algebras (Definition C.3.1.1), algebraic and integral $\mathbb{K}$-algebras (Meta-definitions C.3.3.17 and C.3.3.18, and what it meant for these algebras to be algebraically closed and integrally closed (Definitions C.3.3.1 and C.3.3.2).

Finally, we proved that every cring has a unique integral closure that is an extension and a field if the cring was (Theorem C.3.3.39).

Of course, there were other things, but these are the bullet-points.

C.4 Perfect fields

To be honest, the intuition for what are called *perfect fields* is hard for me to describe. For us, the motivation is simple: (i) every field we encounter in these notes (with exception of the one I construct below simply for the purpose of producing a field that is not perfect) is perfect and (ii) this is the most general sufficient condition on the ground field I am aware of in order for the Jordan-Chevalley Decomposition (Theorem 4.6.4) to hold. It is important for you to know the statement of Jordan-Chevalley, and it's also important to know that it's going to work for a very large class of fields, almost certainly a class large enough that it contains every field you've ever seen before if you're learning linear-algebra for the first time. On the other hand, it is not important for you to know the details of the theory of perfect fields.

So I basically just told you that you shouldn't care about the details about perfect fields, only that essentially everything you'll encounter in the notes is perfect, and so the Jordan-Chevalley Decomposition can be applied. If you're one of those pesky students[5] that likes to know everything "beyond the scope of this course", that's probably not very satisfying, so let me try a little bit harder to motivate perfect fields.

The proof of Jordan-Chevalley uses Galois theory, and, in some sense, perfect fields make Galois theory 'work'. The largest extension of a given field that is Galois its what's called its *separable closure*, which is contained in the algebraic closure. However, the algebraic closure is more intuitive[6], and so it would be nice if Galois theory would work over the algebraic closure. Unfortunately, that's not always the case. In fact, a field is *perfect* iff the separable closure and algebraic closure coincide. Thus, in this sense, perfect fields are precisely the fields in which Galois theory "works" over the algebraic closure.

Anyways, let's get started.

Definition C.4.1 — Separable polynomial Let $\mathbb{F}$ be a field and let $p \in \mathbb{F}[x]$. Then, p is ***separable*** iff the number of distinct roots of p is equal to $\deg(p)$.

R Note that we need to work over a field here as we are implicitly making using of an algebraic closure—see Definition C.3.3.43.

R Intuitively, we think of all the roots of p having "multiplicity 1". Sometimes people say that "p has distinct roots".

R I'm not quite sure where the word "separable" comes from. Perhaps it comes from the fact that, in an algebraic closure, you can 'separate' p into *distinct* linear factor, though I think this is misleading as you can "separate" any polynomial into linear factors, they just won't necessarily be distinct.

[5] That's a joke. Such students are the best type of students.

[6] At least for me.

Definition C.4.2 — Perfect field Let $\mathbb{F}$ be a field. Then, $\mathbb{F}$ is ***perfect*** iff every irreducible polynomial $p \in \mathbb{F}[x]$ is separable.

$\mathbb{F}$ is ***imperfect*** iff it is not perfect.

R For a ring R and $x \in R$ not a unit, x is ***irreducible*** iff whenever $x = ab$, it follows that either a or b is a unit.[a]

This definition of irreducible is one generalization of the concept of a prime integer to a general ring (there are others).

[a] Recall that (Definition A.4.16) a unit is an element with a multiplicative inverse.

There are several conditions one may impose on a field that are equivalent to being perfect.

Theorem C.4.3. Let $\mathbb{F}$ be a field. Then, the following are equivalent.

(i). $\mathbb{F}$ is perfect.
(ii). Either $\mathrm{Char}(\mathbb{F}) = 0$, or $\mathrm{Char}(\mathbb{F}) =: p$ and $\mathbb{F} \ni x \mapsto x^p \in \mathbb{F}$ is a ring automorphism.
(iii). Either $\mathrm{Char}(\mathbb{F}) = 0$, or $\mathrm{Char}(\mathbb{F}) =: p$ and $\mathbb{F} \ni x \mapsto x^p \in \mathbb{F}$ is surjective.

Proof. We leave this as an exercise.

Exercise C.4.4 Prove the result.

■

Most fields you have probably encountered are perfect.

Proposition C.4.5 Let $\mathbb{F}$ be a field. Then, $\mathbb{F}$ is perfect if any of the following are true.

(i). $\mathbb{F}$ is algebraically closed.
(ii). $\mathrm{Char}(\mathbb{F}) = 0$.

(iii). $\mathbb{F}$ is finite.

Proof. We leave this as an exercise.

Exercise C.4.6 Prove the result.

■

Of course, there are examples of imperfect fields.

Exercise C.4.7 — The Freshman's Dream Let $\mathbb{F}$ be a field with $p := \mathrm{Char}(\mathbb{F}) \neq 0$. Show that

$$(x + y)^p = x^p + y^p \tag{C.4.8}$$

for all $x, y \in \mathbb{F}$.

R Hint: Use the Binomial Theorem and argue that the binomial coefficients must vanish (except of course for the first and last ones, both of which are just 1).

▪ **Example C.4.9 — An imperfect field** Let $p \in \mathbb{Z}^+$ be prime, write $\mathbb{F}_p := \mathbb{Z}/p\mathbb{F}$, and define $\mathbb{F} := \mathbb{F}_p(t)$.[a]

We claim that $\mathbb{F}$ is imperfect. To show this, we check that $x^p - t \in \mathbb{F}[x]$ is irreducible but does not have distinct roots.

Exercise C.4.10 Show that $x^p - t \in \mathbb{F}[x]$ is irreducible.

If x_0 is a root of $x^p - t$, then $x_0^p - t = 0$, and hence $t = x_0^p$. But then

$$x^p - t = x^p - x_0^p = (x - x_0)^p, \tag{C.4.11}$$

and hence $(x - x_0)^p$ divides $x^p - t$. As $p \geq 2$, $x^p - t$ cannot have distinct roots.

R This example is quite unimportant for us, and so you shouldn't worry if you don't understand everything going on here.

[a]For any cring $\mathbb{K}$, $\mathbb{K}(x)$ is the *field of fractions* of $\mathbb{K}[x]$. That is, $\mathbb{K}(x)$ is constructed from $\mathbb{K}[x]$ in the same way that $\mathbb{Q}$ is constructed from $\mathbb{Z}$.

C.5 (Semi)simplicity

There is a fundamental concept in the theory of modules called *simplicity*. Indeed, the concept is sufficiently fundamental that direct analogues[7] appear throughout algebra.

Definition C.5.1 — Simple module Let V be an R-module. Then, V is ***simple*** iff the only submodules of V are 0 and V itself.

R Sometimes the term ***irreducible*** is used as a synonym for "simple". As far as I can tell, "irreducible" seems to be the preferred term in the context of representation theory. I will use both, depending on what feels most 'natural' to me in a given context.

R You should compare this with the definition of indecomposability (Definition 4.4.2.15).

Proposition C.5.2 Let V be an R-module. Then, if V is irreducible, V is indecomposable.

Proof. Suppose that V is irreducible. Let $U, W \subseteq V$ be submodules such that $V = U \oplus W$. As V is irreducible, either $U = 0$ or $U = V$. In the former case, we are done. In the latter case, we must have $W = 0$, and we are again done. ∎

[7]And nonanalogues *cough*Lie algebras*cough*.

▪ **Example C.5.3 — An indecomposable module that is not irreducible** Define

$$N := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \tag{C.5.4}$$

and use $\mathbb{N}$ to regard $\mathbb{C}^2$ as a $\mathbb{C}[x]$-module as in Example 4.4.2.1.

Exercise C.5.5 Show that

$$\text{Span}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) \tag{C.5.6}$$

is N-invariant. Deduce that $\mathbb{C}^2$ is not irreducible as a $\mathbb{C}[x]$-module.

Exercise C.5.7 Show that $\mathbb{C}^2$ is not an indecomposable $\mathbb{C}[x]$-module.

We had a term (Proposition 4.4.2.16), *complete-decomposability*, for a module that can be written as a direct-sum of indecomposable modules. So to, we have an analogous term for irreducible modules.

Definition C.5.8 — Semisimple module Let V be an R-module. Then, V is ***semisimple*** iff V can be written as the direct-sum of simple submodules.

R Just as the term "irreducible" is used as a synonym for "simple", the term ***completely-reducible*** is used as a synonym for "semisimple".

R A linear operator $T\colon V \to V$ on a $\mathbb{K}$-module V is ***semisimple*** iff the $\mathbb{K}[x]$-module defined by the action of T is semisimple.

R By Proposition C.5.2, we immediately see that completely-reducible implies completely-indecomposable, but that the converse fails (Example C.5.3).

R Warning: As previously mentioned in the definition of simple ring (Definition C.2.3.1), there is a definition of "semisimple ring", but it is not analogous to "semisimple module" in the way that "simple ring" is analogous to "simple module".

Theorem C.5.9 — Fundamental Theorem of Semisimple Modules. Let V be a $\mathbb{K}$-module. Then, the following are equivalent.

(i). V is semisimple.
(ii). V is a sum of simple submodules.
(iii). For every submodule $W \subseteq V$, there is a submodule $U \subseteq V$ such that $V = U \oplus W$.

R In other words, (iii) says that V is semisimple iff every submodule has a complement.

R Warning: Again, the name of this result is nonstandard.

Proof. We leave this as an exercise.

Exercise C.5.10 Prove the result.

■

Our interest in semisemplicity arises from the fact that semisimple operators are in a certain sense a generalization of diagonalizable operators.

Theorem C.5.11 — Semisimple (linear operator). Let $\mathbb{K}$ be a field, let $\mathbb{A}$ be an algebraic closure of $\mathbb{K}$, let V be a finite-dimensional vector space over $\mathbb{K}$, write $V^{\mathbb{A}} := \mathbb{A} \otimes_{\mathbb{K}} V$, and let $T : V \to V$ be a linear operator. Then, the following are equivalent.

(i). The minimal polynomial of T is separable.
(ii). $T\colon V^{\mathbb{A}} \to V^{\mathbb{A}}$ is diagonalizable.
(iii). The $\mathbb{K}[x]$-module V_T defined by T is semisimple.
(iv). Every T-invariant subspace has a T-invariant complement.

R If these conditions are satisfied, then we say that T is ***semisimple***.

Proof. $((i) \Rightarrow (ii))$ Suppose that the minimal polynomial of T is separable. Denote this minimal polynomial by p and write $p(x) = (x-\lambda_1)\cdots(x-\lambda_m)$, with $\lambda_1, \ldots, \lambda_m$ all distinct. By the Jordan Canonical Form Theorem, we can pick a basis $\mathcal{B}$ for $V^{\mathbb{A}}$ such that $[T]_{\mathcal{B}} = D + N$ where D is a matrix with $\lambda_1, \ldots, \lambda_m$ along the diagonal (each listed a number of times equal to their algebraic multiplicity as roots of the characteristic polynomial), N a matrix of all 0s except for possibly some 1s above the super-diagonal, and $DN = ND$, where $d := \dim(V^{\mathbb{A}})$ Plugging $D + N$ into p, we see that if $N \neq 0$, then $p(D + N) \neq 0$: a contradiction. Therefore, $T\colon V^{\mathbb{A}} \to V^{\mathbb{A}}$ is diagonalizable.

$((ii) \Rightarrow (i))$ Suppose that $T\colon V^{\mathbb{A}} \to V^{\mathbb{A}}$ is diagonalizable. Let $\lambda_1, \ldots, \lambda_m$ denote the distinct eigenvalues of T. Then, $(T - \lambda_1)\cdots(T - \lambda_m) = 0$, and so the minimal polynomial of T cannot have roots of multiplicity more than 1, i.e. is separable.

$((i) \Rightarrow (iii))$ Suppose that the minimal polynomial of T is separable. Let $\mathbb{F}$ be the splitting field of the minimal polynomial of T over $\mathbb{K}$. As the minimal polynomial of T is separable, the extension $\mathbb{K} \hookrightarrow \mathbb{F}$ is Galois.

As $\mathbb{F}$ contains the roots of the minimal polynomial of T, $T\colon V_{\mathbb{F}} \to V_{\mathbb{F}}$ must have an eigenvalue λ. Let $e \in V_{\mathbb{K}(\lambda)} \subseteq V_{\mathbb{F}}$ be a corresponding eigenvector. The orbit of λ under the Galois group consist of precisely the roots of the minimal polynomial of λ. In particular, the number of elements in the orbit of λ

is exactly the degree d of the minimal polynomial of λ (recall that Galois groups transitively permute the roots of irreducible polynomials). Thus, $W' \coloneqq \text{Span}\{\sigma(e) : \sigma \in \text{Gal}(\mathbb{F}/\mathbb{K})\} \subseteq V_{\mathbb{F}}$ has dimension d. So, let $\{b_1, \ldots, b_d\} \subseteq V$ be such that $e = b_1 + \lambda b_2 + \cdots + \lambda^{d-1} b_d$,[a] and define $W \coloneqq \text{Span}\{b_1, \ldots, b_d\} \subseteq V$, so that $W_{\mathbb{F}} = W$. As $T(e) = \lambda e$, it follows that[b] $T(b_1) = -c_0 b_d$, $T(b_2) = b_1 - c_1 b_d$, $T(b_3) = b_2 - c_2 b_d$,..., $T(b_d) = b_{d-1} - c_{d-1} b_d$, where $m_\lambda(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$ is the minimal polynomial of λ. (These equations ensure that $T(e) = \lambda e$). Thus, we have that

$$[T]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{d-1} \end{bmatrix}, \tag{C.5.12}$$

where $\mathcal{B} \coloneqq \{b_1, \ldots, b_d\}$. Thus, $W \coloneqq \text{Span}\{b_1, \ldots, b_d\}$ is a simple submodule of V (note that $c_0 \neq 0$). Doing this for each orbit of eigenvalues under the Galois group, as V is finite-dimensional, we can decompose V into a direct sum of such simple submodules, so that V is semisimple.

($(iii) \Rightarrow (ii)$) Suppose that the representation $\rho\colon \mathbb{K} \to \mathfrak{gl}(V)$ defined by $\rho(1) \coloneqq T$ is semisimple. By the Jordan Canonical Form Theorem, we can write $T = S + N$ for unique linear maps $S, N\colon V \to V$ that satisfy (i) $S\colon V^{\mathbb{A}} \to V^{\mathbb{A}}$ is diagonalizable, (ii) N is nilpotent, and (iii) $SN = NS$. Thus, to prove the result, it suffices to show that $N = 0$. Write $V \coloneqq V_1 \oplus \cdots \oplus V_m$, where each V_k is a simple subrepresentation of V. Thus, $T(V_k) \subseteq V_k$, and no nonzero proper subspace of V_k has this property. For each k, we can apply the Jordan Canonical Form Theorem again to obtain $T|_{V_k} = S_k + N_k$. From uniqueness, we must have that $S = S_1 \oplus \cdots \oplus S_m$ and $N = S_1 \oplus \cdots \oplus S_m$. Thus, each V_k is in fact invariant under both S and N as well. Define $W_k \coloneqq N(V_k) \subseteq V_k$. W_k is of course invariant under N, and so S and N commute, it is also invariant under S, and hence

invariant under T. Therefore, either $W_k = V_k$ or $W_k = 0$. If $W_k := N(V_k) = V_k$, then N will not be nilpotent. Therefore, we must have that $W_k := N(V_k) = 0$, whence it follows that $N = 0$, as desired.

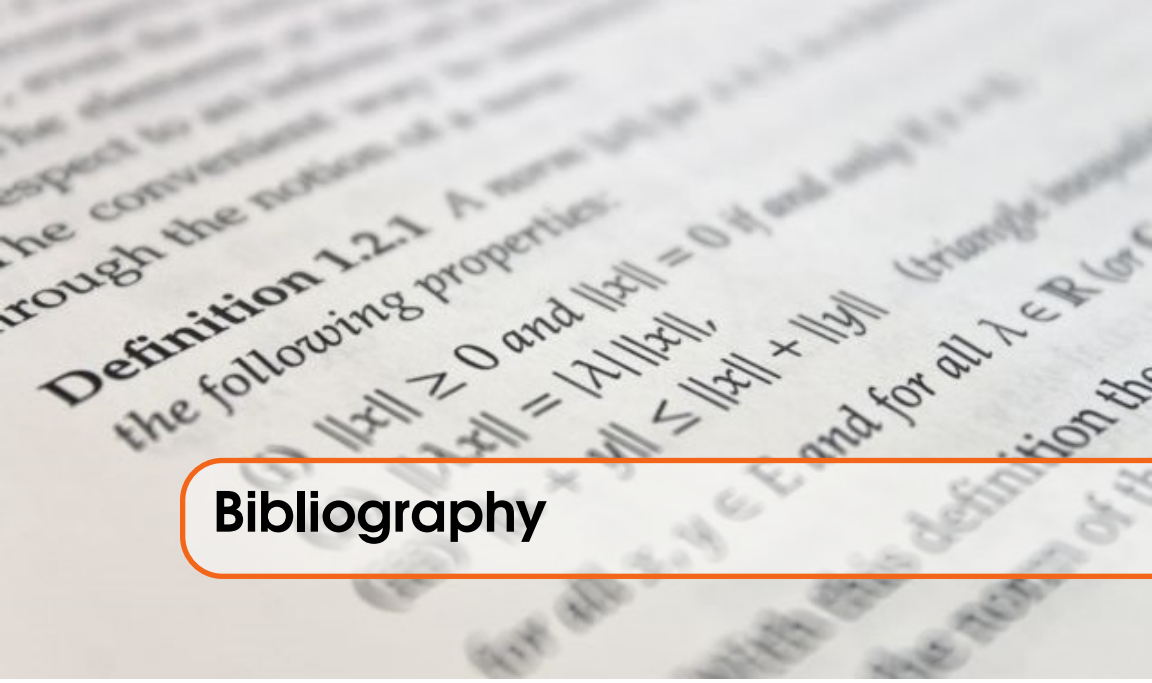
$((iii) \Rightarrow (iv))$ Suppose that the representation $\rho\colon \mathbb{K} \to \mathfrak{gl}(V)$ defined by $\rho(1) := T$ is semisimple. Write $V = V_1 \oplus \cdots \oplus V_m$ for simple subrepresentations $V_k \subseteq V$. Let $W \subseteq V$ be a T-invariant subspace. Then, reordering the V_ks if necessary, without loss of generality $W = V_1 \oplus \cdots \oplus V_n$ for $n \leq m$. Then, $V_{n+1} \oplus \cdots \oplus V_m$ is a T-invariant complement of W.

$((iv) \Rightarrow (iii))$ Suppose that every T-invariant subspace has a T-invariant complement. We proceed by induction of $\dim(V)$. If $\dim(V) = 1$, then V is in fact simple. Now, suppose that the result is true for all representations of $\mathbb{K}$ defined by $1 \mapsto T$ of dimension at most $d - 1$, and let suppose that $\dim(V) = d$. If V itself is simple, we are done. Otherwise, there is a proper nonzero T-invariant subspace $U \subset V$. By hypothesis, U has a T-invariant complement W, and so we have $V = U \oplus W$ as representations. By the induction hypothesis, U and W are both semisimple, and so V is likewise semisimple. ■

---

[a] As $e \in V_{\mathbb{Q}(\lambda)}$, for any basis $\{b_1, \ldots, b_D\}$ of V, we can write $e = \sum_{i=0}^{d-1} \sum_{k=1}^{D} c_{ik} \lambda^i b_k = b'_0 + \lambda b'_1 + \cdots + \lambda^{d-1} b'_{d-1}$ for some $c_{ik} \in \mathbb{K}$, where we have defined $b'_i := \sum_{k=1}^{D} c_{ik} b_k \in V$.

[b] Let $\{e, \sigma_1(e), \ldots, \sigma_{d-1}(e)\}$ be a basis for W'. We have that $\sigma_k(e) = b_1 + \sigma_k(\lambda) b_1 + \sigma_k(\lambda^{d-1}) b_d$ for each σ_k ($\sigma_0 := \mathrm{id}$). These d equations allow us to uniquely solve for each b_j in terms of the $\sigma_k(e)$s (the matrix of coefficients has to be invertible in order for the $\sigma_k(e)$s to be linearly-independent). Applying T to this equation gives d equations of the form $\sigma_k(\lambda)\sigma(e) = T(b_1) + \sigma_k(\lambda) T(b_2) + \cdots + \sigma_k(\lambda^{d-1}) T(b_d)$. Thus, similarly, the $T(b_j)$s are uniquely determined by these d equations, and so, if we can find some expression for each $T(b_j)$ that satisfies these equations, then it must be the correct one. On the other hand, as all the d equations are obtained from the first by applying σ_ks, if we can find expressions for each $T(b_j)$ that satisfies the equation $\lambda e = T(b_1) + \lambda T(b_2) + \cdots + \lambda^{d-1} T(b_d)$, then they must be the correct ones!



Bibliography

[Abb02] Stephen Abbot. *Understanding Analysis*. 2nd. Undergraduate Texts in Mathematics. Springer-Verlag, 2002. ISBN: 978-0387950600.

[Axl15] Sheldon Axler. *Linear Algebra Done Right*. Undergraduate Texts in Mathematics. Springer-Verlag, 2015.

[B C90] John B. Conway. *A Course in Functional Analysis*. 2nd ed. Graduate Texts in Mathematics 96. Springer, 1990. ISBN: 0-387-97245-5.

[C L12] David C. Lay. *Linear Algebra and its applications*. 4th ed. Addison-Wesley, 2012. ISBN: 978-0-321-38517-8.

[Con17] Keith Conrad. *Zorn's Lemma and some applications*. University of Connecticut. 2017. URL: http://www.math.uconn.edu/~kconrad/blurbs/zorn1.pdf (visited on 06/20/2017).

[Gle17] Jonathan Gleason. "Introduction to Analysis". 2017. URL: https://www.academia.edu/15037429/Introduction_to_Analysis (visited on 07/29/2017).

[Gra07] Daniel R. Grayson. *Zorn's Lemma*. 2007. URL: http://www.math.uiuc.edu/~dan/ShortProofs/Zorn.pdf.

[HJS02] Stephen H. Friedberg, Arnold J. Insel, and Lawrence E. Spence. *Linear Algebra*. 4th ed. Pearson, 2002.

[Hön] Chaim Samuel Hönig. *Proof of the well-ordering of cardinal numbers*. URL: http://www.ams.org/journals/proc/1954-005-02/S0002-9939-1954-0060558-3/S0002-9939-1954-0060558-3.pdf.

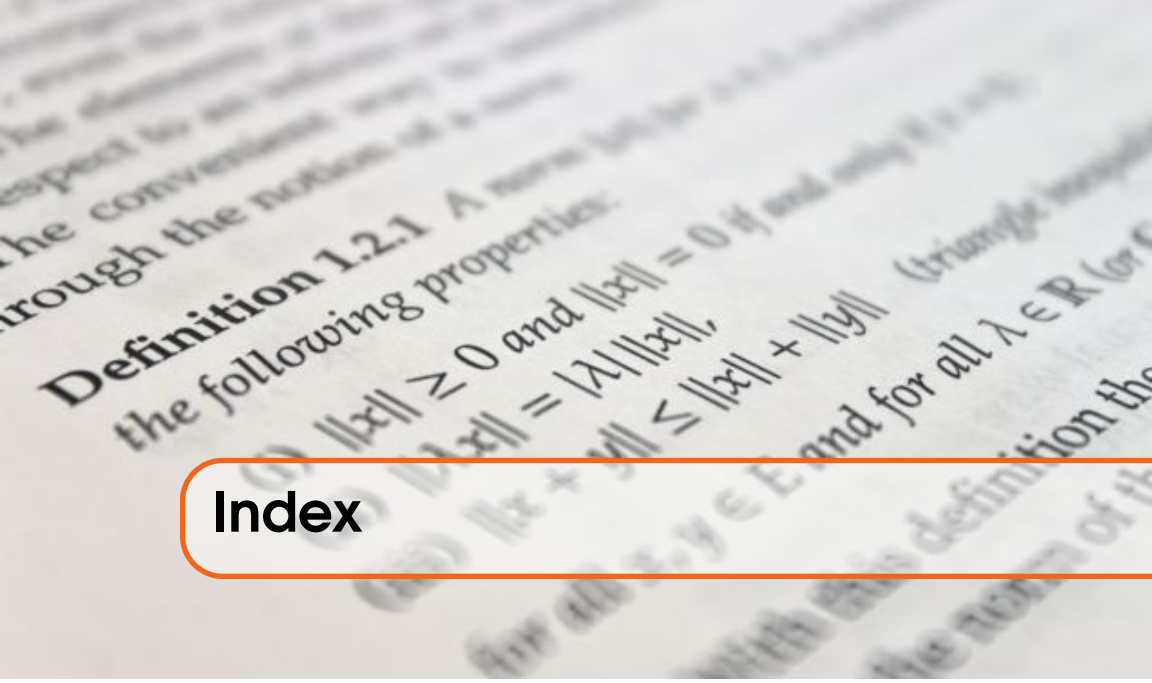
[I M63] I. M. Gel'fand. *Lectures on Linear Algebra*. English. Trans. from the Russian by A. Shenitzer. Interscience Publishers, Inc., 1963.

[Jac89] Nathan Jacobson. *Basic Algebra II*. 2nd ed. W. H. Freeman and Company, 1989. ISBN: 0-7167-1933-9.

[R T05] John R. Taylor. *Classical Mechanics*. University Science Books, 2005.

[SM04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. 3rd ed. John Wiley & Sons, Inc., 2004. ISBN: 0-471-43334-9.

[T Y91] T. Y. Lam. *A Course in Noncommutative Rings*. Graduate Texts in Mathematics. Springer-Verlag, 1991.



Index

N-maximal, 174
$\mathbb{K}$-$\mathbb{L}$ bimodule, 20
$\mathbb{K}$-$\mathbb{L}$-linear transformation, 22
$\mathbb{K}$-algebra, 617
$\mathbb{K}$-module, 2

Absolute value (of an operator), 454
Abstract index notation, 285
Adjoint, 442
Adjugate, 354
Algebraic $\mathbb{K}$-algebra, 636
Algebraic closure, 325, 637
Algebraic closure (of a linear-transformation), 327
Algebraic element, 635
Algebraic extension, 636
Algebraic multiplicity, 184
Algebraically closed, 631
Anti-Hermitian, 447
Anti-self-adjoint, 447
Antisymmetric, 527
Antisymmetric algebra, 319
Antisymmetric product, 314
Antisymmetrization, 311
Antiymmetric (tensor), 308
Argument, 519
Associative, 545
Associative algebra, 618
Augmented matrix, 84
Automorphism, 585

Balanced linear-transformation, 233
Bernstein-Cantor-Schröder Theorem, 562
Bessel's Inequality, 422
Bijective, 521
Bilinear form, 366
Bilinear-transformation, 232
Bimodule-homomorphism, 23
Binary operation, 544

Block-diagonal matrix, 153
Block-diagonalizable, 166
Block-diagonalization, 166
Bounded (linear-transformation), 409
Bra, 391

Cantor's Cardinality Theorem, 574
Cantor's Diagonal Argument, 574
Cardinal number, 561
Cartesian-product, 514, 525
Category, 578
Category of $\mathbb{K}$-modules, 19
Category of functors, 596
Category of magmas, 580
Category of preordered sets, 580
Category of rgs, 581
Category of sets, 579
Category of vector spaces, 19
Cauchy-Schwarz Inequality, 392
Caucy-Bunyakowsky-Schwarz Inequality, 392
Cayley-Hamilton Theorem, 363
Central, 548
Change-of-basis matrix, 109
Characteristic (of a rig), 550
Characteristic polynomial, 360
Closed interval, 534
Codomain (of a function), 518
Codomain (of a morphism), 583
Coefficient matrix, 84
Coextend, 517
Cofactor, 351
Cofinite, 35
Cofunctor, 593
Coimage, 32
Cokernel, 32
Collection, 512
Column (of a matrix), 75
Column space, 96
Column vector, 8
Commutative, 545
Complement, 145, 512
Completely-decomposable module, 168
Completely-reducible module, 650
Complex vector space, 10
Complexification (of a linear-transformation), 327
Complexification (of a vector space), 325
Component (cartesian-product), 525
Component (of a function into a product), 526
Component (of a natural-transformation), 596
Composition, 516, 578
Concrete category, 582

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Conjugate linear-transformation, 383
Conjugate space, 381
Conjugate symmetric, 386
Constant term, 623
Continuous, 406
Continuous (at a point), 406
Contraction, 290
Contrapositive, 499
Contravariant functor, 593
Contravariant rank, 277
Contravariant tensor, 277
Converse, 499
Convex, 432
Coordinate (cartesian-product), 525
Coordinates (of a bilinear form), 369
Coordinates (of a linear-transformation with respect to a decomposition), 157
Coordinates (of a linear-transformation), 100
Coordinates (of a vector with respect to a decomposition), 149
Coordinates (of a vector), 67
Corestriction, 517
Coset, 557
Countably-infinite, 572
Covariant functor, 593
Covariant rank, 277
Covariant tensor, 277
Covectors, 234
Cramer's rule, 355
Crg, 548
Crig, 548
Cring, 548
Crng, 548
Cycle, 306

De Morgan's Laws, 513
Decomposition, 137
Decreasing, 534
Definite form, 386
Degree (of a polynomial), 623
Determinant, 336
Diagonal, 81
Diagonal matrix, 80
Diagonaliation (of a bilinear form), 370
Diagonalizable, 127
Diagonalizable (bilinear form), 370
Diagonalizable (quadratic form), 371
Diagonalization, 127
Differential form, 310
Dimension (of a matrix), 74
Direct-sum, 137
Direct-sum (of linear-transformations), 153
Direct-sum decomposition, 137
Discrete-order, 535
Disjoint, 513
Disjoint-union, 514, 524
Distributive, 548
Division ring, 551

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

DivisionAlgorithm, 624
Domain (of a function), 518
Domain (of a morphism), 583
Dot product, 387
Downward closed, 540
Dual (of a bimodule), 234
Dual (of a linear-transformation), 246
Dual basis, 255
Dual-map, 246
Dual-pair, 243
Dual-space, 234, 410
Dual-vector, 244

Echelon form, 87
Eigenspace, 114
Eigenvalue, 114
Eigenvector, 114
Einstein's equation, 301
Embedding (category theory), 588
Empty-set, 510
Endomorphism, 583
Equinumerous, 560
Equivalence class, 528
Equivalence relation, 528
Evaluation map, 242
Extend, 517
Extension, 622
Extension of scalars, 325
Exterior algebra, 319
External direct-sum, 160

Field, 552
Final space (of a partial-isometry), 480
Form, 310
Free module, 61
Free-variable, 88
Free-variable column, 88
Function, 518
Functor, 590
Fundamental Theorem of Linear Maps, 62

Gauss-Jordan elimination, 93
General algebra, 30
Generalized-eigenspace, 182
Generalized-eigenspace decomposition, 196
Generalized-eigenvalue, 183
Generated ideal, 602
Generated subfield, 644
Geometric multiplicity, 116
Gordon-Motzkin Theorem, 631
Gram-Schmidt Algorithm, 467
Grothendieck universe, 497
Ground ring, 2
Group, 546
Group of units, 549

Hölder's Inequality, 414
Half-closed-open interval, 534
Half-open-closed interval, 534
Hermitian, 447
Hermitian conjugate, 442
Hilbert space, 406
Homomorphism (of magmas), 547
Homomorphism (of rgs), 553
Hyper-connected ring, 605

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Ideal (in a $\mathbb{K}$-module), 30
Ideal (in a group), 556
Ideal (in a ring), 558
Identity (in a category), 578
Identity function, 519
Identity matrix, 82
Iff, 498
Image, 520
Imaginary part (of a linear operator), 448
Imperfect field, 647
Inclusion (disjoint-union), 524
Increasing, 534
Indecomposable module, 167
Index notation, 285
Indexed collection, 524
Indiscrete-order, 535
Infinite, 569
Initial space (of a partial-isometry), 480
Injective, 521
Inner-product, 385
Inner-product space, 386
Integers modulo m, 559
Integral, 551
Integral $\mathbb{K}$-algebra, 636
Integral closure, 637
Integral domain, 551
Integral element, 635
Integral extension, 637
Integrally closed, 631
Intersect, 513
Intersection, 512
Interval, 534
Invariant subspace, 163
Invariant-basis-number property (for modules), 61
Invariant-basis-number property (for rings), 61
Inverse, 499
Inverse (of a function), 520
Irreducible (in a ring), 647
Irreducible module, 649
Isomorphic, 584
Isomorphism, 583

Jordan basis, 197
Jordan block, 193
Jordan canonical form, 197
Jordan normal form, 197

Kernel (of a linear-transformation), 31
Kernel (of a ring homomorphism), 599
Ket, 391
Kronecker delta symbol, 287
Krull's Theorem, 603

Laplace expansion, 349
Leading coefficient, 623
Leading entry, 86
Least-squares-solution, 469
Left coset, 555
Left ideal, 601
Left linear-transformation, 23
Left root, 629
Left-inverse (of a function), 519

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

left-shift operator, 17
Legendre polynomial, 424
Length (of a cycle), 306
Linear operator, 14
Linear-combination, 35
Linear-functional, 234
Linear-transformation, 13
Linear-transformation (of bimodules), 23
Linear-transformation defined by a matrix, 95
Linearly-dependent, 37
Linearly-depenent (subspaces), 139
Linearly-independent, 37
Linearly-independent (subspaces), 139
List, 514
Locally-nilpotent, 181
Lower-bound, 539
Lower-triangular matrix, 80

Magma, 545
Map, 578
Matrix (of a linear-transformation with respect to a basis), 101
Matrix (of linear-transformations), 151
Matrix of minors, 344
Maximal, 539
Maximal ideal, 606
Maximum, 539
Meet, 513
Metric (on a vector space), 298
Min-Max Theorem, 478
Minimal, 539
Minimal polynomial, 211
Minimum, 539
Minkowski's Inequality, 414
Minor, 344
Module homomorphism, 14
Modus ponens, 508
Monic, 623
Monoid, 546
Morphisms, 578
Multilinear-transformation, 232
Multipliable, 76
Multiplicity, 184

Natural numbers, 571
Natural transformation, 595
Natural-isomorphism, 597
Negative index of inertia, 376
Nilpotent, 173
Nondecreasing, 534
Nondegenerate (dual-pair), 244
Nonincreasing, 534
Nonnegative (linear-transformation), 452
Nonnegative form, 386
Nonnegative part, 455
Nonpositive (linear-transformation), 452
Nonpositive part, 455
Nonsingular (dual-pair), 244

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Nonsingular (linear-transformation), 341
Norm, 393
Norm (of an operator), 410
Norm of an inner-product, 393
Normal (linear operator), 456
Normal subgroup, 556
Normalization, 417
Normalized, 417
Null space, 96
Null-space, 31
Nullity, 62

Objects, 578
Open interval, 534
Opposite category, 592
Opposite rg, 552
Ordered pair, 514
Ordinal, 510
Orientation, 358
Oriented vector space, 359
Origin, 10
Orthogonal, 416
Orthogonal (linear-transformation), 449
Orthogonal (subspaces), 417
Orthogonal complement, 249
Orthogonal projection, 464
Orthonormal, 418

Pairing (of a dual-pair), 244
Parallelogram Equality, 396
Parallelogram Identity, 396
Parallelogram Law, 396
Partial-order, 535
Partially-ordered set, 535
Partition, 529
Penrose index notation, 285
Perfect field, 647
Permutation, 306
PID, 604
PIR, 604
Pivot, 88
Pivot column, 88
PolarizationIdentity, 394
Polynomial, 623
Polynomial algebra, 626
Polynomial algebra (single variable), 622
Polynomial function, 628
Poset, 535
Positive index of inertia, 376
Positive-definite, 386
Postfix notation, 4
Power set, 515
Preorder, 533
Preordered set, 533
Primary ring, 611
Prime, 507
Prime ideal, 607
Prime ring, 610
Principal ideal ring, 604
Principla ideal domain instead, 604
Principle of Induction, 507
Principle of Strong Induction, 508
Principle of the Excluded Middle, 504
Principle of Well-Founded Induction, 509
Product (of $\mathbb{K}$-modules), 148
Product of ideals, 602

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Product of matrices, 77
Projection, 146
Projection (cartesian-product), 526
Proof by contradiction, 504
Proof by contraposition, 504
Proper class, 497
Proper subset, 511
Pure tensor, 258
Pythagorean Theorem, 419

QR Factorization, 468
Quadratic form, 366
Quaternionic vector space, 10
Quotient (category theory), 588
Quotient function, 531
Quotient group, 556
Quotient rng, 558
Quotient set, 531
Quotient space, 30

Radical ideal, 607
Radical of an ideal, 607
Radical ring, 610
Range, 520
Rank, 61, 62
Rank m eigenspace, 188
Rank (of a generalized-eigenvector), 188
Rank (of a nilpotent element), 173
Rank (of a tensor), 277
Rational vector space, 10
Rayleigh's Principle, 479
Real part (of a linear operator), 448
Real vector space, 10
Reduced echelon form, 86, 87
Reduced ring, 605
Reflexive, 527
Relation, 515
Relative integral closure, 637
Restriction, 517
Restriction (disjoint-union), 524
Rg, 547
Riesz Representation Theorem, 437
Rig, 549
Right coset, 555
Right ideal, 601
Right linear-transformation, 23
Right root, 629
Right-inverse (of a function), 520
Right-shift operator, 17
Ring, 550
Rng, 549
Rodgrigues' formula, 424
Root, 644
Row (of a matrix), 75
Row operation, 85
Row-equivalent, 86
Row-space, 254
Row-vector, 236
Russel's Paradox, 497

Scalar, 10
Self-adjoint, 447
Semigroup, 545
Seminorm, 393
Semiprime ideal, 607

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Semiprime ring, 610
Semiring, 549
Semisimple (linear operator), 652
Semisimple module, 650
Semisimple operator, 650
Separable polynomial, 646
Sesquilinear, 386
Shift operator, 17
Sign (of a permutation), 307
Signature, 377
Simlar (linear operators), 208
Simple, 610
Simple module, 649
Simple tensor, 258
Singular-value, 483
Skew-field, 551
Small set, 579
Span, 36
Span (of subspaces), 138
Spanning, 37
Spanning (subspaces), 139
Spans, 37
Spans (of subspaces), 139
Square matrix, 80
Square-root (of a nonnegative operator), 453
Standard basis, 45
Statement, 498
Strictly lower-triangular matrix, 80
Strictly upper-triangular matrix, 80
Strong operator topology, 409
Structure morphism (of a $\mathbb{K}$-algebra), 619
sub-Hilbert space, 411
Submodule, 26
Subset, 511
Subspace, 26
Sum of matrices, 75
Super-commutativity, 316
Surjective, 521
Symmetric, 527
Symmetric (tensor), 308
Symmetric algebra, 318
Symmetric group, 306
Symmetric pairing, 298
Symmetric product, 314
Symmetric-difference, 513
Symmetrization, 311

Tensor, 281
Tensor (of rank $\langle k, l \rangle$), 280
Tensor algebra, 281
Tensor of rank $\langle k, l \rangle$, 277
Tensor product (of bimodules), 257
Tensor product (of vectors), 257
Topological span, 412
Total, 527
Total-order, 536
Totally antisymmetric (tensor), 309
Totally symmetric (tensor), 309
Totally-ordered set, 536
Trace, 332
Transcendental element, 635
Transfinite induction, 510
Transitive, 527
Transpose, 246
Transpose (of a matrix), 256

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12

Transposition, 306
Trilinear-transformation, 232
Tuple, 514
Two-sided, 628
Two-sided linear, 23
Two-sided root, 629
Two-sided-inverse (of a function), 520

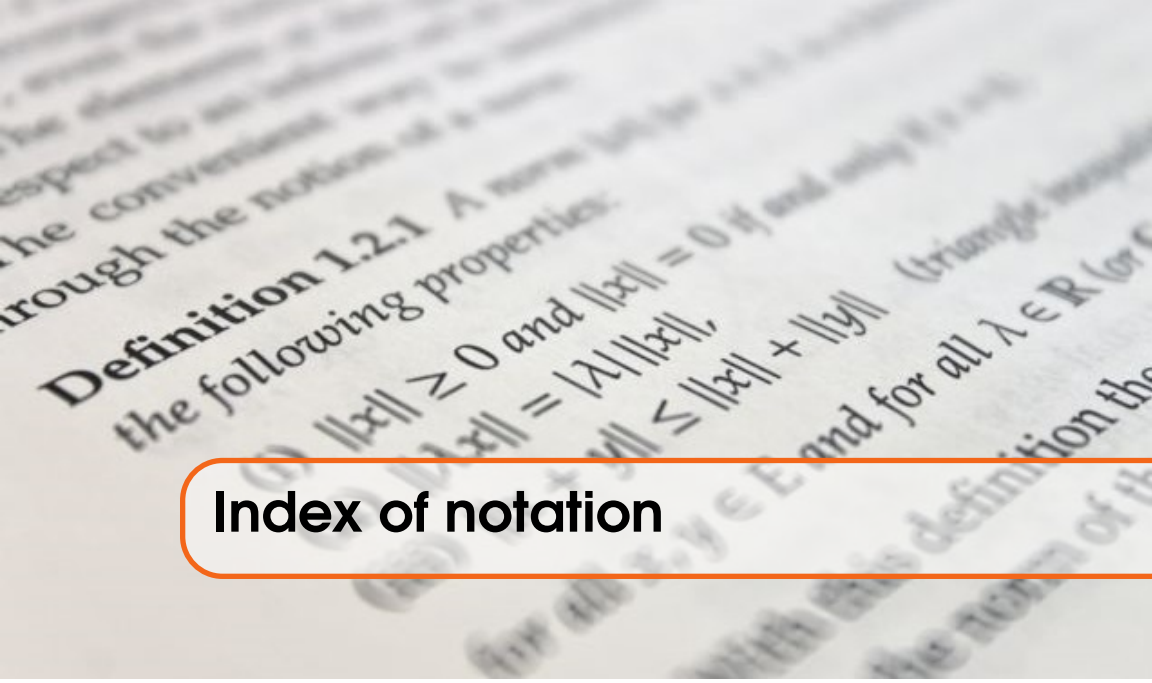
Union, 512
Unitary, 449
Universal algebra, 30
Upper bound, 539
Upper-triangular matrix, 80
Upward closed, 540

Valence, 278
Vector, 10
Vector space, 10
Volume form, 358

Weakly algebraically closed, 631
Weakly integrally closed, 632
Wedge product, 314
Well-defined, 531
Well-founded, 537
Well-founded Induction, 538
Well-order, 536
Well-ordered set, 536

Zero cring, 551
Zorn's Lemma, 541

AMS Open Math Notes: Works in Progress; Reference # OMN:201806.110772; Last Revised: 2018-06-04 09:59:12



Index of notation

$(x_0)p$, 629
$(x_1 \dots x_n)$, 306
2^X, 515
$A + B$, 75
$A \Leftrightarrow B$, 498
$A \Rightarrow B$, 498
$A \triangle B$, 513
$A \cap B$, 512
$A \cong B$, 584
$A \cong_{\mathbf{C}} B$, 584
$A \cup B$, 512
$A^1{}_1 \oplus \cdots \oplus A^m{}_m$, 153
$A^i{}_j$, 74
$A^i{}_\cdot$, 75
$A^\cdot{}_j$, 75
A^*, 445
A^i, 74
A_j, 74
BA, 77
$B \Rightarrow A$, 498
$C^\infty(O)$, 11
G/H, 555
$H\backslash G$, 555
R/S, 557
R^k, 516
$R^\times$, 549
ST, 14
$S \circ R$, 516
$S \odot T$, 314
$S \otimes T$, 264, 272
$S \vee T$, 314
$S \wedge T$, 314
$S^\perp$, 249
$T^{a_1 \cdots a_k}{}_{b_1 \cdots b_l}$, 285
$T^{(a_1 \cdots a_k)}$, 311
$T^{[a_1 \cdots a_k]}$, 311
$T^{\mathbb{L}}$, 326
$T^\dagger$, 246
T_A, 95
V/W, 29
$V \otimes W$, 258
$V \otimes_S W$, 257
$V^{\mathbb{L}}$, 324
$V^\dagger$, 234
$V^{\otimes,\otimes\dagger}$, 281, 282
$V^{\otimes\dagger}$, 282
$V^\otimes$, 282
$V^{k\otimes,l\otimes\dagger}$, 280
$V^{k\otimes}$, 280
$W_1 \oplus \cdots \oplus W_m$, 138
$X \ni x$, 510
$X \setminus Y$, 512
$X \sqcup Y$, 514
$X \subset Y$, 511
$X \subseteq Y$, 511
$X \times Y$, 514
X^{op}, 552
Y^X, 518
Y^{C}, 512
$[x]\mathbb{K}$, 623

$[x_0]$, 528
$[x_0]_\sim$, 528
$\mathbb{A}_\mathbb{K}$, 642
Alg-$\mathbb{K}$, 619
$\mathbb{K}$-**Alg**, 618
$\mathrm{Aut}_\mathbf{C}(A)$, 585
$\mathrm{Cof}(A)_i^j$, 351
$\mathrm{Cof}_\mathcal{B}(T)_j^i$, 351
$\mathrm{Coim}(T)$, 32
$\mathrm{Coker}(T)$, 32
$\mathrm{Col}(A)$, 96
$\mathrm{Eig}(T)$, 114
$\mathrm{Eig}^m_{T,\lambda}$, 188
$\mathrm{Eig}_{\lambda,T}$, 116
$\mathrm{Eig}^\infty_{\lambda,T}$, 184
Eig^m_λ, 188
$\mathrm{Eig}^\infty_\lambda$, 184
$\mathrm{End}_\mathbf{C}(A)$, 583
$\mathbb{F}(S)$, 644
$\mathbb{F}(s_1, \ldots, s_m)$, 644
(S), 602
$(s_1, \ldots, s_m)$, 603
$\mathfrak{I}[T]$, 448
$\mathrm{Im}(f)$, 520
$\mathrm{Iso}_\mathbf{C}(A, B)$, 584
$\mathrm{Jord}_{\lambda,m}$, 193
$\mathbb{K}[X]$, 626
$\mathbb{K}[x]_m$, 11
$\mathbb{K}[x_1, \ldots, x_m]$, 626
$\mathbb{K}^\infty$, 9
$\mathrm{Ker}(T)$, 31
$\mathrm{Ker}(\phi)$, 599
$\Lambda^l(V)$, 309
Mag, 580
Matrix_m, 152
$\mathrm{Matrix}_m(\mathbb{K})$, 82
$\mathrm{Matrix}_{m\times n}$, 152
$\mathrm{Matrix}_{m\times n}(\mathbb{K})$, 82
Mod-$\mathbb{K}$, 19
$\mathbb{K}$-**Mod**, 19
$\mathbb{K}$-**Mod**-$\mathbb{L}$, 23
$\mathrm{Mor}(A, B)$, 578
$\mathrm{Mor}_\mathbf{C}$, 578
$\mathrm{Mor}_\mathbf{C}(A, B)$, 578
$\mathrm{Null}(A)$, 31, 96
$\mathrm{Obj}(\mathbf{C})$, 578
Pre, 580
$\mathrm{Rank}(v)$, 188
$\mathrm{Rank}(x)$, 173
$\mathfrak{R}[T]$, 448
Rg, 581
Rig, 581
Ring, 581
Rng, 581
$\mathrm{Row}(A)$, 254
Set, 579
$\mathrm{Span}(S)$, 36
$\mathrm{Span}(\mathscr{W})$, 138
$\mathrm{Span}(v_1, \ldots, v_m)$, 36
Top$\mathbb{K}$-**Mod**, 407
TopVect$_\mathbb{F}$, 407
Vect$_\mathbb{F}$, 19
Vect, 19
$|T|$, 454
$|X|$, 561
$\aleph_0$, 572
$\bigwedge^k T$, 334
$\bigwedge^k V$, 309
$\bigwedge^\bullet V$, 319
$\bigwedge_l V$, 309
$\bigwedge^k_l V$, 308
$\bigwedge^k_l \mathcal{B}$, 321
$\bigwedge_\bullet V$, 319
$\bigwedge^\bullet_\bullet V$, 319
$\bar{T}$, 383
$\bar{V}$, 381
$\bar{v}$, 382
$\bigoplus_{V\in\mathscr{V}} V$, 160
$\bigoplus_{W\in\mathscr{W}} W$, 137
$\bigotimes^k_l V$, 277
$\langle v|$, 391
$\mathbf{C}^{\mathrm{op}}$, 592
$:=$, 510
$\langle x, y\rangle$, 514
$[B]_\mathcal{B}$, 369
$[T]_\mathcal{B}$, 101
$[T]_{\mathcal{C}\leftarrow\mathcal{B}}$, 100
$[v]_\mathcal{B}$, 67
$[v]_\mathscr{W}$, 149
$\coprod_{X\in\mathscr{X}} X$, 524
$f|^T$, 517
$\deg(p)$, 623
$\det(T)$, 335
$\dim(V)$, 57
$\dim_\mathbb{F}(V)$, 57
ℓ^2, 388
$\emptyset$, 510
ev_{x_0}, 242
$\exists$, 498
$\forall$, 498
id_X, 519
$\mathrm{id}_{m\times m}$, 82
$\ker(T)$, 31
$|v\rangle$, 391
$\mapsto$, 518
$\neg A$, 499
$\|T\|$, 410

$\mathrm{Adj}(A)$, 354
$\mathrm{Sym}^l(V)$, 309
ϕ^a, 299
π_X, 526
$\prod_{X \in \mathscr{X}} X$, 525
proj_{W_0}, 146
$f|_S$, 517
$f|_X$, 524
$\mathrm{sgn}(S)$, 307
$\mathrm{sgn}(\sigma)$, 307
$\sim_{\mathrm{q}}$, 531
$\sqrt{T}$, 453
$\bigvee^k T$, 334
$\bigvee^k V$, 309
$\bigvee^\bullet V$, 318
$\bigvee_l V$, 309
$\bigvee_l^k V$, 308
$\bigvee_l^k \mathcal{B}$, 320
$\bigvee_\bullet V$, 318
$\bigvee_\bullet^\bullet V$, 318
${}^a\delta_b$, 287
${}^i\delta_j$, 287
$\bigotimes^k V$, 278
$\bigotimes^\bullet V$, 281
$\bigotimes_l V$, 278
$\bigotimes_l^k \mathcal{B}$, 282
$\bigotimes_\bullet V$, 281
$\bigotimes_\bullet^\bullet$, 281
$\mathrm{tr}(T)$, 332
$\mathbb{K}(x)$, 649
$\mathbb{N}$, 571
${}_bT^a$, 288
$f(-)$, 519
$f(\cdot)$, 519
$f(x)$, 518
$f(x, y)$, 526
$f\colon X \to Y$, 518
f^{-1}, 520
f_X, 526
g^{ab}, 299
$g_{\bar{a}b}$, 438
$g_{\dot{a}b}$, 439
g_{ab}, 299
$m \leq n$, 561
$m \times n$, 74
$p(x_0)$, 629
$p_{\min,T}$, 211
$p_{\mathrm{char},T}$, 360
p_{char}, 360
$v \otimes w$, 257
v_a, 299
$x \in X$, 510
$x \sim_R y$, 515
$x \sim y$, 515
$x_0/\sim$, 528
$x_1 < x_2$, 533