Euclidean Jordan algebras

for optimization

Michael Orlitzky

Euclidean Jordan algebras for optimization

Michael Orlitzky

Cover image by Vexels

October 20, 2022

WARNING ¡ CUIDADO ! ACHTUNG

This is a draft. It contains more or less correct proofs of statements that say more or less what they should. Beyond that, I make no promises. I've made many, many, many, many large-scale changes to notation without ever going back to proofread from page one. Caveat emptor.

Contents

Glossary

$\mathrm{alg}\,(X)$ . . . . . the (sub)algebra generated by X

const_a . . . . . the constant function that always returns a

$\mathbb{C}$ . . . . . the field of complex numbers

$p \mid q$ . . . . . p divides q

EJA . . . . . Euclidean Jordan algebra

I . . . . . the identity matrix in the appropriate space

id_X . . . . . the identity function or arrow on X

$\mathrm{ideal}\,(X)$ . . . . . the ideal generated by X

$\mathrm{lcm}\,(X)$ . . . . . the least common multiple of the elements of X

$R\,[X]$ . . . . . polynomials with coefficients in R and variable X

$\mathbb{P}^n\,(R)$ . . . . . the polynomial ring $R\,[X_1, X_2, \ldots, X_n]$

$\mathcal{P}\,(X)$ . . . . . the "powerset," or set of all subsets of X

PSD . . . . . positive-semidefinite

$f\restriction_X$ . . . . . the restriction of f to X

$\mathbb{R}$ . . . . . the field of real numbers

$\sigma\,(L)$ . . . . . the set of all eigenvalues of L

SDP . . . . . semidefinite program

$\mathcal{S}^n$ . . . . . the set of n-by-n real symmetric matrices

SOCP . . . . . second-order cone program

1_R . . . . . the multiplicative identity (unit) element of R

Chapter 1

Preface

These notes were written for a class on advanced topics in operations research. Euclidean Jordan algebras are an attractive subject for such a course; as they are used in optimization, everything reduces to a finite-dimensional real inner-product space with a funny multiplication defined on it. Basically, you're in $\mathbb{R}^n$, and that means that even undergraduates can kind of understand what's going on if they've taken linear algebra.

Since Jordan-algebraic methods in optimization are an important research area, one has to wonder—why aren't they more popular? In the author's opinion, it's the books. There are a lot of good books on Jordan algebras and a few resources for Euclidean Jordan algebras, but none of them are "just right" if you want an easy and comprehensive introduction to the subject. We mention some of the more popular resources:

- *The Minnesota Notes on Jordan Algebras and Their Applications*, by Max Koecher [8]. This is a good, readable book on Jordan algebras, but it focuses on general Jordan algebras and not (formally-real) Euclidean ones—you don't meet a Euclidean Jordan algebra until three-quarters of the way through the book. The added generality requires some background that students wouldn't otherwise need to understand the simpler Euclidean setting.

- *Jordan-Algebren* by Hel Braun and Max Koecher. I've heard this is also a good, readable introduction to Jordan algebras. But unless you can speak German, it's a bit of a non-starter.

- *A Taste of Jordan Algebras* by Kevin McCrimmon and *Structure and Representations of Jordan Algebras* by Nathan Jacobson. These are two huge references by experts in the field that cover everything you could possibly want to know about a Jordan algebra. But again, this comes at a price: they are written at a graduate level. McCrimmon is easier than Jacobson, but it's still rough going—and a lot of the material is irrelevant for optimizers.

- *Analysis on Symmetric Cones*, by Jacques Faraut and Adam Korányi[5]. This is the most cited work in the optimization literature. It's comprehensive and generally trustworthy, but it's also next to impossible to read, especially for students. It assumes you have a strong background in abstract algebra, analysis, and algebraic geometry among other things. Much of our material comes from here, but we spend several pages discussing each sentence.

- *Spectral functions and smoothing techniques on Jordan algebras*, by Michel Baes. This was Baes's PhD thesis, and was motivated by optimization—smoothing techniques and spectral sets/function, in particular. Nevertheless, Baes has endeavored to build a foundation from scratch, and often goes into Jacobson-like generality. For researchers, this is nice, because many results for Euclidean Jordan algebreas apply more generally. However, for students, the detours into abstraction necessitate several years of background that they aren't likely to have.

- *Fall 2001 Semidefinite and Second Order Cone Programming Seminar Lecture Notes* by Farid Alizadeh. This is probably the best match for what we're trying to accomplish. However, the material on Euclidean Jordan algebras comprises a relatively small part of a larger course, and thus a small part of their lecture notes. In the interest of brevity, many of the proofs are omitted from the notes, and references to Faraut and Korányi are given in their stead. But as we've said, the book by Faraut and Korányi is nigh unreadable by mere humans.

In summary, what we'd like is something as clear and simple as the lecture notes by Alizadeh, with the depth of Faraut and Korányi, and with everything proved in detail. Our goal is to be accessible to someone with the following background:

- One semester of real analysis (but preferably two).

- Two semesters of linear algebra; one focused on matrices, and one with abstract vector spaces.

- One semester of abstract algebra covering at least rings, ideals, and polynomials.

Basically, everything that we cover in Part I, you should already have seen before. A non-comprehensive list of our assumptions:

- You are intimately familiar with the properties of the real numbers $\mathbb{R}$.

- Sequences, limits, and open/closed sets in $\mathbb{R}^n$ are second nature.

- This is not be the first time you've met the complex numbers $\mathbb{C}$.

- You've added, multiplied, and divided polynomials before.

- The words "ring" and "ideal" do not scare you, having seen the abstract definitions of algebraic structures like groups and vector spaces before.
- You can do changes of basis in a vector space without thinking about it.
- Finding the matrix of a linear operator with respect to a given basis is no problem.
- You can compute eigenvalues, eigenvectors, and eigenspaces, and know why all of them are important.
- You can diagonalize a matrix, or compute its spectral decomposition when possible.
- You recall that there are two things called the "minimal polynomial" and "characteristic polynomial" of a matrix.
- You're willing to fake it if any of these assumptions don't hold.

We won't go into a lot of detail when it comes to the background material; we'll only mention some important results that are cited later. While the list above contains the bare minimums, the following would be nice to have:

- A bit of algebraic geometry, to get a feel for working with polynomials and their solutions.
- Some familiarity with topology (open and closed sets), since we mention the Zariski topology momentarily.
- A bit of programming experience. A lot of these results look harder than they are, and five minutes spent coding up an implementation can be more enlightening than an hour spent staring at a page.

Throughout the notes, we've tried to keep the number of cited references to a minimum. We expect that the reader will want to consult additional sources, and that she probably won't have fifty different books sitting around her at all times. The following is a minimalish list of references to which we will refer by name, rather than by citation. Only in rare cases are we forced to cite other references.

- *Abstract Algebra*, by Beachy and Blair [4]. This is a great introduction to groups, fields, rings, polynomials, and ideals—and that's really all we'll need.
- *Principles of Mathematical Analysis*, by Walter Rudin. This book is famous for being difficult, but it's still the standard most places. It's worth reading, if only so that you can be in on all the jokes about how ridiculously hard it is.

- *Linear Algebra Done Right*, by Sheldon Axler. The best introductory linear algebra book, *by far*. Explains everything geometrically, and avoids introducing coordinates unless they're absolutely necessary. (Just buy this book if you plan to keep doing math.)
- *Advanced Linear Algebra*, by Steven Roman [13]. If you can read Axler's book cover-to-cover, then this is where you go next. It's also well-written, but handles vector spaces of arbitrary dimension, over arbitrary fields—and generalizes to modules over rings. Also treats Banach and Hilbert spaces.
- *Convex Optimization*, by Boyd and Vandenberghe. Free online from the authors.
- *On an Algebraic Generalization of the Quantum Mechanical Formalism*, by Pascual Jordan, John von Neumann, and Eugene Wigner [7]. The paper that started it all. Mainly of historical interest.
- *Analysis on Symmetric Cones*, by Jacques Faraut and Adam Korányi[5]. Mentioned previously.
- *The Minnesota Notes on Jordan Algebras and Their Applications*, by Max Koecher [8]. Mentioned previously.
- *Spectral functions and smoothing techniques on Jordan algebras*, by Michel Baes. Mentioned previously, and free from his advisor.
- *Fall 2001 Semidefinite and Second Order Cone Programming Seminar Lecture Notes* by Farid Alizadeh. Free from the instructor's website.

Finally, we mention some additional resources for background information. These won't be required, but may provide some additional value.

- *Mathematical analysis*, by Tom Apostol. This is what people use to fill in the gaps when they get stuck reading Rudin.
- *Introduction to Analysis*, by Maxwell Rosenlicht. If you prefer a paper copy of your reference books, this one is fifteen bucks on Amazon and gets the job done.
- *Algebra*, by Saunders Mac Lane and Garrett Birkhoff [9]. This is the grown-up version of Beachy and Blair. It uses higher-level ideas from category theory, presents theorems more generally, and covers many of the structures (magmas, monoids, modules, et cetera) that Beachy and Blair omit. They say to read the masters, and these guys are the masters.
- *Matrix Analysis and Applied Linear Algebra* by Carl D. Meyer. This is another good, comprehensive introduction to the most important concepts of linear algebra, but using matrices instead of abstract linear operators like Axler does. Unfortunately, you sometimes just have to know what to do with a box full of numbers.

- Harvard MATH122 (Abstract algebra) lecture videos. Free online from Harvard's Open Learning Initiative and mirrored on Youtube.
- Stanford EE364a (Convex Optimization I) lecture videos. Based on *Convex Optimization* by Boyd and Vandenberge, and taught by Boyd. Available for free, and mirrored on youtube.

1.1 Notation notation

As a matter of honor, I strive in this text to make the notation as consistent as possible without straying too much from widely-accepted conventions. The reader should hold me to the following guidelines.

Generic variables, specifically function arguments and Euclidean Jordan algebra elements, will be denoted by the lowercase Latin letters x, y, and z. If we need more than three of them, or if we need an unspecified number k of them, then $x_1, x_2, \ldots, x_k$ will be used instead.

The capital Latin letters X, Y, and Z will be used to denote polynomial indeterminates. If we need more than three of them, or if we need an unspecified number k of them, then $X_1, X_2, \ldots, X_k$ will be used instead. In the context of characteristic and minimal polynomials (where the indeterminate has something to do with eigenvalues), we will often use the indeterminate Λ instead. For example, we write the characteristic polynomial of a matrix A as $\det(\Lambda I - A)$. While $\det(XI - A)$ is equally correct, I see no reason to torture the reader moreso than we already will by choosing an entirely different letter. The associated (scalar) eigenvalues are denoted by lowercase λ_1, λ_2, et cetera. Polynomials themselves will use the lowercase Latin letters $p, q, \ldots$

Linear operators and matrices that we want to treat like linear operators are written in capital letters. The letters $A, B, \ldots$ are typically used for matrices; the letters $L, M, \ldots$ for linear operators. This rule will be broken frequently when we want to think of a matrix not as a linear operator, but as an element of a Euclidean Jordan algebra where the names $x, y, \ldots$ are more appropriate.

Indexed lowecase Latin letters a_i, b_j, x_k, and so on will be used for the coordinates in a vector space or module. As a result of our index notation, capital Latin letters like A_{ij} will be used for the entries of a matrix A, even though they are technically the coordinates of A with respect to a particular basis. Other "interesting" scalars will be written in the lowercase Greek letters $\alpha, \beta, \ldots$. If $x \in \mathbb{R}^3$, for example, we will write $x = (x_1, x_2, x_3)^T$ even though the x_i happen to belong to the scalar field. If we want to scale x in some specific context, we might write $\alpha(x_1, x_2, x_3)^T$ in that case. We formally define polynomials as module elements that have coordinates, so if p is a polynomial, the coefficients of $X^0, X^1, \ldots$ will be written as $a_0, a_1, \ldots$ rather than as α_i. Perhaps the converse is more useful: we will not use lowercase Greek letters for anything other than scalars.

Part I

Fundamentals

Chapter 2

Vector space structure

2.1 Algebraic building blocks

The goal in this section is to illuminate the relationships between the various algebraic structures that we're going to encounter. The definitions below are a bit verbose and are generally not used in practice. However, each subsequent structure we define will be built from the previous ones, making only the necessary changes or additions, to show how they relate to one another. And perhaps more imporantly, some times you do really need the verbose definition to see what's going on. In any case, we mention some common notational shortcuts that you're likely to see following each definition.

Definition 1. A *magma* (S, μ) is a mathematical structure consisting of,

- A set S.
- A "multiplication" operation $\mu : (S \times S) \to S$.

Magmas are a most basic kind of algebraic structure. All that we impose is the condition of closure on μ, namely that "multiplying" two elements of S gives us back another element of S. Beware that some people use the term "groupoid" to refer to magmas—the name "groupoid" however means something different in other contexts, so we avoid it.

Definition 2. A *semigroup* (S, μ) is a magma where the "multiplication" operation μ is associative.

Example 1. Let $S = \mathbb{Z}$ and let $\mu = \max$. Then for all integers $x, y, z \in S$, we have $\max(\max(x, y), z) = \max(x, \max(y, z)) \in S$; so $(\mathbb{Z}, \max)$ forms a semigroup.

Definition 3. A *monoid* $(M, \mu, 1_M)$ is a mathematical structure consisting of,

- A set M and a "multiplication" operation $\mu : (M \times M) \to M$ such that (M, μ) forms a semigroup.

- A *unit element* $1_M \in M$ such that for any $x \in M$, we have $\mu(1_M, x) = x$ and $\mu(x, 1_M) = x$.

A monoid is thus a semigroup with a unit element. Monoids are important in their own right in computer science (list concatenation) and category theory, among other places.

Convention 1: Units and identities

Unit elements are also commonly called *identity elements*, but we will do our best to avoid that terminology, since it can lead to ambiguity with the identity function or certain named relationships like the *Jordan identity*. The identity matrix can be either, depending on the context! We quote McCrimmon in *A Taste of Jordan Algebras...*

> Note that again the notation 1 for the unit is a generic one-term-fits-all-algebras notation; if we wish to be pedantic, or clear ("Will the real unit please stand up?"), we write 1_A to make clear whose unit it is. The unit element is often called the identity element. We will try to avoid this term, since we often talk about an algebra "with an identity" in the sense of "identical relation" (the Jacobi identity, the Jordan identity, etc.). Of course, in commutative associative rings the term "unit" also is ambiguous, usually meaning "invertible element" (the group of units, etc.), but already in noncommutative ring theory the term is not used this way, and we prefer this lesser of two ambiguities. It is a good idea to think of the unit as a neutral element for multiplication, just as 0 is the neutral element for addition.

Example 2. Let $M = (\mathbb{Z} \cup \{-\infty\})$ and let $\mu = \max$. We saw in Example 1 that $(\mathbb{Z}, \max)$ forms a semigroup, and it's not hard to see that the addition of the element "$-\infty$" does not change that. However, in this case, we have a unit element:

$$\forall x \in M : \max(x, -\infty) = x = \max(-\infty, x).$$

As a result, $((M, \mu), -\infty)$ forms a monoid.

Another perspective is that a monoid is like a group, but without the requirement that we have inverses.

Definition 4. A *group* (G, μ, e, ι) consists of,

- A set G such that (G, μ, e) forms a monoid.
- An *inverse* operation $\iota : G \to G$ such that $\mu(g, \iota(g)) = \mu(\iota(g), g) = e$ for any $g \in G$.

If $\mu(g, h) = \mu(h, g)$ for all $g, h \in G$ (that is, if multiplication is commutative), then the entire structure is called an *abelian* group, after the mathematician Niels Henrik Abel.

Convention 2: Group notation

Typically the group operations and unit element are understood, and we say "the group G" to refer to the entire structure, leaving the multiplication, inverse, and unit elements implicit. Since a priori the group operation acts like multiplication, people usually write gh for the product of g and h when the group structure is understood. Likewise, we write g^{-1} for the multiplicative inverse of g. An exception to that rule is when the group is abelian. In that case, the group operation acts like addition, and the "product" of g and h is written $g + h$. The inverse of g is then written $-g$ to agree with the intuition behind addition.

When a single symbol like G is used for the entire group, people also sometimes repurpose that symbol to refer only to the underlying set. For example, you might see $\phi : G \to G$ written to indicate that ϕ is a function on whatever set underlies the group G. This is unambiguous since there's only one set involved in the definition of a group.

To summarize: a group is a set where we can multiply two elements to get another element of the set, and this multiplication has a unit element and inverses.

Definition 5. A *ring* $(R, +, 0, -(\cdot), \cdot, 1)$ consists of a set R such that,

Roman, Preliminaries, Part 2

- $(R, +, 0, -(\cdot))$ forms an abelian group.
- $(R, \cdot, 1)$ forms a monoid.

- Monoid "multiplication" distributes over group "addition" on both sides:

$$\forall x, y, z \in R : x \cdot (y + z) = (x \cdot y) + (x \cdot z)\,,$$
$$\forall x, y, z \in R : (x + y) \cdot z = (x \cdot z) + (y \cdot z)\,.$$

If $x \cdot y = y \cdot x$ for all $x, y \in R$, then the entire structure a *commutative ring*.

Keep in mind that addition is *always* commutative in a ring, so the fact that addition commutes does not make the ring commutative. The name "commutative ring" refers to the multiplication.

Convention 3: Ring notation

Since the additive structure of a ring forms an abelian group, everyone follows Convention 2 and writes the group operation as addition, its unit element as zero, and its inverse as negation. The multiplicative (monoid) structure of a ring is modeled on that of the integers, and so we write it the same way we do integer multiplication, either by juxtaposition gh or with a dot, like $g \cdot h$. For the same reason, the group unit is almost always written as "1," since 1 is the multiplicative unit element for integers.

Since the operations and unit elements are always written the same, most people omit them and say something like "if R is a ring," which means that R is a set on which there exists a ring structure. And as collateral damage, we sometimes reuse the ring symbol R to refer only to the underlying set. For example, you will see $\phi : R \to R$ used to indicate that ϕ is a function on whatever set underlies the ring R. This is unambiguous since there's only one set involved in the definition of a ring.

Authors disagree on whether or not rings should have multiplicative identity (unit) elements. Ours do. When there is no multiplicative identity, there is is a tongue-in-cheek convention to call the resulting structure a *rng*; that is, a "ring" but without the "i" (get it?). This is a decent enough convention, and easy to remember, so we adopt it.

A *subring* of a given ring is a subset of the ring's underlying set R that itself forms a ring using the addition and multiplication operations (appropriately restricted) from the bigger ring. Since our rings have unit elements, subrings must too.

Definition 6. If $(R, +, 0, -(\cdot), \cdot, 1)$ is a commutative ring, then a *ring ideal* in R is a subset $I \subseteq R$ such that (after restricting the domain and codomain of the ring operations appropriately),

- $(I, +, 0, -(\cdot))$ forms a subgroup of $(R, +, 0, -(\cdot))$,
- $(I, \cdot)$ forms a sub-semigroup of $(R, \cdot)$.
- $\forall i \in I, \forall r \in R : i \cdot r \in I$.

If $I = Rx \coloneqq \{rx \mid r \in R\}$ for some $x \in R$, then I is called a *principal ideal*.

We don't say that I forms a subring of G because we just mentioned that subrings have a unit element, and we don't want to require ring ideals to have them too: if a ring ideal contains the unit element of the ring, the ring ideal is the whole ring. This is also why we say that $(I, \cdot)$ should form a sub-semigroup in the definition of a ring ideal rather than a sub-monoid.

For some motivation, recall from group theory that if H is a subgroup of G, then G/H does not necessarily form a group. We need H to be a *normal subgroup*, so that the "mod" operation works the way we want it to. Ring ideals are the same concept, but for rings. The set of equivalence classes R/I need not be a ring unless I is a ring ideal.

Before we move on to fields, here are two special types of commutative ring you'll want to know.

Definition 7. If $(R, +, 0, -(\cdot), \cdot, 1)$ is a commutative ring with $1 \neq 0$ and if, for all $a, b \in R$, $ab = 0$ implies ($a = 0$ or $b = 0$), then $(R, +, 0, -(\cdot), \cdot, 1)$ is an *integral domain*. An integral domain where every ring ideal is a principal ideal is a *principal ideal domain*.

Beachy and Blair, Definition 5.1.7 and Definition 5.3.3

The set of integers $\mathbb{Z}$ forms an integral domain, which is how integral domains got their name. It's a little less obvious, but Example 5.3.1 in Beachy and Blair shows that the integers form a principal ideal domain as well.

Definition 8. A *field* $\left(F, +, 0, -(\cdot), \cdot, 1, (\cdot)^{-1}\right)$ consists of a set F such that

- $(F, +, 0, -(\cdot), \cdot, 1)$ forms a commutative ring, and
- $\left(F \setminus \{0\}, +, 1, (\cdot)^{-1}\right)$ forms an abelian group.

Fields add a multiplicative inverse to the concept of a commutative ring, but with the caveat that there is no inverse for the additive unit (zero) of the ring. This is easy enough to remember if you think of the real numbers, where there is no multiplicative inverse of zero because we can't divide by zero.

Convention 4: Field notation

Fields often appear in "blackboard" font; for example, a general field is commonly denoted by $\mathbb{F}$. As always, when it's clear from the context or when we just don't feel like writing it all out, we use the single letter $\mathbb{F}$ to represent the entire field structure, leaving the operations, unit elements, and inverses implicit.

Perhaps more importantly, we will sometimes use the symbol $\mathbb{F}$ that denotes the entire field structure to refer only to the underlying set. For example, we might write $\phi : \mathbb{F} \to \mathbb{F}$ to indicate that ϕ is a function on whatever set underlies the field $\mathbb{F}$. This is largely unambiguous, since (if you squint) there's only one set involved in the definition of a field.

2.2 Vector and Hilbert spaces

Our first definition in this section is going to look a bit strange at first, so we preface it with a motivating example.

Example 3. Most people would agree that in $\mathbb{R}^3$, we have the identity

$$(1 + 2 \cdot 2) \cdot \left((1, 0, 0)^T + (0, 0, 1)^T \right) = (5, 0, 5)^T .$$

But what's really going on here? The "plus" in $(1 + 2 \cdot 2)$ is addition of real numbers, but the "plus" in $(1, 0, 0)^T + (0, 0, 1)^T$ is addition of *vectors*. Moreover, after simplifying, the "dot" in $2 \cdot 2$ is not the same "dot" in between $5 \cdot (1, 0, 1)^T$. We've written the operators the same, but they're doing two different things. We should really have two *different* addition/multiplication operations, and we should know how they interact!

The above example motivates the definition of a module, which works just like our example but explicitly keeps the operations separate. In other words, scaling a vector is not the same thing as multiplying two numbers, and addition of numbers and vectors get two separate operators. As you read, you can think of the ring $\mathcal{R}$ as being the real numbers and the abelian group $\mathcal{M}$ as being vectors. The "$\star$" operation is what scales a vector by a real number.

Definition 9. An *$\mathcal{R}$-module* $(\mathcal{M}, \mathcal{R}, \star)$ consists of, Roman, Chapter 4

- An abelian group $\mathcal{M} \coloneqq (M, +_M, 0_M, -_M (\cdot))$ of module elements,

- A commutative ring $\mathcal{R} \coloneqq (R, +_R, 0_R, -_R(\cdot), \cdot_R, 1_R)$ of scalars,
- A *scaling* operation $\star : (R \times M) \to M$ satisfying the following laws,

$$\begin{aligned}
\forall \alpha \in R, \forall x, y \in M: \quad & \alpha \star (x +_M y) &&= (\alpha \star x) +_M (\alpha \star y) \\
\forall \alpha, \beta \in R, \forall x \in M: \quad & (\alpha +_R \beta) \star x &&= (\alpha \star x) +_M (\beta \star x) \\
\forall \alpha, \beta \in R, \forall x \in M: \quad & (\alpha \cdot \beta) \star x &&= \alpha \star (\beta \star x) \\
\forall x \in M: \quad & 1 \star x &&= x.
\end{aligned}$$

A module can be thought of as "a vector space, but over a ring instead of a field." It is tempting to call the elements of M in Definition 9 "vectors," but we take care to avoid doing so, since the name "vector" suggests an element of a "vector space." The name $\mathcal{R}$-module is by analogy to $\mathbb{F}$-vector-space. In hindsight, if we think of a commutative ring as being a module over itself (Roman, Example 4.1.3), then Definitions 6 and 9 say that the ring ideals in that ring are precisely the submodules of the resulting module.

Convention 5: Module notation

It's at this point that the structures become too complicated and we just assume that everyone knows what we're talking about. Typically we will just say that (M, R) is a module, and it's understood that M is a set on which there exists some additive group structure, and that R is a commutative ring that can be used to scale elements of M. Sadly, the subscripts on the operations are not used in practice. You will instead see the three module operations conflated as in Example 3.

Example 4. Let $\mathbb{Z}^3$ be the set of all 3-by-1 column matrices whose entries are integers. If we define addition of these objects by

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \coloneqq \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{bmatrix}$$

and the scaling operation by

$$\alpha \star \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \coloneqq \begin{bmatrix} \alpha x_1 \\ \alpha x_2 \\ \alpha x_3 \end{bmatrix},$$

then the resulting structure forms a $\mathbb{Z}$-module. Of course, inside the brackets, addition and multiplication are just the usual addition and multiplication of integers.

The general theory of modules is a lot more complicated than that of vector spaces, but we won't need most of it. It is however nice to know the definition, because a vector space is simply a module over a ring that happens to be a field. You will also see the name "module" a lot in SageMath, where vector spaces are implemented as modules. Finally, it will save us a lot of time if we are able to pretend that we're allowed to put polynomials inside of vectors and matrices. The theory of modules tells us that this is mathematically okay.

A *free module* is the name for a module with a basis, and for example, we can construct the free module that consists of triples of integers, as in Example 4.

```
sage: M = FreeModule(ZZ,3)
sage: M.basis()
[
(1, 0, 0),
(0, 1, 0),
(0, 0, 1)
]
```

When an R-module has a basis, we can use that basis as a coordinate system, much like we do with vectors in a real vector space. In an n-dimensional real vector space, the coordinate vectors live in $\mathbb{R}^n$, and in an R-module the coordinates will live in R^n. To act on those coordinate representations, we can define matrices whose entries are in R, and the set of all such matrices will itself form an R-module, exactly how the set of all real n-by-n matrices forms a real vector space of dimension n^2.

Definition 10 (matrix notation)**.** If R is a commutative ring, then R^m denotes the set of all m-by-1 column matrices whose entries are elements of R. The set R^m forms an R-module in an obvious way; if $\alpha \in R$ and $x, y \in R^m$, then the addition and scaling operations are performed componentwise,

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix} := \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_m + y_m \end{bmatrix}$$

$$\alpha \star \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{bmatrix} := \begin{bmatrix} \alpha r_1 \\ \alpha r_2 \\ \vdots \\ \alpha r_m \end{bmatrix}.$$

We further define $R^{m\times n}$ to be the set of m-by-n matrices with entries in R. If $A \in R^{m\times n}$, then we write A_{ij} to indicate the element in the i^{th} row and j^{th}

column of A,

$$A = \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mn} \end{bmatrix}.$$

Addition and scaling of these matrices works just like addition and scaling of matrices whose entries come from a field. The set $R^{m\times n}$ therefore also forms an R-module with the operations

$$A + B \coloneqq \begin{bmatrix} A_{11} + B_{11} & \cdots & A_{1n} + B_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} + B_{m1} & \cdots & A_{mn} + B_{mn} \end{bmatrix}$$

$$\alpha A \coloneqq \begin{bmatrix} \alpha A_{11} & \cdots & \alpha A_{1n} \\ \vdots & \ddots & \vdots \\ \alpha A_{m1} & \cdots & \alpha A_{mn} \end{bmatrix}$$

If the dimensions of A and B are compatible, that is if $A \in R^{m\times n}$ and if $B \in R^{n\times p}$, then matrix multiplication is defined in the usual way,

$$AB \coloneqq \begin{bmatrix} C_{11} & \cdots & C_{1p} \\ \vdots & \ddots & \vdots \\ C_{m1} & \cdots & C_{mp} \end{bmatrix}, \text{ where}$$

$$C_{ij} \coloneqq \sum_{k=1}^{n} A_{ik} B_{kj}.$$

Thus when $m = n$, the set $R^{n\times n}$ forms a ring where the multiplication operation is matrix multiplication. Its unit element is the n-by-n identity matrix,

$$I \coloneqq \begin{bmatrix} 1_R & 0 & 0 & \cdots & 0 \\ 0 & 1_R & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1_R & 0 \\ 0 & 0 & \cdots & 0 & 1_R \end{bmatrix} = 1_{R^{n\times n}} \in R^{n\times n}.$$

Convention 6: All identity matrices look the same

The notation "I" for an identity matrix mentions neither the size $n\times n$ nor the ring R. The size and nature of its entries can usually be inferred from the context. For example, if Λ belongs to some

ring R (that isn't a ring of matrices!), then you should probably deduce that the I in the expression ΛI refers to a matrix with 1_R on the diagonal. Likewise if you see $I + A$ where $A \in R^{n \times n}$.

This is not as mathematically infuriating as it sounds. In Section 3.3, we will adopt the convention of representing constant polynomials by their sole nonzero coefficient. This is well-founded whenever there exists a natural inclusion map from the base ring to the larger ring that sends one unit element to the other. With that in mind, you can think of "I" as a matrix of "ones," where the meaning of each 1 depends on the context.

So far we've been building up to the definitions of vector space and algebra. Almost all optimization takes place in a vector space with some additional structure. First let's review what a vector space is, and what kinds of additional structure we might impose on one.

Definition 11. A *vector space* $(\mathcal{V}, \mathbb{F}, \star)$ is a module where the ring $\mathbb{F}$ is a field. The elements of the underlying abelian group are called *vectors*, and the elements of the field are called *scalars*.

Combining all of the properties of fields and modules should give you the usual long list of axioms associated with a vector space.

You must know the underlying field and all of the operations (vector addition, field multiplication, field addition, vector scaling, et cetera) in order to specify a vector space. It is therefore incorrect to say "let V be a vector space..." with no further information. Nevertheless, that's what people do. Be aware that you need to infer the rest of the information from the context. Another caveat is that the field multiplication and vector scaling are often written the same way. The multiplication that takes π and turns it into 2π is not the same as the multiplication that takes $x \in V$ and turns it into $2x$ (one works on vectors and the other on real numbers), but you will almost certainly find them both denoted by a dot or by juxtaposition. Sorry.

Convention 7: Vector space notation

After this section, we conform and write $(V, \mathbb{F})$ to denote a vector space, where V itself denotes the set of vectors. The operations are all implicit and are written the usual way, like they are in $\mathbb{R}^n$ (Example 3).

Definition 12. A *normed vector space* $(\mathcal{V}, \mathbb{F}, \star, \|\cdot\|)$ consists of,

- A vector space $(\mathcal{V}, \mathbb{F}, \star)$ where $\mathcal{V} = (V, +, 0, -(\cdot))$ is its abelian group of vectors with a vector-addition operation.
- A subfield $\mathbb{F}$ of either the real numbers $\mathbb{R}$ or complex numbers $\mathbb{C}$.
- A function called a *norm*, defined on V,

$$\|\cdot\| : V \to \mathbb{F},$$

that satisfies three properties:

  - Triangle inequality: $\|x + y\| \leq \|x\| + \|y\|$.
  - Absolute homogeneity: $\|\alpha x\| = |\alpha| \, \|x\|$ for $\alpha \in \mathbb{F}$.
  - Positive-definiteness: $\|x\| = 0$ only when $x = 0$.

Norms are one way to define a "distance" between two vectors in a vector space. If we think of $\|x\|$ as the length of the vector x, then we can also think of $\|x - y\|$ as the length of the segment from x to y (that is, the distance between the two points). When $y = 0$, we get $\|x - y\| = \|x - 0\| = \|x\|$ as the distance from 0 to x, which is exactly what we call the "length" of a vector.

Remark 1. Even though we have defined the codomain of the norm function to be the field $\mathbb{F}$, our use of the "less than or equal to" in the triangle inequality implies that the codomain of the norm is contained in the field of real numbers. However, the choice of $\mathbb{F}$ was not merely to impress the reader: if $\mathbb{F}$ is a subfield of the real numbers (like the rational numbers $\mathbb{Q}$ or the algebraic reals), then the norm of an element should also belong to that smaller field. If $\mathbb{F} = \mathbb{Q}$, then you can't have an element with norm π.

In general, there may be more than one function defined on a single vector space that satisfies the properties of a norm. In finite-dimensional spaces, however, they are all equivalent in a sense.

Proposition 1 (equivalence of norms)**.** *If $(\mathcal{V}, \mathbb{F}, \star)$ if a finite-dimensional vector space and if $\|\cdot\|_a : V \to \mathbb{F}$ and $\|\cdot\|_b : V \to \mathbb{F}$ are two norms on V, then there exist constants $\alpha, \beta > 0$ in $\mathbb{F}$ such that* *Boyd, A.1.4*

$$\forall x \in V : \alpha \|x\|_a \leq \|x\|_b \leq \beta \|x\|_b .$$

In particular, both norms induce the same open/closed sets, functions that are continuous in one norm are continuous in the other, and sequences that converge (or diverge) in one norm converge (or diverge) respectively in the other.

Definition 13. An *inner-product space* $(\mathcal{V}, \mathbb{F}, \star, \langle \cdot, \cdot \rangle)$ consists of,

- A vector space $(\mathcal{V}, \mathbb{F}, \star)$ where $\mathcal{V} = (V, +, 0, -(\cdot))$ is its abelian group of vectors with a vector-addition operation.
- A subfield $\mathbb{F}$ of either the real numbers $\mathbb{R}$ or complex numbers $\mathbb{C}$.
- A function called an *inner product* defined on $V \times V$,

  $$\langle \cdot, \cdot \rangle : (V \times V) \to \mathbb{F},$$

  that satisfies three properties:

  - Conjugate symmetry: $\langle x, y \rangle = \overline{\langle y, x \rangle}$.
  - Linearity in first argument: $\langle \alpha x + y, z \rangle = \alpha \langle x, z \rangle + \langle y, z \rangle$.
  - Positive-definiteness: $\langle x, x \rangle > 0$ for all nonzero $x \in V$.

In every inner-product space there is a natural norm $\|\cdot\| : V \to \mathbb{F}$ defined by $\|x\| := \sqrt{\langle x, x \rangle}$. The properties necessary of an inner-product ensure that this function is indeed a norm.

Remark 2. As with a normed vector space, the field $\mathbb{F}$ must be either real or complex in an inner-product space. This is so that the complex conjugate makes sense in the "conjugate symmetry" axiom, and ensures that the natural norm on the inner-product space has a codomain compatible with the properties of a norm (as in Remark 1).

For the most part, we will consider only real vector spaces, where $\mathbb{F} = \mathbb{R}$. We have tried not to overcomplicate these definitions, but on the other hand we need them general enough to be sure that everything is justified. Particularly when working in SageMath, we will need to use fields other than the real numbers, because most real numbers can't be represented exactly on a computer. The best we can do is approximate them, and this leads to some problems:

```
sage: RR
Real Field with 53 bits of precision
sage: A = matrix(RR, [[  3,  5 ],
....:                 [ 30, 50 ]])
sage: A.rank()
2
```

Since the second row of that matrix is a multiple of (ten times) the first, its rank should be one. What went wrong?

Warning 1: Floating point breaks linear algebra

Floating point numbers are merely approximations, and the computer doesn't have a good way of determining when two approximations are equal. As a result, most linear algebra should be done with rational numbers or the algebraic real field (the algebraic reals are the rationals with all square roots, cube roots, and so on added in).

The rational field and real algebraic field are both usable in SageMath:

```
sage: QQ
Rational Field
sage: AA
Algebraic Real Field
sage: QQ.is_subring(AA)
True
sage: AA.is_subring(RealLazyField())
True
sage: A = matrix(QQ, [[  3,  5 ],
....:                 [ 30, 50 ]])
sage: A.rank()
1
sage: A = matrix(AA, [[  3,  5 ],
....:                 [ 30, 50 ]])
sage: A.rank()
1
```

However, as far as the theory is concerned, you can usually imagine that we're working in $\mathbb{R}^n$ with real scalars. The following theorem says that every finite-dimensional real inner-product space of the same dimension m is essentially the same. Thus, up to isomorphism, it generally suffices to do things in $\mathbb{R}^n$ with the usual inner-product.

Theorem 1. *Any m-dimensional real inner-product space is isometric to $\mathbb{R}^m$.*

This result will be proved in Exercise 5.

Simplification 1: Real inner-product spaces

When $\mathbb{F} = \mathbb{R}$ in an inner-product space, two properties of an inner-product can be simplified:

- Symmetry:
$$\forall x, y \in V : \langle x, y \rangle = \langle y, x \rangle .$$
- Bilinearity:
$$\forall \alpha \in \mathbb{R}, \forall x, y, z \in V : \langle \alpha x + y, z \rangle = \alpha \langle x, z \rangle + \langle y, z \rangle$$

Thanks to symmetry, bilinearity need only be checked on one

side.

In a moment (in Section 2.3), we will discuss continuity and compactness in a vector space setting. Certain continuity and compactness results get complicated in infinite dimensions, or in spaces that are not "complete." For the sake of brevity, we will state the simplified versions of these results in a finite-dimensional complete inner-product space.

Definition 14. A normed vector space in which every Cauchy sequence converges is called *complete*. A *Hilbert space* is a complete inner-product space.

Chapter 13 in Roman is devoted entirely to Hilbert spaces. Since our inner-product spaces will all be finite-dimensional, and since the fields $\mathbb{R}$ and $\mathbb{C}$ are complete, the only way that we could wind up with an incomplete inner-product space would be to choose an incomplete subfield of $\mathbb{R}$ or $\mathbb{C}$ as the base field. For example, $\mathbb{R}^3$ forms a Hilbert space but $\mathbb{Q}^3$ does not. Examples 12.9 and 12.10 in Roman discuss the completeness of $\mathbb{R}^n$ and $\mathbb{C}^n$ briefly. We mention this caveat only because we have explicitly left open the possibility of choosing such a subfield in Definition 13 and the remarks that follow it. However, for the purposes of the theory, we'll be using the real or complex field and there's nothing to worry about.

Roman, examples 12.4, 12.14, and 13.1

Example 5. The space $\ell_2(\mathbb{R})$ consists of all square-summable sequences of real numbers,

$$\ell_2(\mathbb{R}) \coloneqq \left\{ (x_1, x_2, \ldots)^T \;\middle|\; x_i \in \mathbb{R}, \sum_{i=1}^{\infty} x_i^2 \in \mathbb{R} \right\}.$$

This set forms a vector space over $\mathbb{R}$ with componentwise addition and scaling, just like in $\mathbb{R}^n$. However, there also exists a natural inner-product on the space,

$$\langle x, y \rangle \coloneqq \sum_{i=1}^{\infty} x_i y_i,$$

which induces the norm

$$\|x\| \coloneqq \langle x, x \rangle^{1/2} = \left(\sum_{i=1}^{\infty} x_i^2 \right)^{1/2}.$$

The definition of $\ell_2(\mathbb{R})$ ensures that the sum in the norm converges, so that we can actually take its square root. Since the norm converges, a general version of Cauchy-Schwartz can be used to show that the sum in the inner-product converges as well, even when $y \neq x$. This normed vector space is complete and separable [13], and is one of the most important examples of a Hilbert space.

2.3 Continuity and compactness

The proper setting in which to discuss continuity and compactness is in a *topological space*. However, introducing all of the necessary terminology from topology would take us too far abroad of our main goal, which is to *use* these concepts in finite-dimensional inner-product spaces. So, without going into the details, we will note that every normed vector space (and thus every inner-product space) can be thought of as a topological space, and leave it at that. Likewise—in case the reader is familiar with the concept—every normed vector space also forms a *metric space* where the distance between two points is the norm of their difference. Thus when we state things for normed vector spaces, you may apply any results that you know for metric spaces.

The following is used as the definition of continuity in a topological space. It is equivalent to the usual epsilon-delta definition in $\mathbb{R}^n$, but we don't have epsilons and deltas in a topological space, so the more general formulation is used. It will be useful, in particular, to know that the preimage of an open or closed set under a continuous function is of the same type.

Definition 15. Let V and W be finite-dimensional Hilbert spaces and $f : V \to W$ be a function. We say that f is *continuous* on V if the preimage of every open set in W is open in V.

Exercise 1 (continuous preimage of closed set is closed). Let $f : V \to W$ be a continuous function between two topological spaces V and W, so that (by Definition 15) the preimage under f of every open set in W is open in V:

$$Y \text{ is open in } W \implies f^{-1}(Y) = \{x \in V \mid f(x) \in Y\} \text{ is open in } V.$$

Prove that the preimage under f of every *closed* set in W is *closed* in V. Feel free to take $V = W = \mathbb{R}^n$ to simplify things. A closed set is, by definition, a set that is the complement of some open set.

Hint: show that the "preimage of" operation plays nice with "complement of" operation, and then use the fact that every closed set is the complement of some open set. Note that V is both open and closed as a subset of itself.

Since open and closed sets are dual to one another, we could just as well have used the condition in Exercise 1 as our definition of a continuous function. And in a finite-dimensional Hilbert space, either is equivalent to the usual epsilon-delta condition that we get by taking the definition of continuity in $\mathbb{R}$ and therein replacing the absolute value with a norm.

Rudin, Theorems 4.6 and 4.8

Theorem 2. *If V and W are finite-dimensional Hilbert spaces and if $f : V \to W$ is a function, then the following are equivalent:*

- *f is continuous on V in the sense of Definition 15.*
- *For every convergent sequence $x_n \to x$ in V we have*

$$\lim_{n\to\infty} f(x_n) = f\left(\lim_{n\to\infty} x_n\right) = f(x).$$

- *f satisfies the usual epsilon-delta definition of continuity,*

$$\forall x \in V, \forall \epsilon > 0, \exists \delta > 0 : \|x - y\| < \delta \implies \|f(x) - f(y)\| < \epsilon.$$

And of course, using any of those definitions, we have the following basic results.

Proposition 2. *Addition is continuous on every normed vector space V.*

Proof. Suppose that $(x, y)_n$ is a sequence converging to (x, y) in $V \times V$, and let f denote the "plus" function on $V \times V$. Then there exist two sequences in V such that $x_n \to x$ and $y_n \to y$ individually, and we can use the triangle inequality to see that

$$\begin{aligned} \|f((x, y)) - f((x_n, y_n))\| &= \|(x + y) - (x_n + y_n)\| \\ &= \|(x - x_n) + (y - y_n)\| \\ &\leq \|x - x_n\| + \|y - y_n\| \\ &\to 0 + 0. \end{aligned}$$

□

Proposition 3. *If V,W, and Z are finite-dimensional Hilbert spaces and if $f : V \to W$ and $g : W \to Z$ are continuous, then the composition $(g \circ f) : V \to Z$ is continuous.*

The next important concept, that of a compact set, is often described as a generalization of finite sets.

Definition 16. A set X in a finite-dimensional Hilbert space is *compact* if every collection of open sets that covers X can be reduced to a finite set. More formally, we say that X is compact if, whenever

$$X \subseteq \bigcup_{i \in I} O_i$$

for open sets O_i, there exists a finite subcollection of the O_i that also covers X:

$$\exists m \in \mathbb{N} : X \subseteq \bigcup_{i=1}^{m} O_i.$$

This definition is a bit weird, but it has its roots in a simpler setting. Recall that a *bounded set* X in $\mathbb{R}^n$ is a set whose elements are all contained within some norm ball,

$$X \text{ is bounded} \iff \exists M \in \mathbb{R} : [\forall x \in X : \|x\| < M].$$

Bounded sets are defined similarly in any normed vector space. In $\mathbb{R}^n$ compactness is equivalent to being closed and bounded. However, in a topological space, there is no notion of "bounded," only that of "open." Thus, for compactness to have meaning in more general spaces, the funny Definition 16 is used.

Theorem 3 (Heine-Borel)**.** *In any finite-dimensional Hilbert space, a set is compact if and only if it is both closed and bounded.*

The Heine-Borel theorem is usually stated in $\mathbb{R}^n$, but Theorem 1 says that every finite-dimensional real Hilbert space is basically $\mathbb{R}^n$ for this purpose. Indeed, we have taken it a bit further and dropped the word "real" because the same thing holds in any finite-dimensional Hilbert space, and in particular $\mathbb{C}^n$.

But why should we care about continuity and compactness at all? One of the most important theorems in optimization says that a (real) continuous function on a compact set always achieves its minimum and maximum. This is a result of the next proposition, which says that the continuous image of a compact set is compact.

Proposition 4. *If V, W are finite-dimensional Hilbert spaces with X compact in V and if $f : V \to W$ is continuous, then $f(X)$ is compact in W.* *Rudin Theorem 4.14*

Theorem 4. *Let V be a finite-dimensional Hilbert space. If X is a compact set in V, and if $f : V \to \mathbb{R}$ is a continuous function, then f achieves its maximum/minimum on X. More precisely,* *Rudin Theorem 4.16*

$$\exists x_0 \in X : \sup\left(\{f(x) \mid x \in X\}\right) = f(x_0),$$

and likewise for the infimum. Thus we can replace "sup" with "max" if we like.

Proof. Since Proposition 4 tells us that

$$f(X) \coloneqq \{f(x) \mid x \in X\}$$

is compact, Theorem 3 says that it's closed and bounded. Thus both

$$\sup(f(X)) \quad \text{and} \quad \inf(f(X))$$

are finite real numbers, and are the limit (by the definitions of infimum and supremum) of real numbers in $f(X)$. But then the fact that $f(X)$ is closed implies that those numbers are actually in $f(X)$ itself. □

Example 6. The same is *not* true for non-compact sets: what is the supremum of $f(x) = 1/x$ on the set $X = (0, 1) \subseteq \mathbb{R}$? The open interval X is not compact in this case (by Theorem 3), because it's not closed.

Example 7. Let $X \subseteq \mathbb{R}^n$ be closed and bounded, and let f be continuous on $\mathbb{R}^n$. Then f attains its maximum on X by Theorems 3 and 4, and we can hope to find it. If $A \in \mathbb{R}^{n \times n}$ is some matrix, then the map $x \mapsto Ax$ is continuous, and Proposition 4 tells us that $A(X) \coloneqq \{Ax \mid x \in X\}$ is also a compact set. Thus we can try to maximize f over the set $A(X)$, too.

Finally, there is another definition of compactness called *sequential compactness* that makes some limit arguments easier. For us, sequential compactness and compactness will be the same thing. The following theorem says that compact sets are sequentially-compact, and that's the direction we'll need.

Theorem 5 (sequential compactness)**.** *If V is a finite-dimensional Hilbert space, then $X \subseteq V$ is compact if and only if every sequence in X has some subsequence that converges to a limit in X.*

Rudin, Theorem 3.6

On the other hand, if we are given a convergent sequence, we can put it inside compact set because the sequence itself is bounded by some closed ball.

Theorem 6. *If V is a normed vector space, then every convergent sequence in V is contained in a bounded subset of V. In particular, if V is a finite-dimensional Hilbert space, then every convergent sequence in V is contained inside some compact subset of V.*

Proof. Theorem 3.2 in Rudin states that every convergent sequence in a metric space (of which normed vector spaces are one example) is contained inside some bounded set X. If moreover V is a Hilbert space, then it contains its limits, and $\mathrm{cl}\,(X) \supseteq X$ is a subset of V as well. Thus the closed and bounded (that is, compact) set $\mathrm{cl}\,(X)$ does the job. □

2.4 Algebras

Definition 17. An *algebra* $(\mathcal{M}, \mathcal{R}, \star, \circ)$ consists of,

- A module $(\mathcal{M}, \mathcal{R}, \star)$, where $\mathcal{M} = (M, +, 0, -(\cdot))$ is its abelian group of module elements and $\mathcal{R}$ is its commutative ring.
- A multiplication operation "$\circ$" such that $(M, \circ)$ forms a magma.
- The additional condition that the magma multiplication is bilinear with respect to the addition and scalar multiplication of the module:

$$\forall \alpha \in \mathcal{R}, \forall x, y, z \in M : ((\alpha \star x) + y) \circ z = \alpha \star (x \circ z) + \alpha \star (y \circ z)$$
$$\forall \alpha \in \mathcal{R}, \forall x, y, z \in M : z \circ ((\alpha \star x) + y) = \alpha \star (z \circ x) + \alpha \star (y \circ z)\,.$$

If the magma multiplication is commutative, then the entire structure is called a *commutative algebra*. If $(M, \circ)$ forms a semigroup (that is, if the multiplication is associative), then the entire structure is called an *associative algebra*. If there exists some $1_M \in M$ such that

$$\forall x \in M : 1_M \circ x = x \text{ and } x \circ 1_M = x,$$

then the entire structure is a *unital algebra* and 1_M is its unit element.

The most common application of Definition 17 will be to vector spaces, where the commutative ring happens to be a field. Since every vector space is a module, a vector space that comes with a magmatic multiplication forms an algebra. The reason for the more-general definition is because we want to talk about algebras of polynomials later, and there the coefficients (the scalars)

might not come from a field. Allowing algebras to be over a module also agrees with the SageMath definition in the `MagmaticAlgebras` category:

```
sage: from sage.categories.magmatic_algebras import *
sage: print(MagmaticAlgebras.__doc__)

    The category of algebras over a given base ring.

    An algebra over a ring `R` is a module over `R` endowed
    with a bilinear multiplication...
```

Warning 2: Algebras may not be rings

The "vector multiplication" in an algebra may not be associative. In other words, the vector addition and multiplication may not give rise to a ring, because multiplication must be associative in a ring. In an algebra, multiplication is sometimes commutative, sometimes not. Some algebras have multiplicative unit elements and some don't.

Example 8 (algebra of linear operators)**.** If $(V, \mathbb{F})$ is a vector space, then the $\mathbb{F}$-vector-space of linear operators on V, which we denote by $\mathcal{B}(V)$, forms an associative unital algebra whose multiplication is function composition and whose unit element is the identity operator id_V on V. For $L, M \in \mathcal{B}(V)$ and $\alpha \in \mathbb{F}$, define

$$\begin{aligned} \text{Vector scaling: } & \alpha \star L \coloneqq x \mapsto \alpha L(x) \\ \text{Vector addition: } & L + M \coloneqq x \mapsto L(x) + M(x) \\ \text{Vector multiplication: } & L \circ M \coloneqq x \mapsto L(M(x)). \end{aligned}$$

Normally in this algebra, we write simply αL for $\alpha \star L$ and LM for $L \circ M$ since these objects act like matrices, and that's how we write the corresponding operations for matrices.

Composition is a valid multiplication in this example because both functions are linear. If $N \in \mathcal{B}(V)$ is any other linear operator on V, then

$$\begin{aligned} \forall x \in V : [(\alpha \star L + M) \circ N](x) &= \alpha L(N(x)) + M(N(x)) \\ &= [(\alpha \star (L \circ N)) + (M \circ N)](x) \end{aligned}$$

showing that—as functions, and thus as algebra elements—we have

$$(\alpha \star L + M) \circ N = (\alpha \star (L \circ N)) + (M \circ N) .$$

In other words, our "multiplication" is linear in the first (left) component. The process to show that it's linear in the second component is identical. Combining the two shows that we do indeed have an algebra. Here, the identity operator does somewhat obviously satisfy the definition of a unit element with respect to the algebra multiplication. Thus, this algebra is unital. Finally, function composition is always associative. Since the multiplication in this algebra is composition, that multiplication is associative, and the whole thing is an associative algebra.

Example 9 (algebra of functions)**.** If $(M, R, \cdot)$ is an algebra over R and if F is some set of functions from X to M, then we can add, multiply, and scale them. Define for $f, g \in F$ and $\alpha \in R$,

$$\begin{aligned} \text{Module scaling: } & \alpha \star f \coloneqq x \mapsto \alpha f(x) \\ \text{Module addition: } & f + g \coloneqq x \mapsto f(x) + g(x) \\ \text{Algebra multiplication: } & f \bullet g \coloneqq x \mapsto f(x) \cdot g(x) . \end{aligned}$$

(We have used a dot/disc instead of a circle to indicate algebra multiplication to avoid confusion with function composition.) If the functions defined above belong to F for all $f, g \in F$ and $\alpha \in R$, then with the proper bookkeeping, the set F forms another algebra.

Even if $X = M$, the identity function id_M on M is *not* a unit element for this algebra, since $(\mathrm{id}_M \bullet f)(x) \coloneqq \mathrm{id}_M(x) f(x) = x f(x) \neq f(x)$. However, if $(M, R, \circ)$ is unital with multiplicative unit 1_M, then the constant function $\mathrm{const}_{1_M} \coloneqq x \mapsto 1_M$ works instead:

$$\begin{aligned} (\mathrm{const}_{1_M} \bullet f)(x) &\coloneqq \mathrm{const}_{1_M}(x) \cdot f(x) = 1_M \cdot f(x) = f(x) , \\ (f \bullet \mathrm{const}_{1_M})(x) &\coloneqq f(x) \cdot \mathrm{const}_{1_M}(x) = f(x) \cdot \mathrm{const}_{1_M} = f(x) . \end{aligned}$$

So if $\mathrm{const}_{1_M} \in F$, this algebra is unital as well. Finally, if $(M, R, \cdot)$ is associative, then it easily follows that the algebra of functions is associative too.

Convention 8: Linear function composition

In the algebra of linear operators, we used the function composition symbol $L \circ M$ to indicate the composition of L with M. No one does this: instead, they write LM to mean the same thing. This is by analogy with matrices, where the product of L

and M is written LM and represents the composition of the two functions whose matrix representations are L and M.

From now on, we use juxtaposition to indicate both the composition of linear operators and matrix multiplication.

Example 10. In $\mathbb{R}^3$, the vector *cross product* defined by

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \times \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{bmatrix} \tag{2.1}$$

is a bilinear "multiplication," and thus induces an algebra on $\mathbb{R}^3$.

Exercise 2 (vector cross product is an algebra operation). Show that the cross product defined on $\mathbb{R}^3$ by Equation (2.1) is bilinear, and that it therefore makes $\mathbb{R}^3$ into an algebra. Afterwards, show that the cross product is neither commutative nor associative. A counterexample suffices here; try a few values of x, y, z until commutativity and associativity fail.

In the later chapters, our focus will be on a particular type of commutative (but not associative) type of algebra called a Jordan algebra. The next result tells us that, in that scenario, the "Jordan multiplication" is continuous. A rigorous proof of the same result with a condition for infinite-dimensional spaces is given in Rudin's Theorem 2.17 [14]. Later on in Lemma 2 we do prove something similar in the infinite-dimensional space of multivariate polynomials.

Proposition 5. *If $(\mathcal{V}, \mathbb{F}, \star, \|\cdot\|)$ is a finite-dimensional Hilbert space and if $(\mathcal{V}, \mathbb{F}, \star, \circ)$ forms an algebra, then the algebra multiplication is continuous.*

Proof. Let $\{e_1, e_2, \ldots, e_n\}$ be a basis for $\mathcal{V}$, and suppose that for any $x, y \in \mathcal{V}$ we have the basis representations

$$\begin{aligned} x &= x_1e_1 + x_2e_2 + \cdots + x_ne_n, \text{ and} \\ y &= y_1e_1 + y_2e_2 + \cdots + y_ne_n. \end{aligned}$$

Then using the bilinearity of the multiplication operator, we can expand,

$$x \circ y = \sum_{i=1}^{n} \sum_{j=1}^{n} x_iy_j \left(e_i \circ e_j\right).$$

But here, the products $e_i \circ e_j$ are fixed (they don't involve x or y in any way). As a result, the multiplication function

$$(x, y) \mapsto= \sum_{i=1}^{n} \sum_{j=1}^{n} x_iy_j \left(e_i \circ e_j\right),$$

is now "obviously continuous" by Proposition 3 because it's a composition of things that are continuous—addition and multiplication of the components of x and y by each other and by the constants $e_i \circ e_j$. □

2.5 Solutions to exercises

Solution to Exercise 1 (continuous preimage of closed set is closed). First we show that $f^{-1}(W \setminus Y) = f^{-1}(W) \setminus f^{-1}(Y)$ for all subsets Y of W. Suppose that $x \in f^{-1}(W \setminus Y)$; then by definition of the preimage, $f(x) \in W$ but $f(x) \notin Y$. Thus x is in $f^{-1}(W)$, but not in $f^{-1}(Y)$. In other words, $x \in f^{-1}(W) \setminus f^{-1}(Y)$. In the other direction, suppose that $x \in f^{-1}(W) \setminus f^{-1}(Y)$. Then $f(x) \in W$, but $f(x) \notin Y$ since $x \notin f^{-1}(Y)$. This is the same thing as saying that $x \in f^{-1}(W \setminus Y)$.

Now that we know that preimage "plays nice" with complements, suppose that $Y \subseteq W$ is closed. By definition, Y is the complement of some open set in W; let's say $Y = W \setminus X$. Then we have

$$f^{-1}(Y) = f^{-1}(W \setminus X) = f^{-1}(W) \setminus f^{-1}(X) = V \setminus f^{-1}(X)$$

and this set should be closed: the whole space V is always closed, and $f^{-1}(X)$ is open because X is open and f is continuous. Thus $f^{-1}(Y)$ is the complement of the open set $f^{-1}(X)$ in V, and is therefore closed.

Solution to Exercise 2 (vector cross product is an algebra operation). Let $\alpha \in \mathbb{R}$, and suppose that

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \; y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}, \; z = \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}.$$

First we show that the cross product is linear in the first component:

$$\begin{aligned}
(\alpha x + y) \times z &\coloneqq \begin{bmatrix} (\alpha x_2 + y_2) z_3 - (\alpha x_3 + y_3) z_2 \\ (\alpha x_3 + y_3) z_1 - (\alpha x_1 + y_1) z_3 \\ (\alpha x_1 + y_1) z_2 - (\alpha x_2 + y_2) z_1 \end{bmatrix} \\
&= \begin{bmatrix} \alpha x_2 z_3 + y_2 z_3 - \alpha x_3 z_2 - y_3 z_2 \\ \alpha x_3 z_1 + y_3 z_1 - \alpha x_1 z_3 - y_1 z_3 \\ \alpha x_1 z_2 + y_1 z_2 - \alpha x_2 z_1 - y_2 z_1 \end{bmatrix} \\
&= \begin{bmatrix} (\alpha x_2 z_3 - \alpha x_3 z_2) + (y_2 z_3 - y_3 z_2) \\ (\alpha x_3 z_1 - \alpha x_1 z_3) + (y_3 z_1 - y_1 z_3) \\ (\alpha x_1 z_2 - \alpha x_2 z_1) + (y_1 z_2 - y_2 z_1) \end{bmatrix} \\
&= \alpha (x \times z) + (y \times z).
\end{aligned}$$

The same thing needs to happen in the second component:

$$\begin{aligned} x \times (\alpha y + z) &\coloneqq \begin{bmatrix} x_2 (\alpha y_3 + z_3) - x_3 (\alpha y_2 + z_2) \\ x_3 (\alpha y_1 + z_1) - x_1 (\alpha y_3 + z_3) \\ x_1 (\alpha y_2 + z_2) - x_2 (\alpha y_1 + z_1) . \end{bmatrix} \\ &= \begin{bmatrix} \alpha x_2 y_3 + x_2 z_3 - \alpha x_3 y_2 - x_3 z_2 \\ \alpha x_3 y_1 + x_3 z_1 - \alpha x_1 y_3 - x_1 z_3 \\ \alpha x_1 y_2 + x_1 z_2 - \alpha x_2 y_1 - x_2 z_1 . \end{bmatrix} \\ &= \begin{bmatrix} (\alpha x_2 y_3 - \alpha x_3 y_2) + (x_2 z_3 - x_3 z_2) \\ (\alpha x_3 y_1 - \alpha x_1 y_3) + (x_3 z_1 - x_1 z_3) \\ (\alpha x_1 y_2 - \alpha x_2 y_1) + (x_1 z_2 - x_2 z_1) . \end{bmatrix} \\ &= \alpha (x \times y) + (x \times z) . \end{aligned}$$

To show that the cross product is neither associative or commutative, the following example suffices:

```
sage: e1 = vector(QQ,[1,0,0])
sage: e2 = vector(QQ,[0,1,0])
sage: e3 = vector(QQ,[0,0,1])
sage: e1.cross_product(e2)
(0, 0, 1)
sage: e2.cross_product(e1)
(0, 0, -1)
sage: e = e1 + e2 + e3
sage: (e.cross_product(e2)).cross_product(e3)
(0, 1, 0)
sage: e.cross_product(e2.cross_product(e3))
(0, 1, -1)
```

Chapter 3

Polynomials and power-associativity

3.1 Univariate polynomials

One of the most important rings is the ring of polynomials. If R is some other commutative ring, we write $R[X]$ to denote the ring of polynomials with coefficients in R and one variable X. Informally, a polynomial $p \in R[X]$ of degree d is an expression that looks like

$$\alpha_0 X^0 + \alpha_1 X^1 + \cdots + \alpha_d X^d$$

for some coefficients $\alpha_i \in R$. This corresponds to a "polynomial function,"

$$x \mapsto \alpha_0 + \alpha_1 x + \cdots + \alpha_d x^d,$$

and multiplication, addition, and scaling of $p, q \in R[X]$ are defined in a way that makes everything agree with the corresponding operations on "polynomial functions" in the algebra of functions. Equality, however, is more subtle: we say that two polynomials p and q in $R[X]$ are equal if and only if the coefficients of their respective powers of X are equal as elements of R. This is all very hand-wavy, which is why we make the following formal definition.

Beachy and Blair, Example 5.1.2

Definition 18. If R is a commutative ring, and if we define the infinite cartesian product

$$R^\infty \coloneqq \bigtimes_{i=0}^{\infty} R = \left\{ (a_0, a_1, a_2, \ldots)^T \;\middle|\; a_i \in R \right\},$$

then the commutative *univariate polynomial ring over* R, or *the ring of univariate polynomials with coefficients in* R, is

$$R[X] \coloneqq \left\{ (a_0, a_1, \ldots)^T \in R^\infty \;\middle|\; a_i \neq 0 \text{ for only finitely many } i \right\} \subseteq R^\infty.$$

under suitable addition, subtraction, and multiplication operations. The definition of equality, inherited from R^∞, is componentwise. The symbol X is merely a name that we assign by convention to the element $(0,1,0,0,\ldots)^T$. For compatibility with the way we write polynomial functions, we further define

$$\begin{aligned} X^0 &= (1,0,0,0,0,\ldots)^T, \\ X^2 &= (0,0,1,0,0,\ldots)^T, \\ X^3 &= (0,0,0,1,0,0\ldots)^T, \\ &\vdots \end{aligned}$$

Thus X^k is shorthand for the tuple with 1 in its k^{th} component and zeros elsewhere.

Addition and subtraction in $R[X]$ are pointwise, "obvious," and in fact inherited from the module R^∞. If $p = (a_0, a_1, \ldots)^T$, $q = (b_0, b_1, \ldots)^T$, then

$$\begin{aligned} p + q &\coloneqq (a_0 + b_0, a_1 + b_1, \ldots)^T && \text{(addition)} \\ p - q &\coloneqq (a_0 - b_0, a_1 - b_1, \ldots)^T && \text{(subtraction).} \end{aligned}$$

Corresponding to these operations, we have the additive unit element $(0,0,\ldots)^T$, also inherited from R^∞, such that

$$(0,0,\ldots)^T + (a_0, a_1, \ldots)^T = (0 + a_0, 0 + a_1, \ldots)^T = (a_0, a_1, \ldots)^T.$$

The ring laws for addition all hold in $R[X]$ because equality in $R[X]$ is defined componentwise, and the ring laws hold in each component due to R itself being a ring. Sums and differences of polynomials all have a finite number of nonzero entries, because, for example, in $p + q$ you're eventually just adding $0 + 0$ componentwise. Defining multiplication, on the other hand, is a bit trickier and is left as an exercise.

Exercise 3 (polynomial multiplication). Suppose that R is a commutative ring, and let $p, q \in R[X]$ be given by

$$\begin{aligned} p &= (a_0, a_1, a_2, \ldots, a_I, 0, 0, \ldots)^T, \\ q &= (b_0, b_1, b_2, \ldots, b_J, 0, 0, \ldots)^T. \end{aligned}$$

From Definition 18, we see that these elements can be expressed as

$$p = \sum_{i=0}^{I} a_i X^i \quad \text{and} \quad q = \sum_{j=0}^{J} b_j X^j.$$

Define the product pq in a way that agrees with your intuition about how polynomial functions should act. Specifically, your formula should satisfy $X^i X^j =$

X^{i+j}, and therefore X^0 should be the multiplicative unit element. Prove that your multiplication is commutative, associative, and distributes over addition.

In hindsight, the name X in $R[X]$ is completely irrelevant; the ring $R[Y]$ is identical to $R[X]$. Both Y and X simply refer to a polynomial that already exists in the ring. We will however try not to be too pedantic in this regard.

Simplification 2: This ring is an algebra, but it's a ring

The ring $R[X]$ naturally forms an algebra under Definition 18 since we can scale polynomials by elements of R just like we'd scale a vector. But we're going to do what everyone does and ignore the "scaling" operation to treat $R[X]$ as a ring.

In a ring, there's only one set to worry about, the things that get added and multiplied. In an algebra, there's two: you also need a set of scalars, which is often (but not necessarily) different from the set of ring elements. For the polynomial ring $R[X]$ in particular, there are several reasonable choices for the scalars... which means that we'd always have to state which one we're using if we wanted to treat $R[X]$ as an algebra.

Particularly in multivariate polynomial rings, the "obvious" scaling operation isn't the one that makes them act like multivariate polynomial functions. In summary: treating the polynomials as an algebra makes a lot of things pointlessly awkward, so we avoid it except in a few critical special cases.

Definition 19. The *degree* of a nonzero polynomial $(a_0, a_1, \ldots)^T \in R[X]$ is

Beachy and Blair, Example 5.1.2

$$\deg\left((a_0, a_1, \ldots)^T\right) \coloneqq \max\left(\{i \in \mathbb{N} \mid a_i \neq 0\}\right).$$

The degree of the zero polynomial is undefined.

Definition 20. If $p = (a_0, a_1, \ldots)^T \in R[X]$ is a nonzero polynomial and if $d \coloneqq \deg(p)$ is the degree of p, then p is *monic* if and only if $a_d = 1_R$.

Beachy and Blair, Definition 4.1.4

Proposition 6. *If R is a commutative ring, then the ring $R[X]$ is commutative and unital, and $\left\{X^k \;\middle|\; k \in \mathbb{N}\right\}$ is a basis for the underlying free module.*

Of course, every polynomial $p \in R[X]$ induces a "polynomial function" on R in an obvious way. To be clear, when we talk about a "polynomial function," we mean something like the following.

Definition 21. If R is a commutative ring and if $(M, R, \circ)$ is an associative unital algebra over R, then to each $p = (a_0, a_1, \ldots, a_d, 0, 0, \ldots)^T \in R[X]$ we define the associated *polynomial function on* R,

$$\begin{aligned} &p\restriction_M : M \to M \\ &p\restriction_M := x \mapsto a_0 x^0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \end{aligned}$$

that lives in a *different* algebra, namely the algebra of functions on M (Example 9). The addition, subtraction, and multiplication operations in $R[X]$ are defined precisely so that the map $p \mapsto p\restriction_M$ is a ring homomorphism. In general, each polynomial object could have many associated functions, each with different domains and/or codomains. The notation above is an abuse of the function restriction notation $f\restriction_X$, because that symbol means something like "think of f as being a function defined on X instead," which is more or less what we want to say about the polynomial.

Example 11. If R is a commutative ring, then in particular, R forms a commutative algebra over itself. As a result, the function

$$\begin{aligned} &p\restriction_R : R \to R \\ &p\restriction_R = x \mapsto a_0 x^0 + a_1 x + a_2 x^2 + \cdots + a_d x^d, \end{aligned}$$

is defined on R.

Example 12. Let V be a finite-dimensional vector space over $\mathbb{R}$, and recall the associative unital algebra of linear operators on V. If

$$p = a_0 X^0 + a_1 X + a_2 X^2 + \cdots + a_d X^d \in \mathbb{R}[X],$$

then we can evaluate p on a linear operator L to get back another linear operator,

$$p\restriction_{\mathcal{B}(V)}(L) = a_0 L^0 + a_1 L + a_2 L^2 + \cdots + a_d L^d \in \mathcal{B}(V).$$

This idea is used extensively in the study of minimal and characteristic polynomials for linear operators.

Later we'll want to do the same sort of thing in a Euclidean Jordan algebra, which is *not* associative. This only works when the algebra has another special property, called *power-associativity*, that we discuss in Section 3.5.

Convention 9: Polynomial notation

We will write

$$p = a_0 X^0 + a_1 X + a_2 X^2 + \cdots + a_d X^d \in R[X],$$

to indicate the polynomial object

$$p = (a_0, a_1, \ldots, a_d, 0, 0, \ldots)^T.$$

Specifying the ring $R[X]$ ensures that the terms X^i are interpreted as infinite tuples (the basis for R^∞), and not as literal powers of some function's argument. Likewise, whenever we specify that some object lives in a polynomial ring, like

$$\left(X - \lambda_1 X^0\right)\left(X - \lambda_2 X^0\right)\cdots\left(X - \lambda_d X^0\right) \in R[X],$$

we mean that the multiplication should be carried out formally in the ring $R[X]$ to obtain some infinite tuple as the result. (After Section 3.3, we will cease to litter every equation with X^0 symbols.)

On the other hand, when we wish to talk about a polynomial *function*, we will usually specify its domain and codomain, and will always refer to it using the "restriction" notation,

$$\begin{aligned} &p\restriction_R : R \to R \\ &p\restriction_R = x \mapsto a_0 x^0 + a_1 x + a_2 x^2 + \cdots + a_d x^d. \end{aligned}$$

The codomain does not appear in the symbol $p\restriction_R$, but we will never have two polynomials in scope with the same domains and different codomains, so hopefully no confusion ensues.

Remark 3. When we express a polynomial

$$p = a_0 X^0 + a_1 X + a_2 X^2 + \cdots + a_d X^d \in R[X] \tag{3.3}$$

in terms of the basis $X^0, X^1, \ldots$, then the degree of p (from Definition 19) will be the largest exponent appearing in that expression after all of the products have been expanded. When written in a form like Equation (3.3), the degree is easy to determine. However, when the polynomial is written as a product like $\left(X - b_1 X^0\right)\left(X^2 + b_2 X^0\right)$, its degree (which is three, in this case) is not obvious

because the highest power X^3 doesn't appear until after the multiplication is carried out.

Example 13. If $p, q \in R[X]$ are both monic and have the same degree $d \coloneqq \deg(p) = \deg(q)$, then $\deg(p-q) < d$. Using our notation, we can write p and q in terms of the basis elements $X^0, X^1, \ldots, X^d$,

$$p = a_0X^0 + a_1X^1 + \cdots + a_{(d-1)}X^{d-1} + X^d$$
$$q = b_0X^0 + b_1X^1 + \cdots + b_{(d-1)}X^{d-1} + X^d.$$

Subtracting, we obtain

$$p - q = c_0X^0 + c_1X^1 + \cdots + c_{(d-1)}X^{d-1} + 0X^d,$$

where $c_i \coloneqq a_i - b_i$, and $c_d = 1 - 1 = 0$. The maximum index i such that c_i is non-zero is now at most $d-1$, so $\deg(p-q) \leq d-1$.

Example 14. If $p, q \in \mathbb{F}[X]$ for some field $\mathbb{F}$, then $\deg(pq) = \deg(p) + \deg(q)$. Suppose that $\deg(p) = m$ and $\deg(q) = n$, and let

$$p = a_0X^0 + a_1X^1 + \cdots + +a_mX^m$$
$$q = b_0X^0 + b_1X^1 + \cdots + +b_nX^n.$$

Then formally multiplying the two gives

$$pq = c_0X^0 + \cdots + c_{(m+n)}X^{m+n},$$

where $c_0 = a_0b_0$, $c_{m+n} = a_mb_n$, and X^{m+n} is clearly the largest power that appears. Now because $\mathbb{F}$ is a field and since $a_m, b_n \in \mathbb{F}$ were non-zero, their product is non-zero as well. Thus, c_{m+n} is the (non-zero) coeffcient of the largest power of X appearing in pq, and its index $m+n = \deg(p) + \deg(q)$ is the degree of pq.

Warning 3: Polynomials outnumber functions

If $p = q$ in $R[X]$, then clearly $p\restriction_R(x) = q\restriction_R(x)$ for all $x \in R$. However, the converse is not generally true. Over some rings, we'll have equality of the functions $p\restriction_R = q\restriction_R$, but have $p \neq q$ as polynomial objects. This depends on the ring R, and is Example 4.1.4 in Beachy and Blair.

Exercise 1. *Find a commutative ring R and a two polynomials $p, q \in R[X]$ such that $p\restriction_R(x) = q\restriction_R(x)$ for all $x \in R$, but $p \neq q$ in $R[X]$.*

The converse does hold under some additional assumptions, one of which we'll prove. Unfortunately we have to do this in a pretty general setting, because we'll eventually want the result to apply to multivariate polynomial rings.

Recall that a *root* of a function f is a value x such that $f(x) = 0$. We'll want to be a little careful throwing around the word "root" in the context of polynomials to avoid confusion. People often talk about the "roots of a polynomial," but unless you know which function they're talking about, the term can be ambiguous. We have already seen in Examples 11 and 12 that there can be more than one function associated with a single polynomial, and those functions will have different roots.

Lemma 1. *If R is an integral domain and if $f \in R[X]$ is a nonzero polynomial, then $f\restriction_R$ has at most $\deg(f)$ roots.*

Proof. Using the division algorithm (Theorem 4.2.1 in Beachy and Blair), we can pick any $c \in R$ and divide f by $g := (X - c)$ to obtain $f = qg + r$, where $q, r \in R[X]$ and either $\deg(r) < \deg(g) = 1$, or $r = 0$. In Beachy and Blair, the division algorithm is stated only for polynomials over a field; however, it is easy to check that when g is monic, the proof goes through without ever needing to use the fact that the coefficients come from a field. For peace of mind, refer to Theorem 19 in Mac Lane and Birkhoff [9].

Now since either $r = 0$ or $\deg(r) = 0$, we may think of r as being a scalar multiple of 1_R, a "constant polynomial." Thus, evaluating, we have

$$f\restriction_R(c) = 0 \iff r = 0 \iff f = q(X - c) \iff (X - c) \mid f.$$

Thus, $f\restriction_R(c) = 0$ if and only if $X - c$ divides f in $R[X]$.

We proceed by induction. The statement holds if $\deg(f) = 0$, since then $f\restriction_R$ is a (nonzero) constant function with no roots. Assuming it holds for $\deg(f) = k$, we want to show that it holds for $\deg(f) = k + 1$ as well. Suppose $c \in R$ is a root of $f\restriction_R$. Then we can divide f by $(X - c)$ and conclude that $f = q(X - c)$, where the degree of q is necessarily one less than the degree of f. Since R is an integral domain, any root d of $f\restriction_R$ satisfies $f\restriction_R(d) = q\restriction_R(d)(d - c) = 0$, implying either that $d = c$, or that d is a root of $q\restriction_R$ (which has at most k possible roots, by our assumption). The one root of $(X - c)\restriction_R$ and the at-most k roots of $q\restriction_R$ give at most $k + 1$ roots of $f\restriction_R$. □

Theorem 7. *If $(V, R, \circ)$ is a nontrivial, associative, and unital algebra over an infinite integral domain R and if $p\restriction_V = q\restriction_V$ as functions on V, then $p = q$ in $R[X]$. As a result, the map $p \mapsto p\restriction_V$ is a ring isomorpism.*

Proof. Addition and multiplication in $R[X]$ are defined so that the map $p \mapsto p\restriction_V$ is a ring homomorphism, where now we think of

$$p\restriction_V : V \to V$$
$$p\restriction_V = x \mapsto a_0 1_V + a_1 x + a_2 x^2 + \cdots + a_k x^k$$

as a polynomial function on V. The only question that remains is whether or not two distinct elements of $R[X]$ can map to the same function on V. Let

$$p = (a_0, a_1, \ldots, a_k, 0, 0, \ldots)^T, \text{ and}$$
$$q = (b_0, b_1, \ldots, b_\ell, 0, 0, \ldots)^T$$

be two polynomials in $R[X]$. If $p \neq q$, then they differ in one or more coordinates. Let d be the largest index where $p_d \neq q_d$. Then

$$\forall \alpha \in R : \begin{cases} (p\restriction_V - q\restriction_V)(\alpha 1_V) \\ = \\ (a_0 - b_0)1_V + \alpha(a_1 - b_1)1_V + \cdots + \alpha^d(a_d - b_d)1_V \end{cases}$$

which can never be identically zero. If it were, then since $1_V \neq 0$, we would conclude that

$$\forall \alpha \in R : (a_0 - b_0) + \alpha(a_1 - b_1) + \cdots + \alpha^d(a_d - b_d) = 0.$$

But, this is the same thing as saying that

$$\forall \alpha \in R : (p - q)\restriction_R(\alpha) = 0.$$

That cannot happen, as it would give us an infinite number of roots for the polynomial function $(p-q)\restriction_R$, in violation of Lemma 1. Thus, $p\restriction_V \neq q\restriction_V$, and we have shown that the map $p \mapsto p\restriction_V$ is injective. All of the other pieces were already in place, so we conclude that $p \mapsto p\restriction_V$ is a ring isomorphism. □

It follows that $p \mapsto p\restriction_V$ is a ring isomorphism when the underlying algebra is over an infinite field like $\mathbb{R}$. We will use this result liberally later on.

Corollary 1. *If R is an infinite integral domain, then $p \mapsto p\restriction_R$ is a ring isomorphism.*

Corollary 2. *If $\mathbb{F}$ is an infinite field, then $p \mapsto p\restriction_{\mathbb{F}}$ is a ring isomorphism.*

Definition 22. If R is a commutative ring and if $X \subseteq R$, then the *ring ideal of R generated by X* is

$$\text{ideal}(X) \coloneqq \left\{ \sum rx \;\middle|\; r \in R, x \in X \right\}.$$

Theorem 8. *If R is a field, then every ring ideal I in $R[X]$ is generated by a single element,*

$$\exists p \in R[X] : I = \text{ideal}(\{p\}).$$

In other words, $R[X]$ is a principal ideal domain.

Beachy and Blair, Theorem 4.2.2 and Example 5.3.2

This is a well-known result that you should keep in the back of your mind for the rest of your life. It follows fairly easily from the polynomial division algorithm Theorem 4.2.1 in Beachy and Blair. It's also useful for determining when one polynomial expressed as a product of irreducible factors divides another.

Proposition 7. *If D is a principal ideal domain, if $p \in D$ is irreducible, and if $q, r \in D$ with $p \mid qr$, then $p \mid q$ or $p \mid r$.*

Beachy and Blair, Proposition 9.1.8

Corollary 3. *If R is a field and if $p \mid q$ for some $p, q \in R[X]$ that factor into monic irreducible terms as*

$$q = \left(X - a_1 X^0\right)\left(X - a_2 X^0\right) \cdots \left(X - a_k X^0\right)$$

and

$$p = p_1 p_2 \cdots p_\ell,$$

then $\ell \leq k$ and each p_i is equal to some $\left(X - a_j X^0\right)$. In other words, p is a product of some subset of the monic irreducible factors of q, and the roots of $p\restriction_R$ are a subset of the roots of $q\restriction_R$.

Proof. The polynomial ring $R[X]$ is a principal ideal domain by Theorem 8. Each irreducible factor p_i of p must also divide q by Proposition 9.1.3 in Beachy and Blair. By induction/recursion, this means that p_i must divide some irreducible factor $\left(X - a_j X^0\right)$ of q; and the only way that can happen is if they are equal. Thus the irreducible factors of p are a subset of those of q. □

The SageMath project was started by algebraic geometers, so it has strong support for polynomials. One nice feature is that, in a univariate polynomial ring, it can compute the unique generator of every ideal.

```
sage: R = PolynomialRing(QQ, 'X')
sage: X = R.gen()
sage: p1 = X^4 - 2*X^3 + 2*X - 4
sage: p2 = X^3 - X^2 - 6*X + 8
sage: R.ideal([p1,p2])
Principal ideal (X - 2) of Univariate Polynomial Ring in
X over Rational Field
```

Before we move on to multivariate polynomials, we record a folklore theorem that says something like "the roots of a real polynomial function are continuous functions of the polynomial's coefficients." A precise statement of this result is a bit technical and perilous, especially in the real case, so we punt and cite it from someone else [1].

Theorem 9. *If $p \in \mathbb{R}[X]$ is a monic polynomial of degree $d \geq 1$, that is if*

Alexandrian, Theorem 3.5

$$p = X^d + \sum_{k=0}^{d-1} a_k X^k \in \mathbb{R}[X]$$

and if λ is a root of $p\restriction_{\mathbb{R}}$ with multiplicity one, then for all sufficiently-small $\epsilon > 0$ there exists a $\delta > 0$ such that for any

$$q = X^d + \sum_{k=0}^{d-1} b_k X^k \in \mathbb{R}[X]$$

satisfying $|a_k - b_k| < \delta$ for all $k \in \{0, 1, \ldots, d-1\}$, the polynomial function $q\restriction_{\mathbb{R}}$ has a root μ of multiplicity one with $|\lambda - \mu| < \epsilon$.

This statement is awkward to parse, but if you've seen the infinity norm before, it's defined on $\mathbb{R}^n$ to be $\|x\|_\infty \coloneqq \max\{|x_i| \mid i \in \{0, 1, 2, \ldots, n\}\}$. If we extend that definition to $\mathbb{R}[X]$, then the condition on the coeffcients a_k and b_k in Theorem 9 simply says that $\|p - q\|_\infty < \delta$, so it's a typical continuity condition. Stated casually: if $p\restriction_{\mathbb{R}}$ has a real multiplicity-one root and if q is close to p, then $q\restriction_{\mathbb{R}}$ also has a real multiplicity-one root nearby.

3.2 Multivariate polynomials

We can also define polynomials with other numbers of variables, like zero or two. Recall that we constructed $R[X_1]$ as a subset of the free module

$$R^\infty \coloneqq \bigtimes_{i=0}^{\infty} R = \left\{ (a_0, a_1, a_2, \ldots)^T \;\middle|\; a_i \in R \right\}.$$

This is a Cartesian product, made up of countably-infinite copies of R with pointwise addition and subtraction. The subset $R[X_1]$, when endowed with a multiplication, gives rise to the univariate polynomial ring.

To construct a *multivariate* polynomial ring, we simply repeat the process, defining $R[X_1, X_2] \coloneqq (R[X_1])[X_2]$. Since $R[X_1]$ is itself a commutative ring by Proposition 6, this results in another polynomial ring whose coefficients now come from $R[X_1]$. In other words, a multivariate polynomial ring is just a univariate polynomial ring but with coefficients in some other polynomial ring. This means that technically, our Definition 19 of the degree of a polynomial extends to multivariate polynomials. Likewise, we can use Definition 20 to talk about monic multivariate polynomials. But please, don't. No one is going to know what you're talking about. We will never use either term in a multivariate context.

Proposition 8. *If R is a commutative ring, then $R[X_1, X_2, \ldots, X_n]$ is a commutative ring.*

Proof. True for R and $R[X_1]$, and if you assume that it's true with $n-1$ variables, then by definition, the induction hypothesis says it works for n variables as well. □

SageMath supports multivariate polynomials too, and lets you treat them like functions of multiple variables so long as the base ring is commutative.

```
sage: R = PolynomialRing(QQ, ['X', 'Y', 'Z'])
sage: X,Y,Z = R.gens()
sage: p = (-1)*X + (3/4)*Y - 8*Z
sage: p
-X + 3/4*Y - 8*Z
sage: p(X=0, Y=0, Z=2)
-16
```

These functions will play a big part later on because we'll be evaluating them on the coordinates x_1, x_2, x_n of a vector x in some n-dimensional vector space. When we do so, we will use the fact that the multiple-argument polynomial function is continuous. Let's define precisely what we mean by these statements. For notational convenience, we'll use a single symbol to denote a generic multivariate polynomial ring.

Definition 23. If R is a commutative ring, then we denote a general polynomial ring with coefficients in R and n indeterminates $X_1, X_2, \ldots, X_n$ by

$$\mathbb{P}^n(R) \coloneqq \begin{cases} R & \text{if } n = 0, \\ R[X_1, X_2, \ldots, X_n] & \text{otherwise} \end{cases}.$$

Keeping in mind our recursive definition of multivariate polynomial rings, this definition is also recursive, because $\mathbb{P}^n(R) = \mathbb{P}^{n-1}(R)[X_n]$.

If you think of $\mathbb{P}^1(R)$ as an operation that adds one variable to R, then the notation $\mathbb{P}^n(R)$ can be thought of as performing the "add one variable" operation n times.

Definition 24. Suppose that R is a commutative ring and that $p \in \mathbb{P}^n(R)$. We define a multivariate polynomial function $p\restriction_{R^n} : R^n \to R$ recursively by,

$$p\restriction_{R^n} = x \mapsto \begin{cases} p\restriction_R(x_n) & \text{if } n = 1, \\ [p\restriction_R(x_n)]\restriction_{R^{n-1}}\left((x_1, \ldots, x_{n-1})^T\right) & \text{if } n > 1. \end{cases}$$

The recursive definition of multivariate polynomials and functions is convenient in some aspects—particular for proofs by induction—but is overly cumbersome in others. This next proposition gives us an explicit representation of a multivariate polynomial in terms of its indeterminates, which amounts to a basis representation. This will make it obvious, for example, that multivariate polynomial functions are continuous.

Proposition 9. *Suppose that R is a commutative ring, that $p \in \mathbb{P}^n(R)$, and that d_k is the largest power of X_k appearing in p. Then there exist $a_{(i_1,i_2,\ldots,i_n)} \in$*

R, for $i_k \in \{0, 1, \ldots, d_k\}$*, such that*

$$p = \sum_{i_1=0}^{d_1} \sum_{i_2=0}^{d_2} \cdots \sum_{i_n=0}^{d_n} a_{(i_1,i_2,\ldots,i_n)} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \tag{3.4}$$

and the function $p\restriction_{R^n} : R^n \to R$ *in Definition 24 is given explicitly by*

$$p\restriction_{R^n} = x \mapsto \sum_{i_1=0}^{d_1} \sum_{i_2=0}^{d_2} \cdots \sum_{i_n=0}^{d_n} a_{(i_1,i_2,\ldots,i_n)} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Proof. The form of p follows from induction. Clearly, for $n = 1$, we have

$$p = \sum_{i_1}^{d_1} a_{i_1} X_1^{i_1} \quad \text{with} \quad a_{i_1} \in R$$

which is already what we're looking for. If we assume the form Equation (3.4) for polynomials with $n-1$ variables, then a polynomial in n variables is by our definition just a univariate polynomial with coefficients in a ring of some more polynomials:

$$p = \sum_{i_n}^{d_n} C_{i_n} X_n^{i_n}, \text{ where } C_{i_n} \in \mathbb{P}^{n-1}(R).$$

Now apply the induction hypothesis to C_{i_n},

$$p = \sum_{i_n}^{d_n} \underbrace{\left[\sum_{i_1=0}^{d_1} \sum_{i_2=0}^{d_2} \cdots \sum_{i_{n-1}=0}^{d_{n-1}} a_{(i_1,i_2,\ldots,i_{n-1})} X_1^{i_1} X_2^{i_2} \cdots X_{n-1}^{i_{n-1}} \right]}_{C_{i_n}} X_n^{i_n}.$$

Since each C_{i_n} has its own coefficients that we've written $a_{(i_1,i_2,\ldots,i_{n-1})}$, it makes sense to label them $a_{(i_1,i_2,\ldots,i_{n-1},i_n)}$ instead. Now just distribute and reorder the sums to achieve the desired form.

Now that we know p has the form Equation (3.4), it is straightforward to show what the evaluation functions look like, too. Again, for $n = 1$, the result is trivial and follows from immediately from the $n = 1$ case in Definition 24, which is just univariate polynomial function evaluation:

$$p = \sum_{i_1=0}^{d_1} a_{i_1} X_1^{i_1} \in \mathbb{P}^1(R) \implies p\restriction_{R^1} = x_1 \mapsto \sum_{i_1=0}^{d_1} a_{i_1} x_1^{i_1} \in \mathbb{P}^0(R).$$

Now, assuming that the result holds in $\mathbb{P}^{n-1}(R)$, we have for the $n > 1$ case,

$$\begin{aligned} p\restriction_{R^n} = x \mapsto [p\restriction_R (x_n)]\restriction_{R^{n-1}} \left((x_1, \ldots, x_{n-1})^T\right) \\ = \left[\sum_{i_n}^{d_n} C_{i_n} x_n^{i_n}\right]\restriction_{R^{n-1}} \left((x_1, \ldots, x_{n-1})^T\right) \\ = \sum_{i_n}^{d_n} C_{i_n}\restriction_{R^{n-1}} \left((x_1, \ldots, x_{n-1})^T\right) x_n^{i_n}. \end{aligned}$$

Apply the inductive hypothesis here, expand, and rename the coefficients again to achieve the desired result. □

Simplification 3: Explicit multivariable polynomials

Proposition 9 is how you should think of multivariate polynomials and their associated functions. We've defined everything carefully by induction/recursion to be sure that it works, but the explicit formulas are what make most results "obvious."

An explicit representation also allows us to define the concept of a homogeneous polynomial, which will be useful later in one very specific but critical situation.

Definition 25. Let R be a commutative ring. If $p \in \mathbb{P}^n(R)$, then we say that p is a *homogeneous polynomial* of degree k if $i_1 + i_2 + \cdots + i_n = k$ whenever $a_{(i_1,i_2,\ldots,i_n)} \neq 0$ in Equation (3.4). If M is a module over R, then $f : M \to R$ is a *homogeneous function* of degree k if $f(\alpha x) = \alpha^k f(x)$ for all $x \in M$ and all $\alpha \in R$.

The explicit form of a multivariate polynomial in Proposition 9 is nothing more than a basis representation; the set $\left\{X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \;\middle|\; i_1, i_2, \ldots, i_n \in \mathbb{N}\right\}$ is the basis for the space. The explicit form makes a lot of tricky things "obvious." For example, we can now see that the polynomial-to-function mapping is a homomorphism, and that it extends to something "homomorphism-like" for the functions associated with matrices of polynomials as in Convention 10.

Proposition 10. *If R is a commutative ring, then the mapping $p \mapsto p\restriction_{R^n}$ from $\mathbb{P}^n(R)$ into the corresponding algebra of functions is a ring homomorphism. Moreover, if two matrices A, B have entries in $\mathbb{P}^n(R)$ and if their dimensions are compatible (if matrix addition and multiplication make sense), then*

$$\forall x \in R^n : \begin{cases} [AB]\restriction_{R^n}(x) = A\restriction_{R^n}(x)\, B\restriction_{R^n}(x), \text{ and} \\ [A+B]\restriction_{R^n}(x) = A\restriction_{R^n}(x) + B\restriction_{R^n}(x). \end{cases}$$

Proof. The fact that $p \mapsto p\restriction_{R^n}$ is a ring homomorphism follows from Proposition 9 which lets you check the homomorphism conditions directly. Using the formula for matrix multiplication,

$$[AB]_{ij} \coloneqq \sum_{\ell=1}^{m} A_{i\ell} B_{\ell j}.$$

And since we just showed that $M_{ij} \mapsto M_{ij}\restriction_{R^n}$ is a homomorphism,

$$\begin{aligned}[AB]_{ij}\restriction_{R^n}(x) &= \sum_{\ell=1}^{n} A_{i\ell}\restriction_{R^n}(x)\, B_{\ell j}\restriction_{R^n}(x) \\ &= \left[A\restriction_{R^n}(x)\, B\restriction_{R^n}(x)\right]_{ij},\end{aligned}$$

The corresponding claim for addition is similar but easier. □

Since we went to the trouble of defining an R-module in Definition 9, we might as well look at one more imporant example: matrices with polynomial entries form a module over the coefficient ring of those polynomials.

Example 15. Let R be a commutative ring, and $\mathbb{P}^n(R)$ be the ring of polynomials in n variables whose coefficients come from R. Consider the set M of m-by-1 column matrices whose entries are in $\mathbb{P}^n(R)$, Roman, Example 4.1.2

$$M = \left\{ (p_1, p_2, \ldots, p_m)^T \;\middle|\; p \in \mathbb{P}^n(R) \right\} = \left[\mathbb{P}^n(R)\right]^{m\times 1}.$$

Recall Definition 10. The set M forms a free module over the ring $\mathbb{P}^n(R)$, with the entries of the matrix and the scalars both being polynomials: the zero polynomial is in M, you can add two elements of M together to get another element of M, and you can scale an element of M by $s \in \mathbb{P}^n(R)$ to get $(sp_1, sp_2, \ldots, sp_m)^T$. All of the module laws are satisfied, so we have a module.

We can also construct matrices to act on M. Suppose that $A \in \left[\mathbb{P}^n(R)\right]^{m\times m}$. Then if $x \in M$, the product Ax is defined in exactly the way that matrix multiplication normally is, and gives rise to a function on M. Sometimes, thinking of "a matrix with polynomial entries" will make our arguments simpler, and this example shows that the idea makes sense.

Note that SageMath does support matrices with polynomial entries.

```
sage: P = PolynomialRing(QQ, ['X', 'Y', 'Z'])
sage: X,Y,Z = P.gens()
sage: p1 = (-1)*X + (3/4)*Y - 8*Z
sage: p2 = X^2 - Y^2 + 3*Z
sage: p3 = Z
sage: m = vector(P, [p1,p2,p3])
sage: m
(-X + 3/4*Y - 8*Z, X^2 - Y^2 + 3*Z, Z)
sage: m.parent()
Ambient free module of rank 3 over the integral domain
Multivariate Polynomial Ring in X, Y, Z over Rational Field
sage: m.parent().basis()
[
(1, 0, 0),
(0, 1, 0),
(0, 0, 1)
]
sage: A = matrix.diagonal(P, [X,Y,Z])
sage: A
[X 0 0]
[0 Y 0]
[0 0 Z]
sage: A*m
(-X^2 + 3/4*X*Y - 8*X*Z, X^2*Y - Y^3 + 3*Y*Z, Z^2)
```

The one thing to be wary of here is that, in other contexts where the ring R can be non-commutative, it's possible to construct a polynomial-esque expression that is actually not a polynomial. For example, if R is non-commutative, then $XY \in R[X,Y]$ but not $YX \in R[X,Y]$, since in the latter case the coefficients (the stuff on the left) are supposed to come from $R[X]$ and you can't just switch them. To avoid these sorts of surprises, SageMath won't let you define a multivariate polynomial ring over a non-commutative base ring:

```
sage: R = MatrixSpace(QQ,2)
sage: R.is_ring()
True
sage: R.is_commutative()
False
sage: R_XY = PolynomialRing(R, ['X', 'Y'])
Traceback (most recent call last):
...
TypeError: The base ring Full MatrixSpace of 2 by 2 dense
matrices over Rational Field is not a commutative ring
```

Instead, it makes you define an equivalent structure, one level at a time, as a univariate polynomial ring whose coefficients come from another univariate polynomial ring, just like we did. This prevents you from doing something illegal as in the preceding example:

```
sage: R = MatrixSpace(QQ,2)
sage: R_X = PolynomialRing(R, 'X')
sage: R_XY = PolynomialRing(R_X, 'Y')
sage: R_XY
Univariate Polynomial Ring in Y over Univariate Polynomial
Ring in X over Full MatrixSpace of 2 by 2 dense matrices
over Rational Field
```

The way that *we* avoid these problems is by not allowing the ring R to be non-commutative. Too many things go wrong to make the generality worthwhile.

One final bit of polynomial notation is in order. We have just seen that we can sensibly construct matrices whose entries are polynomials in $\mathbb{P}^n(R)$. As a result, each entry of the matrix corresponds to a function from R^n to R as in Definition 24, and the matrix itself naturally corresponds to a function that takes an element of R^n and returns a matrix whose entries are in R.

Convention 10: Polynomial matrix function notation

If $A \coloneqq \left[A_{ij}\right] \in \left[\mathbb{P}^n\left(R\right)\right]^{\ell \times m}$ is a matrix whose entries are multivariate polynomials, then we write $A\restriction_{R^n}$ for the function

$$A\restriction_{R^n} : R^n \to R^{\ell \times n}$$
$$A\restriction_{R^n} = x \mapsto \left[A_{ij}\restriction_{R^n}\left(x\right)\right]$$

that takes x, feeds it to the functions that correspond to the polynomial entries of A, and then combines all of the results back into a matrix of the appropriate size.

One of our main results for univariate polynomials was that the ring of univariate polynomials is isorphic to an ring of polynomial functions. We'd like to say the same for multivariate polynomials, but in Theorem 7 it was crucial that the ring R be an integral domain. So if we want to apply Theorem 7 to $\mathbb{P}^n\left(R\right)$, for example, we will eventually need to know that its coefficient ring $\mathbb{P}^{n-1}\left(R\right)$ is an integral domain. Fortunately this is true, and we can simply cite the result.

Theorem 10. *If R is an integral domain, then so is $R\left[X\right]$.*

Beachy and Blair, Example 5.1.8

Corollary 4. *If R is an integral domain, then the multivariate polynomial rings $\mathbb{P}^n\left(R\right)$ are integral domains for any $n \geq 1$.*

Proof. Follows from repeated applications Theorem 10 to our recursive Definition 23 definition of $\mathbb{P}^n\left(R\right)$ as $\mathbb{P}^{n-1}\left(R\right)\left[X_n\right]$. □

These results can be combined with Lemma 1 to conclude that if R is an integral domain and if $f \in \mathbb{P}^n\left(R\right)$, then $f\restriction_R$ has only a finite number of roots. But be careful! The function $f\restriction_R$ only "evaluates" one indeterminate, and the same cannot be said of the function $f\restriction_{R^n}$. For example, if $f = XY - 1 \in \mathbb{R}\left[X, Y\right]$, then $f\restriction_{\mathbb{R}}$ has no roots, since there is no polynomial in X that we can substitute for Y to get the zero polynomial. The function $f\restriction_{\mathbb{R}^2}$ on the other hand has an infinite number of roots of the form $\left(x, \frac{1}{x}\right)$.

Theorem 11. *If R is an infinite integral domain, then the map $\phi = p \mapsto p\restriction_{R^n}$ is a ring isomorphism between $\mathbb{P}^n\left(R\right)$ and the ring of multivariate polynomial functions (the image of ϕ).*

Proof. This true for $n = 1$, as that's Theorem 7. We proceed by induction, assuming that it holds for any $k < n$.

If you care to check, Proposition 9 shows that ϕ is a ring homomorphism, so we need only show that it is injective. Suppose that $\phi(p) = \phi(q)$ so that

$$p\restriction_{R^n} = q\restriction_{R^n}$$
$$\iff$$
$$[p\restriction_R(x_n)]\restriction_{R^{n-1}}\left((x_1,\ldots,x_{n-1})^T\right) = [q\restriction_R(x_n)]\restriction_{R^{n-1}}\left((x_1,\ldots,x_{n-1})^T\right).$$

Our inductive hypothesis can be applied to conclude that

$$p\restriction_R(x_n) = q\restriction_R(x_n)$$

in $\mathbb{P}^{n-1}(R)$. But $\mathbb{P}^{n-1}(R)$ is an (infinite) integral domain by Corollary 4, so Theorem 7 can now be applied to conclude that $p = q$. □

The *isomorphism* result relies on the base ring being an infinite integral domain, but you should keep in mind that the map into the function space is always a *homomorphism* by Proposition 10. Using the polynomial/function isomorphism we can also finally demonstrate the relationship between homogeneous polynomials and homogeneous functions as in Definition 25.

Proposition 11. *Suppose R is an infinite integral domain and that $p \in \mathbb{P}^n(R)$ has the explicit form Equation (3.4). Then p is homogeneous of degree k if and only if $p\restriction_{R^n}$ is homogeneous of degree k.*

Proof. Suppose $p \in \mathbb{P}^n(R)$ is homogeneous of degree k. By simply evaluating,

$$\begin{aligned}
p\restriction_{R^n}(\alpha x) &= \sum_{i_1=0}^{d_1}\sum_{i_2=0}^{d_2}\cdots\sum_{i_n=0}^{d_n} a_{(i_1,i_2,\ldots,i_n)}(\alpha x_1)^{i_1}(\alpha x_2)^{i_2}\cdots(\alpha x_n)^{i_n} \\
&= \sum_{i_1=0}^{d_1}\sum_{i_2=0}^{d_2}\cdots\sum_{i_n=0}^{d_n} a_{(i_1,i_2,\ldots,i_n)}\alpha^{i_1}\alpha^{i_2}\cdots\alpha^{i_n}x_1^{i_1}x_2^{i_2}\cdots\alpha x_n^{i_n} \\
&= \alpha^{(i_1+i_2+\cdots i_n)}p\restriction_{R^n}(x) \\
&= \alpha^k p\restriction_{R^n}(x).
\end{aligned}$$

Conversely, suppose that $p\restriction_{R^n}(\alpha x) = \alpha^k p\restriction_{R^n}(x)$ for all $\alpha \in R$ and $x \in R^n$. Then for all $\alpha \in R$ and $x \in R^n$,

$$p\restriction_{R^n}(\alpha x) - \alpha^k p\restriction_{R^n}(x) = 0$$
$$\iff$$
$$\sum_{i_1=0}^{d_1}\sum_{i_2=0}^{d_2}\cdots\sum_{i_n=0}^{d_n} a_{(i_1,i_2,\ldots,i_n)}\left[\alpha^{(i_1+i_2+\cdots+i_n)} - \alpha^k\right]x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} = 0.$$

But these are simply the polynomial functions $q_\alpha\restriction_{R^n}$ corresponding to

$$q_\alpha \coloneqq \sum_{i_1=0}^{d_1}\sum_{i_2=0}^{d_2}\cdots\sum_{i_n=0}^{d_n} b_{(i_1,i_2,\ldots,i_n)}X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n},$$

where

$$b_{(i_1,i_2,\ldots,i_n)} \coloneqq a_{(i_1,i_2,\ldots,i_n)} \left[\alpha^{(i_1+i_2+\cdots+i_n)} - \alpha^k\right].$$

By Theorem 11, the functions $q_\alpha\restriction_{R^n}$ can be identically zero only if the coefficients of the q_α are all zero. Since R is an integral domain, we conclude that for all $i_1, i_2, \ldots, i_n$, we have $\alpha^{(i_1+i_2+\cdots+i_n)} - \alpha^k = 0$, from which it follows that $i_1 + i_2 + \cdots + i_n = k$, since otherwise in an infinite ring we would reach a contradiction. □

Another interesting fact that pops out of the explicit representation and function isomorphism is that we can interpret a polynomial as living in another ring where the indeterminates are rearranged when it is convenient. For a concrete example, suppose $p \in \mathbb{R}[X, Y, \Lambda]$ has the explicit representation from Equation (3.4),

$$p = \sum_{i_1=0}^{d_1} \sum_{i_2=0}^{d_2} \sum_{i_3=0}^{d_3} a_{(i_1,i_2,i_3)} X^{i_1} Y^{i_2} \Lambda^{i_3}$$

Rings like $\mathbb{R}[X, Y, \Lambda]$ will appear often, since we often start with a ring like $\mathbb{R}[X, Y]$ whose indeterminates represent coordinates in $\mathbb{R}^2$, and then later tack on another indeterminate to computing things like the minimal and characteristic polynomial based on those coordinates. However, the variable order X, Y, Λ is awkward for that purpose, since our definition of a polynomial function insists that we replace Λ first; you can't replace X or Y until you've replaced Λ, so if you want a function from $\mathbb{R}^2$ to $\mathbb{R}[\Lambda]$, you're out of luck.

To work around that problem, define a new polynomial $q \in \mathbb{R}[\Lambda, X, Y]$ with the explicit representation,

$$q \coloneqq \sum_{i_1=0}^{d_1} \sum_{i_2=0}^{d_2} \sum_{i_3=0}^{d_3} a_{(i_1,i_2,i_3)} \Lambda^{i_3} X^{i_1} Y^{i_2}$$

Technically $\mathbb{R}[X, Y, \Lambda]$ and $\mathbb{R}[\Lambda, X, Y]$ are the same ring but with the names of the basis elements swapped, but p and q will still generally be different polynomials. In other words, q is *not* what you'd get from renaming $X \to \Lambda$, $Y \to X$, and $\Lambda \to Y$ in the expression for p, because the exponents are wrong.

Now, it is easy to see that for all $(x, y, \lambda) \in \mathbb{R}^3$, we have $p\restriction_{\mathbb{R}^3}(x, y, \lambda) = q\restriction_{\mathbb{R}^3}(\lambda, x, y)$. Just substitute into the explicit representation, and look at the two results: they're the same expression. These two functions are in fact related to one another by an isomorphism in the function ring. If $f : \mathbb{R}^3 \to \mathbb{R}$ is a function, define $\tau(f) \coloneqq (\lambda, x, y) \mapsto f(x, y, \lambda)$. Check that τ is a homomorphism of the function ring:

$$\begin{aligned}
\tau(fg + h)(\lambda, x, y) &\coloneqq [fg + h](x, y, \lambda) \\
&= f(x, y, \lambda)\, g(x, y, \lambda) + h(x, y, \lambda) \\
&= \tau(f)(\lambda, x, y)\, \tau(g)(\lambda, x, y) + \tau(h)(\lambda, x, y).
\end{aligned}$$

The map τ is also bijective, making it an isomorphism. Finally, let ϕ denote the map that takes p to $p\restriction_{\mathbb{R}^3}$. Note that $\phi(q) = q\restriction_{\mathbb{R}^3}$ as well, since p and q technically live in the same polynomial ring. Now, we've just shown that

$$\phi^{-1}(\tau(\phi(p))) = q,$$

where both ϕ and τ are ring isomorphisms. As a result, the composition is a ring isomorphism sending p to q. Phew.

Now, suppose we want to define a function on $\mathbb{R}^2$ that takes $(x, y)^T$ and substitutes them into X and Y respectively in the expression for p. It's pretty clear that this can be done, but it's not at all obvious how you'd define such a function using only Definition 24. But now, we have a way. Let $\tilde{p} \coloneqq q\restriction_{\mathbb{R}^2} = \left[\phi^{-1}(\tau(\phi(p)))\right]\restriction_{\mathbb{R}^2}$, and let's see what happens:

$$\begin{aligned}
\tilde{p}(x, y) &\coloneqq q\restriction_{\mathbb{R}^2}(x, y) \\
&= \sum_{i_1=0}^{d_1}\sum_{i_2=0}^{d_2}\sum_{i_3=0}^{d_3} a_{(i_1,i_2,i_3)}\Lambda^{i_3}x^{i_1}y^{i_2} \\
&= \sum_{i_1=0}^{d_1}\sum_{i_2=0}^{d_2}\sum_{i_3=0}^{d_3} a_{(i_1,i_2,i_3)}x^{i_1}y^{i_2}\Lambda^{i_3}.
\end{aligned}$$

Refer back to the explicit representation of p. This is precisely what we were looking for. Moreover, the map $p \mapsto \tilde{p}$ is an isomorphism, because getting from p to q involved an isomorphism, and then getting from q to $q\restriction_{\mathbb{R}^2}$ involved another isomorphism—namely Theorem 11.

The isomorphism ϕ is inherent to the polynomial ring, and works for any p. Likewise, the only magic contained within τ is that it rearranges the arguments to the function it acts on in some particular way. By considering all of the various rearrangements given by the various maps τ, we can obtain functions to replace any subset of the indeterminates in p by real numbers in a formal way.

The details of this construction can promptly be forgotten. The main idea is summarized in the following theorem, to which we will refer when necessary.

Theorem 12. *If R is an infinite integral domain and if $p \in \mathbb{P}^n(R)$, then for any subset of indices $I \coloneqq \{k_1, k_2, \ldots, k_m\} \subseteq \{1, 2, \ldots, n\}$, there exists a function $p\restriction_{R^I} : R^m \to R^{n-m}$ such that $\tilde{p}(x_{k_1}, x_{k_2}, \ldots, x_{k_m})$ is the polynomial in R^{n-m} that you'd get by replacing each X_{k_j} with x_{k_j} in Equation (3.4). The mapping $p \mapsto p\restriction_{R^I}$ is an isomorphism between the polynomial ring and the ring of polynomial functions that $p\restriction_{R^I}$ lives in, and it extends to an additive and multiplicative function on polynomial matrices analogous to the result in Proposition 10.*

Proof. The same steps we followed in our example work for the general case. Given p, you can relabel the indeterminates and permute the exponents so that the indeterminates you want to substute for come last (and in order) and the resulting polynomial q has an associated function $q\restriction_{R^n}$ whose arguments are

similarly permuted. Call τ the isomorphism that permutes the arguments of $p\restriction_{R^n}$ to make it agree with $q\restriction_{R^n}$, and then construct an explicit isomorphism between p and q that can be used to define $p\restriction_I \coloneqq q\restriction_{R^m} : R^m \to R^{n-m}$.

The claim about matrices is proved exactly like the analogous clam in Proposition 10, which used only the fact that the polynomial-to-function map was a homomorphism. □

Convention 11: More polynomial notation

This is hopefully the last bit of polynomial notation we'll need. When $p \in \mathbb{P}^n(R)$, we now know that there are a number of polynomial functions associated with it. If $I = \{i_1, i_2, \ldots, i_k\}$ is a set of indices, we'll adopt the convention that $p\restriction_{R^I}$ is the function that takes k arguments and substitutes them for $X_{i_1}, X_{i_2}, \ldots, X_{i_k}$, in order.

For a typical example, let $p \in \mathbb{P}^n(\mathbb{R})[\Lambda]$, so that p has $n+1$ indeterminates $X_1, X_2, \ldots, X_n, \Lambda$. If we write $\bar{n}$ to denote the set $\{1, 2, \ldots, n\}$, then $p\restriction_{\mathbb{R}^{\bar{n}}}$ is the function that takes a vector in $\mathbb{R}^n$, substitutes its components into $X_1, X_2, \ldots, X_n$, and returns a polynomial in $\mathbb{R}[\Lambda]$.

This new ability to substitute for any number of indeterminates in any order is mirrored by SageMath.

```
sage: R = PolynomialRing(QQ, 'X,Y,Z')
sage: X,Y,Z = R.gens()
sage: p = X + 2*Y + 3*Z
sage: p(Y=7)
X + 3*Z + 14
sage: p(Y=7, Z=2)
X + 20
```

3.3 Polynomial ring embeddings

One final matter of notation deserves our attention. Suppose that R is a commutative ring, and that $R[X]$ is the ring of polynomials with coefficients in R.

For example, if $R = \mathbb{Z}$, then we would have $7 \in \mathbb{Z}$ and there would exist a "constant polynomial,"

$$p \coloneqq 7 \cdot 1_{\mathbb{Z}[X]} = (7, 0, 0, \ldots)^T$$

whose associated function on R is

$$p\restriction_{\mathbb{Z}} = x \mapsto 7.$$

In fact, the map that takes $7 \in \mathbb{Z}$ to $7 \cdot 1_{\mathbb{Z}[X]}$ is an injective, unit-preserving ring homomorphism called the canonical embedding.

Definition 26. If R is a commutative ring, then the function

$$\begin{aligned} \iota &: R \to R[X] \\ \iota &= x \mapsto x \cdot 1_R \end{aligned}$$

is the *canonical embedding* of R into $R[X]$.

In light of this, if R is a commutative ring, then the name of any element $x \in R$ will be used simultaneously to refer to either the ring element or the element $\iota(x) \in R[X]$, depending on the context. Following our previous example, the symbol "7" may mean either the integer $7 \in \mathbb{Z}$, or the constant polynomial $\iota(7) = 7 \cdot 1_{\mathbb{Z}[X]} \in \mathbb{Z}[X]$. Why settle for such imprecise notation? In this case, it's almost unavoidable. A few examples should make our case.

Beachy and Blair, Section 5.4

Example 16. In the usual set-theoretic construction, the rational numbers are constructed as ordered pairs of integers $(a, b) \in \mathbb{Z}^2$ modulo the equivalence relation $(a, b) \sim (c, d) \iff ad = bc$. Ignoring the details, it should be clear that the intergers are *not* a subset of the rational numbers under this construction. Nevertheless, we pretend that $\mathbb{Z} \subseteq \mathbb{Q}$, because there is a canonical embedding $x \mapsto \frac{x}{1} \coloneqq [(x, 1)]$ of the integers into the rational numbers. And we write the rational number "7" the same way we write the integer "7". These are non-polynomial rings, but this example should convince you that this type of notational hackery is nothing new.

Example 17. In Corollary 3, we factored a polynomial $q \in R[X]$ as

$$q = \left(X - a_1 X^0\right)\left(X - a_2 X^0\right) \cdots \left(X - a_k X^0\right).$$

Compared to

$$q = (X - a_1)(X - a_2) \cdots (X - a_k),$$

the former expression is rather clumsy. We will be factoring polynomials often, and it's nice to be able to read the roots of the corresponding functions off of the polynomials themselves. But the expression $X - a_i$ here does not make sense unless we take a_i to mean $\iota(a_i) = a_i \cdot 1_{R[X]}$ so that $X - a_i = X - a_i X^0$.

Example 18. Later on we claim that the polynomial $\det(\Lambda I - A) \in \mathbb{R}[\Lambda]$ is the characteristic polynomial of a matrix $A \in \mathbb{R}^{n\times n}$. If the matrix I here has real entries, then a priori the expression ΛI doesn't make sense. We need to treat the "1" entries in I as belonging to the ring $\mathbb{R}[\Lambda]$ for the scaling operation to make sense.

Afterwards, the expression $\Lambda I - A$ is still nonsense unless A contains polynomial entries. Since a priori its entries are real, we need to apply the canonical embedding to them so that the A within the determinant has entries in $\mathbb{R}[\Lambda]$.

Example 19. Our multivariate polynomial notation allows us to write things like $X_1 \in R[X_1, X_2, \ldots, X_n]$. But the symbol X_1 lives in $R[X_1]$, and saying that it belongs to the "larger" ring is, you guessed it, incorrect. The canonical embedding allows us to think of X_1 as living in $R[X_1, X_2]$, and so on, up to $R[X_1, X_2, \ldots, X_n]$ without resorting to oppressive notational gimmicks.

For the sake of clarity, we might have been willing to do everything explicitly, excepting this last example. The remainder of the text would be incomprehensible if we were not allowed to treat $R[X_1]$ as a subset of $R[X_1, X_2]$. And when we treat $\mathbb{P}^0(R) = R$ as a subset of $\mathbb{P}^1(R) = R[X_1]$, that's quite literally the same thing. So in many cases, we will need to use these canonical embeddings implicitly. But at that point, we might as well make full use of them, and apply them consistently whenever they might clean up the notation.

SageMath follows this convention, for the same reasons. Under the hood, the following example checks for a canonical embedding of the integers into the polynomial ring, and uses it to "coerce" the integer 3 into the polynomial ring where it becomes $3X^0$:

```
sage: R = PolynomialRing(ZZ,'X')
sage: X = R.gen()
sage: p = X^2 + X
sage: p + 3
X^2 + X + 3
```

The same is true for multivariate polynomials, where "smaller" polynomial rings can be coerced into "larger" ones, but not the other way around:

```
sage: R1 = PolynomialRing(ZZ,'X1')
sage: X1 = R1.gen()
sage: R2 = PolynomialRing(R1,'X2')
sage: X2 = R2.gen()
sage: X2 + X1 in R1
False
sage: X2 + X1 in R2
True
sage: R1.has_coerce_map_from(R2)
False
sage: R2.has_coerce_map_from(R1)
True
```

3.4 Rational functions

If you have spent any time at all studying mathematics, you will not be surprised to hear that "rational functions" are not functions. The space of rational functions is the most general type of polynomial space that we'll encounter. Rather than *actual* polynomials, the rational functions consist of polynomial *fractions*. That is, fractions of the form p/q where both p and q are themselves polynomials. But we have to be careful what we mean here.

Recall from Example 16 that the rational numbers $\mathbb{Q}$ can be constructed from pairs of integers under an appropriate equivalence relation. Instead of thinking of $a/b \in \mathbb{Q}$ as a single number, we think of a, b as being integers, and a/b as being the equivalense class $[(a,b)]$ under the equivalence relation $(a,b) \sim (c,d) \iff ab = cd$. We then declare the "integers" to be the subset $\{[(a,1)] \mid a \in \mathbb{Z}\}$. The corresponding embedding is a ring homomorphism. This construction generalizes to any integral domain—things that act like the integers—and not just to pairs of integers themselves.

Definition 27. If R is an integral domain, the *fraction field* of R is

Beachy and Blair, Definition 5.4.5

$$\operatorname{Frac}(R) \coloneqq \{[(a,b)] \mid a, b \in R\}$$

under the equivalence relation $(a,b) \sim (c,d) \iff ab = cd$. Each pair $(c,d) \in [(a,b)]$ is called a *representative* of the equivalence class $[(a,b)]$, and the equivalence class $[(a,b)]$ is usually denoted by a/b or $\frac{a}{b}$.

Addition in a fraction field is defined by

$$\frac{a}{b} + \frac{c}{d} \coloneqq \frac{ad + bc}{bd}$$

and multiplication is defined by

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) \coloneqq \frac{ac}{bd}.$$

The additive identity (zero) element of $\mathrm{Frac}(R)$ is $0_R/1_R$ and its unit is $1_R/1_R$, as can easily be checked from the definition:

$$\forall \left(\frac{a}{b}\right) \in \mathrm{Frac}(R) : \frac{a}{b} + \frac{0_R}{1_R} \coloneqq \frac{a \cdot 1_R + b \cdot 0_R}{b \cdot 1_R} = \frac{a}{b},$$
$$\forall \left(\frac{a}{b}\right) \in \mathrm{Frac}(R) : \left(\frac{a}{b}\right)\left(\frac{1_R}{1_R}\right) \coloneqq \frac{a \cdot 1_R}{b \cdot 1_R} = \frac{a}{b}.$$

Beware that superficially-similar name "quotient field" refers to something else entirely, which is why we have avoided Beachy and Blair's $Q(R)$ notation that is suggestive of the word "quotient." The fact that a fraction field is indeed a field requires some justification. It is also true that the original integral domain always embeds into its fraction field. We punt to the references for the proofs.

Beachy and Blair, Theorem 5.4.4

Theorem 13. *If R is an integral domain, then* $\mathrm{Frac}(R)$ *is a field, and the map $\iota = a \mapsto [(a, 1)]$ is a ring isomorphism between R and $\iota(R)$.*

It can in fact be shown that $\mathrm{Frac}(R)$ is the *smallest* field that contains a subring isomorphic to R. Though this is somewhat "obvious" considering that we started with R and constructed $\mathrm{Frac}(R)$ by adding in all of the things that would have to be there in a field. But how does this all apply to polynomials and rational functions? The field of (multivariate) rational functions is the fraction field of the (multivariate) polynomial ring over some integral domain R. We need to mention one important example.

Example 20. As we have just seen, the polynomial ring $R \coloneqq \mathbb{P}^n(\mathbb{R})$ is an integral domain. We can therefore form its field of rational functions $\mathbb{F} \coloneqq \mathrm{Frac}(R)$. Let ι denote the injective ring homomorphism $a \mapsto a/1_R$, from R into $\mathbb{F}$, from Theorem 13. Then, for example,

$$a/1 = 0_{\mathbb{F}} \iff \iota(a) = 0_R \iff \forall x \in \mathbb{R}^n : a\restriction_{\mathbb{R}^n}(x) = 0.$$

The last equivalence is due to the polynomial/function isomorphism Theorem 11.

Unfortunately, it's not always easy to turn a fraction into a function as in the previous example. We discuss a way out of the mess in Chapter B.

Warning 4: Rational functions aren't functions

Since we know how to turn two polynomials $p, q \in \mathbb{P}^n(R)$ into functions, you may be tempted to think of the formal quotient p/q as a function as well—namely the one that takes some $x \in R^n$ and produces $p\restriction_{R^n}(x) / q\restriction_{R^n}(x)$. But in general, that doesn't work,

because $q\restriction_{R^n}(x)$ could be zero.

3.5 Power-associative algebras

Next we want to investigate the relationship between polynomials and algebras. There's a special type of algebra where polynomials make sense, and this is what we'll be dealing with by and large. Recall from Theorem 7 that univariate polynomials over an infinite field are essentially the same as the polynomial functions on an associative unital algebra over that field. The same is true in slightly more generality; in particular we'll need to know it for Euclidean Jordan algebras, which are not associative, but rather *power-associative*.

Definition 28. If $(V, \circ)$ is a unital algebra and if $X \subseteq V$, then the *subalgebra of V generated by X* is written $\operatorname{alg}(X)$ and is defined to be the intersection of all subalgebras of V that contain $\{1_V\} \cup X$. Alizadeh, Definition 33

We insist that $\operatorname{alg}(X)$ contain the unit element of V so that it contains all powers in V (in particular, the power zero) of the elements of X. In general, a subalgebra of V might have a different unit element than V itself; with $\operatorname{alg}(X)$ we want the unit elements to be the same.

Another way to think of $\operatorname{alg}(X)$ is as the set of all elements of X, and all scalar multiples of elements of X, and all sums of those things, and then all products of those things, and then all sums of the products... and so on. Basically, you start with X and then you keep adding the things that have to be there to satisfy the definition of an algebra. This is similar to how $\operatorname{span}(X)$ is the smallest subspace containing X, but can also be thought of as "all linear combinations of things in X". With the span, this can be written out explicitly,

$$\operatorname{span}(X) = \left\{ \sum_{i=1}^{m} \alpha_i x_i \;\middle|\; m \in \mathbb{N}, \alpha_i \in \mathbb{R}, x_i \in X \right\}.$$

However, in an algebra, it's not so easy to write down exactly what that means because we don't know a priori that we only need to consider a finite number of products. For example, if $x_1, x_2 \in X$, then $x_1 \circ x_2$ needs to be in $\operatorname{alg}(X)$, but then $x_2 \circ (x_1 \circ x_2)$ needs to be there too, and $x_1 \circ (x_2 \circ (x_1 \circ x_2)) \ldots$. Those might all be different, and it's not clear when we can stop, which makes it hard to write down "all things of that form." That's why we use the abstract Definition 28 instead.

Definition 29. If $(V, \circ)$ is a unital algebra and if $\operatorname{alg}(\{x\})$ is associative for all $x \in V$, then $(V, \circ)$ is *power-associative*. In any power-associative algebra, we Alizadeh, Definition 34; Baes, Definition 2.2.11

define

$$\begin{aligned} x^0 &\coloneqq 1_V \\ x^1 &\coloneqq x \\ x^k &\coloneqq x \circ x^{k-1} = \underbrace{x \circ (x \circ (\cdots \circ (x \circ x)))}_{k-1 \text{ multiplications}}, \text{ for } k \geq 2 \end{aligned}$$

and the expression for x^k can be parenthesized in any order.

Convention 12: Power notation

We will only ever use the power notation x^k in a power-associative algebra where the meaning is unambiguous.

When $X = \{x\}$ is a singleton set in a finite-dimensional power-associative unital algebra, $\operatorname{alg}(X)$ has a particularly nice description.

Proposition 12. *If $(V, \circ)$ is a finite-dimensional power-associative unital algebra, if $x \in V$, and if $d \coloneqq \dim(\operatorname{alg}(\{x\}))$, then*

$$\operatorname{alg}(\{x\}) = \left\{ \sum_{i=0}^{d-1} \alpha_i x^i \;\middle|\; \alpha_i \in \mathbb{F} \right\} = \operatorname{span}\left(\left\{ x^i \;\middle|\; i \in \{0, 1, 2, \ldots, d-1\} \right\}\right).$$

Proof. To start, define a subspace of V,

$$W \coloneqq \operatorname{span}\left(\left\{ x^i \;\middle|\; i \in \mathbb{N} \right\}\right).$$

Since V is finite-dimensional and since $W \subseteq V$, we can let $d \coloneqq \dim(W)$ and know for sure that $d \in \mathbb{N}$ is finite.

Since $(V, \circ)$ is unital, we have $1_V \in \operatorname{alg}(\{x\})$ by Definition 28. Moreover every product of any number of x terms in any order is necessarily in $\operatorname{alg}(\{x\})$; and all sums and scalar multiples of those things have to be in $\operatorname{alg}(\{x\})$ too. Thus,

$$W \subseteq \operatorname{alg}(\{x\}).$$

On the other hand, restricting the algebra operations to W shows that W is a subalgebra of V. From the definition of span, the algebra $(W, \circ)$ is closed under addition and scalar multiplication. Using the fact that $\operatorname{alg}(\{x\})$ is associative, we also see that it is closed under algebra multiplication:

$$\left(\sum_{i=0}^{m_1} \alpha_i x^i\right) \circ \left(\sum_{j=0}^{m_2} \beta_j x^j\right) = \sum_{i=0}^{m_1} \sum_{j=0}^{m_2} \alpha_i \beta_j x^{i+j} \in W.$$

Now since $\text{alg}(\{x\})$ is supposed to be the smallest subalgebra of V containing both x and the unit element and since W is such a subalgebra, we have

$$\text{alg}(\{x\}) \subseteq W.$$

Therefore $\text{alg}(\{x\}) = W$, and it remains only to show that the first d powers of x span W; in other words that

$$W = \left\{ \sum_{i=0}^{d-1} \alpha_i x^i \;\middle|\; \alpha_i \in \mathbb{F} \right\}.$$

We'll use a dimension argument. Clearly,

$$\left\{ \sum_{i=0}^{d-1} \alpha_i x^i \;\middle|\; \alpha_i \in \mathbb{F} \right\} \subseteq W,$$

so for them to be unequal we must have

$$\dim\left(\left\{ \sum_{i=0}^{d-1} \alpha_i x^i \;\middle|\; \alpha_i \in \mathbb{F} \right\} \right) < \dim(W) = d.$$

Suppose that's true, so that without loss of generality, x^{d-1} can be written as a linear combination of the other powers. Then

$$\exists \alpha_0, \alpha_1, \ldots, \alpha_{d-2} \in \mathbb{R} : x^{d-1} = \sum_{i=0}^{d-2} \alpha_i x^i.$$

But then,

$$W = \text{span}\left(\left\{x^i \;\middle|\; 0 \leq i \leq d-2\right\}\right) + \text{span}\left(\left\{x^i \;\middle|\; i \geq d\right\}\right)$$

and now we claim that any element in the second span can be written as a linear combination of elements of the first. For if $k \geq d-1$, then $k = q(d-1) + r$ where $0 \leq r < d-1$ by the division algorithm for natural numbers, and

$$x^k = \underbrace{x^{d-1}x^{d-1}\cdots x^{d-1}}_{q \text{ times}} x^r.$$

Each term of degree $d-1$ in this product can be replaced by a sum of terms of degree less than $d-1$, since x^{d-1} was a linear combination of the lower-degree terms. After expanding, the process can be repeated, at each step replacing all terms of degree greater than $d-2$ by terms of strictly smaller degree. This process terminates when there are no terms of degree greater than $d-2$ left in the expression for x^k. At that point, we have shown that $x^k \in \text{span}\left(\left\{x^i \;\middle|\; 0 \leq i \leq n-2\right\}\right)$, meaning that the second direct summand in the formula for W above is contained in the first. In other words, that

$$W = \text{span}\left(\left\{x^i \;\middle|\; 0 \leq i \leq d-2\right\}\right).$$

This would contradict the fact that $\dim(W) = n$, so when we supposed that x^{d-1} was a linear combination of the lower powers, that was impossible. $\square$

Corollary 5. *If $(V, \circ)$ is a finite-dimensional power-associative unital algebra, if $x \in V$, and if $d \coloneqq \dim(\operatorname{alg}(\{x\}))$, then*

$$\left\{x^0, x^1, x^2, \ldots, x^d\right\}$$

is a basis for $\operatorname{alg}(\{x\})$.

The main reason we care about power-associative algebras is because they're the most general type of algebra that we know how to evaluate a polynomial on. The power-associativity is critical in the following definition to ensure that $\operatorname{alg}(\{x\})$ is associative for all x. Otherwise, the meaning of $p\restriction_{\operatorname{alg}(\{x\})}$ would be unclear.

Definition 30. If $p \in R[X]$ and if $(M, R, \circ)$ is a power-associative and unital algebra over R, then we define an associated *polynomial function on M* by

$$\begin{aligned} p\restriction_M &: M \to M \\ p\restriction_M &= x \mapsto p\restriction_{\operatorname{alg}(\{x\})}(x)\,. \end{aligned}$$

Since M is associative, $\operatorname{alg}(\{x\})$ is associative. We interpret the result as living in M even though a priori the codomain of $p\restriction_{\operatorname{alg}(\{x\})}$ is $\operatorname{alg}(\{x\})$.

Corollary 6. *If $(V, \mathbb{F}, \circ)$ is a nontrivial, power-associative, and unital algebra over an infinite field $\mathbb{F}$ and if $p\restriction_V = q\restriction_V$ as functions on V, then $p = q$ in $\mathbb{F}[X]$. As a result, the map $p \mapsto p\restriction_V$ is a ring isomorpism.*

Proof. Since V is nontrivial, there exists a nonzero $x \in V$, and $\operatorname{alg}(\{x\})$ is therefore a nontrivial, associative, unital subalgebra over $\mathbb{F}$. By definition,

$$\begin{gathered} p\restriction_V = q\restriction_V \\ \iff \\ \forall z \in V : p\restriction_{\operatorname{alg}(\{z\})}(z) = p\restriction_{\operatorname{alg}(\{z\})}(z)\,. \end{gathered}$$

In particular, this holds for all $z \in \operatorname{alg}(\{x\})$, where we have $\operatorname{alg}(\{z\}) = \operatorname{alg}(\{x\})$. If we denote $\operatorname{alg}(\{x\})$ by W, then

$$\begin{gathered} p\restriction_V = q\restriction_V \\ \implies \\ \forall z \in W : p\restriction_W(z) = p\restriction_W(z)\,, \end{gathered}$$

where again, we reiterate that W is a nontrivial associative unital algebra. Since these two functions are equal on W, Theorem 7 shows that $p = q$ in $\mathbb{F}[X]$. □

3.6 Polynomial continuity

Everyone knows that multivariate polynomial functions are continuous, right? It's not so easy to formalize that, but it's a crucial fact that we can't in good

conscience omit. Specifically, we want to show that the functions in Definition 24 are continuous, but to do so, we have to give up on using a general ring R. For continuity, we'll need convergent sequences and series, and to fall back on existing results it's just easier to work in the familiar setting of the real numbers.

Recall Example 5, where we saw the space $\ell_2(\mathbb{R})$ consisting of all square-summable infinite sequences of real numbers. The way that we defined a univariate polynomial with real coefficients was as a subset,

$$\mathbb{R}[X_1] \coloneqq \left\{ (a_0, a_1, \ldots)^T \in \mathbb{R}^\infty \;\middle|\; a_i \neq 0 \text{ for only finitely many } i \right\} \subseteq \mathbb{R}^\infty.$$

In hindsight, the fact that the elements of $\mathbb{R}[X_1]$ have only a finite number of non-zero coordinates means that $\mathbb{R}[X_1]$ is actually a subset of $\ell_2(\mathbb{R})$, which is of course a subset of $\mathbb{R}^\infty$. This means that $\mathbb{R}[X_1]$ inherits a norm from the $\ell_2(\mathbb{R})$, namely

$$\left\| a_0 + a_1 X_1^1 + \cdots + a_d X_1^d \right\|_{\mathbb{P}^1(\mathbb{R})} \coloneqq \left(\sum_{i=0}^{d} a_i^2 \right)^{\frac{1}{2}}.$$

Now for a multivariate polynomial, we can define a norm recursively. The trick is to realize that, with multivariate polynomials, we're dealing with a Cartesian product space. In two variables, for example,

$$\mathbb{R}[X_1, X_2] \coloneqq \left\{ (a_0, a_1, \ldots)^T \in (\mathbb{R}[X_1])^\infty \;\middle|\; a_i \neq 0 \text{ for only finitely many } i \right\}$$

which is a subspace of the Cartesian product $(\ell_2(\mathbb{R}))^\infty \subseteq (\mathbb{R}[X_1])^\infty$. Cartesian product spaces have a natural norm inherited from their constituent spaces via the Pythagorean theorem. Basically, we just define

$$\left\| a_0 + a_1 X_2^1 + \cdots + a_d X_2^d \right\|_{\mathbb{R}[X_1, X_2]} \coloneqq \left(\sum_{i=0}^{d} \|a_i\|_{\mathbb{R}[X_1]}^2 \right)^{\frac{1}{2}}.$$

and since there are only a finite number of non-zero a_i, this sum is guaranteed to exist. And we can continue this process indefinitely (well, to a finite extent), since it works at every subsequent step.

Definition 31. The norm on $\mathbb{P}^n(\mathbb{R})$ is defined recursively by

$$\left\| a_0 + a_1 X_n^1 + \cdots + a_d X_n^d \right\|_{\mathbb{P}^n(\mathbb{R})} \coloneqq \left(\sum_{i=0}^{d} \|a_i\|_{\mathbb{P}^{n-1}(\mathbb{R})}^2 \right)^{\frac{1}{2}}$$

where the base case in $\mathbb{P}^0(\mathbb{R}) = \mathbb{R}$ simply uses the absolute value.

Contradicting Simplification 2, we have secretly introduced a scaling operation for polynomials here. To reuse some machinery, we began thinking of $R[X_1]$ as a subset of $\ell_2(\mathbb{R})$, which of course has a natural scaling operation (by real numbers) defined on it. We must also allow this scaling operation to

exist in the background for our polynomials, since any polynomial norm must support "pulling out" a scalar in absolute value. Nevertheless, we will still treat polynomial rings as rings for algebraic purposes.

And now that we have a norm on polynomial spaces, we can talk about continuity there. The first, most basic thing we might try to prove is that addition and multiplication of polynomials are continuous operations. Since $\mathbb{P}^n(\mathbb{R})$ is a ring structure on top of a Hilbert space, you might be tempted to apply Proposition 5; however, the space $\mathbb{P}^n(\mathbb{R})$ is *not* finite-dimensional, even though each individual element has a finite number of non-zero coordinates.

Lemma 2 (polynomial ring operation continuity)**.** *If $p, q \in \mathbb{P}^n(\mathbb{R})$, then the maps $(p, q) \mapsto pq$ and $(p, q) \mapsto p + q$ are continuous.*

Proof. Suppose that

$$p = a_0 + a_1 X_n^1 + \cdots a_{d_1} X_n^{d_1},$$
$$q = b_0 + b_1 X_n^1 + \cdots a_{d_2} X_n^{d_2}.$$

Then, the polynomial multiplication formula gives

$$pq = \sum_{i=0}^{d_1} \sum_{j=0}^{d_2} a_i b_j X_n^{i+j}.$$

We claim that polynomial multiplication is bounded; that is, that

$$\forall p, q \in \mathbb{P}^n(\mathbb{R}) : \|pq\|_{\mathbb{P}^n(\mathbb{R})} \leq \|p\|_{\mathbb{P}^n(\mathbb{R})} \|q\|_{\mathbb{P}^n(\mathbb{R})}.$$

This is true when $n = 1$, since

$$\begin{aligned}
\|pq\|_{\mathbb{P}^1(\mathbb{R})}^2 &= \sum_{i=0}^{d_1} \sum_{j=0}^{d_2} \|a_i b_j\|_{\mathbb{R}}^2 \\
&\leq \sum_{i=0}^{d_1} \sum_{j=0}^{d_2} a_i^2 b_j^2 \\
&= \sum_{i=0}^{d_1} a_i^2 \sum_{j=0}^{d_2} b_j^2 \\
&= \sum_{i=0}^{d_1} a_i^2 \|q\|_{\mathbb{P}^1(\mathbb{R})}^2 \\
&= \|q\|_{\mathbb{P}^1(\mathbb{R})}^2 \|p\|_{\mathbb{P}^1(\mathbb{R})}^2.
\end{aligned}$$

And if we assume that it works for $n-1$, then

$$\begin{aligned}
\|pq\|^2_{\mathbb{P}^n(\mathbb{R})} &= \sum_{i=0}^{d_1}\sum_{j=0}^{d_2} \|a_i b_j\|^2_{\mathbb{P}^n(\mathbb{R})} \\
&\leq \sum_{i=0}^{d_1}\sum_{j=0}^{d_2} \|a_i\|^2_{\mathbb{P}^n(\mathbb{R})} \|b_j\|^2_{\mathbb{P}^n(\mathbb{R})} \\
&= \sum_{i=0}^{d_1} \|a_i\|^2_{\mathbb{P}^n(\mathbb{R})} \left(\sum_{j=0}^{d_2} \|b_j\|^2_{\mathbb{P}^n(\mathbb{R})} \right) \\
&= \|q\|_{\mathbb{P}^n(\mathbb{R})} \|p\|_{\mathbb{P}^n(\mathbb{R})} .
\end{aligned}$$

Thus it's true in general by induction. And boundedness implies continuity. If $(p,q)_m$ is a sequence converging to (p,q), then $p_m \to p$ and $q_m \to q$. Then thanks to boundedness, we have

$$\begin{aligned}
\|pq - p_m q_m\|_{\mathbb{P}^n(\mathbb{R})} &= \|pq - p_m q + p_m q - p_m q_m\|_{\mathbb{P}^n(\mathbb{R})} \\
&= \|(p-p_m)\, q + p_m\,(q-q_m)\|_{\mathbb{P}^n(\mathbb{R})} \\
&\leq \|(p-p_m)\, q\|_{\mathbb{P}^n(\mathbb{R})} + \|p_m\,(q-q_m)\|_{\mathbb{P}^n(\mathbb{R})} \\
&\leq \|p-p_m\|_{\mathbb{P}^n(\mathbb{R})} \|q\|_{\mathbb{P}^n(\mathbb{R})} + \|p_m\|_{\mathbb{P}^n(\mathbb{R})} \|q-q_m\|_{\mathbb{P}^n(\mathbb{R})} .
\end{aligned}$$

Since Theorem 6 shows that convergent sequences are bounded, both terms here go to zero. The fact that addition is continuous follows from Proposition 2, given that $\mathbb{P}^n(\mathbb{R})$ is a normed vector space. □

The continuity of polynomial operations will be often be used implicitly. The next thing we'll need to know is that *univariate* polynomial evaluation is continuous. This will be the "base case" in our proof for multivariate polynomial functions, but we prove it as a separate result because we know how to evaluate univariate polynomials in a more general setting now.

Proposition 13 (univariate polynomial function continuity)**.** *If* $p = a_0 + a_1 X^1 + \cdots + a_d X^d \in \mathbb{R}[X]$ *and if* $(V, \mathbb{R}, \circ)$ *is a finite-dimensional, normed, unital, power-associative algebra, then* $p\restriction_V$ *is continuous.*

Proof. Suppose that $x_m \to x$ in V. Then by the triangle inequality,

$$\begin{aligned}
\|p\restriction_V(x) - p\restriction_V(x_m)\| &= \left\|a_0 1_V + a_1 (x - x_m) + \cdots + a_d \left(x^d - x_m^d\right)\right\| \\
&\leq \sum_{i=0}^{d} |a_0| \left\|x^i - x_m^i\right\|
\end{aligned}$$

which goes to zero by the continuity of the field operations. □

Finally, we use this result to show that the function $p\restriction_{\mathbb{R}^n}$ is continuous. We needed a norm on the polynomial spaces for this to make sense.

Proposition 14. *If $p \in \mathbb{P}^n(\mathbb{R})$, then the function $p\restriction_{\mathbb{R}^n} : \mathbb{R}^n \to R$ in Definition 24 is continuous.*

Proof. Suppose that $\delta \in \mathbb{R}^n$, and notice that as $\delta \to 0$, the explicit representation of $p\restriction_{\mathbb{R}^n}$ from Proposition 9 gives us (after suppressing some of the indices for notational convenience),

$$p\restriction_{\mathbb{R}^n}(x+\delta) - p\restriction_{\mathbb{R}^n}(x)$$
$$=$$
$$\sum_{i_1=0}^{d_1} \cdots \sum_{i_n=0}^{d_n} a_{(i_1,i_2,\ldots,i_n)} (x_1+\delta_1)^{i_1} \cdots (x_n+\delta_n)^{i_n}$$
$$-$$
$$\sum_{i_1=0}^{d_1} \cdots \sum_{i_n=0}^{d_n} a_{(i_1,i_2,\ldots,i_n)} x_1^{i_1} \cdots x_n^{i_n}.$$

If you put the $\mathbb{R}$ norm (absolute value) around this expression and apply the triangle inequality, you wind up with,

$$|p\restriction_{\mathbb{R}^n}(x+\delta) - p\restriction_{\mathbb{R}^n}(x)|$$
$$\leq$$
$$\sum \left|a_{(i_1,i_2,\ldots,i_n)}\right| \underbrace{\left|\left[(x_1+\delta_1)^{i_1} \cdots (x_k+\delta_k)^{i_k}\right] - \left[x_1^{i_1} \cdots x_k^{i_k}\right]\right|}_{\to 0},$$

Since part of each term is constant, and the other part involving δ is going to zero by Lemma 2, the whole thing is going to zero. □

Finally, we'll need to know that convergence as polynomials implies convergence as functions.

Proposition 15. *If $p^{(\ell)}$ is a sequence in $\mathbb{P}^n(\mathbb{R})$ converging to p, then $p^{(\ell)}\restriction_{\mathbb{R}^n} \to p\restriction_{\mathbb{R}^n}$ pointwise on $\mathbb{R}$.*

Proof. First note that this is obvious for $n = 1$, the case that we all learned in kindergarten. This lets us restrict our attention to $n > 1$, and to assume that it holds for $1 \leq k < n$.

Next suppose that each element $p^{(\ell)}$ in the sequence has the form,

$$p^{(\ell)} = a_0^{(\ell)} X_n^0 + a_1^{(\ell)} X_n^1 + \cdots + a_d^{(\ell)} X_n^d,$$

and that p itself is

$$p = a_0 X_n^0 + a_1 X_n^1 + \cdots + a_d X_n^d.$$

Definition 31 implies that

$$\lim_{\ell\to\infty} p^{(\ell)} = p \iff \forall i \in \{0,1,2,\ldots,d\} : \lim_{\ell\to\infty} \left\|a_i^{(\ell)} - a_i\right\|_{\mathbb{P}^{n-1}(\mathbb{R})} = 0.$$

Use Definition 24 to expand $p^{(\ell)}\restriction_{\mathbb{R}^n}(x)$

$$\begin{aligned} p^{(\ell)}\restriction_{\mathbb{R}^n}(x) &= \left[p^{(\ell)}\restriction_R(x_n)\right]\restriction_{R^{n-1}}\left((x_1,\ldots,x_{n-1})^T\right) \\ &= \left[\sum_{i=0}^{d} a_i^{(\ell)} x_n^i\right]\restriction_{\mathbb{R}^{n-1}}\left((x_1,x_2,\ldots,x_{n-1})^T\right) \\ &= \sum_{i=0}^{d} a_i^{(\ell)}\restriction_{\mathbb{R}^{n-1}}\left((x_1,x_2,\ldots,x_{n-1})^T\right) x_n^i, \end{aligned}$$

and likewise for

$$p\restriction_{\mathbb{R}^n}(x) = \sum_{i=0}^{d} a_i\restriction_{\mathbb{R}^{n-1}}\left((x_1,x_2,\ldots,x_{n-1})^T\right) x_n^i.$$

Let $\hat{x} \coloneqq (x_1,x_2,\ldots,x_{n-1})^T$ to clean up the notation a bit; then subtract, take absolute value, and apply the triangle inequality:

$$\left|p^{(\ell)}\restriction_{\mathbb{R}^n}(x) - p\restriction_{\mathbb{R}^n}(x)\right| \leq \sum_{i=0}^{d}\left|a_i^{(\ell)}\restriction_{\mathbb{R}^{n-1}}(\hat{x}) - a_i\restriction_{\mathbb{R}^{n-1}}(\hat{x})\right|\left|x_n^i\right|.$$

We showed above that $a_i^{(\ell)} \to a_i$ in $\mathbb{P}^{n-1}(\mathbb{R})$, the induction hypothesis therefore shows that this entire sum goes to zero. □

3.7 Solutions to exercises

Solution to Exercise 3 (polynomial multiplication). Beginning with the expression,

$$pq = \left(\sum_{i=0}^{I} a_i X^i\right)\left(\sum_{j=0}^{J} b_j X^j\right),$$

we can begin to impose some of the properties that we would like this multiplication to have. For multiplication to be distributive, we must be able to expand,

$$pq = \sum_{i=0}^{I}\sum_{j=0}^{J} a_i X^i b_j X^j.$$

Then if we're going to have commutativity and $X^iX^j = X^{i+j}$, we should be able to regroup, so we define

$$pq \coloneqq \sum_{i=0}^{I}\sum_{j=0}^{J}(a_ib_j)\,X^{i+j}. \tag{3.1}$$

This answer is already correct. It's commutative, because the products $a_i b_j$ in the coefficients commute, as do the sums $i+j$ and the sums of module elements that arise from the two big sigmas; so the expression won't change if you switch p and q. And it's distributive because we defined it to be: if

$$r = \sum_{k=0}^{K} c_k X^k \in R\left[X\right],$$

and if we write $M \coloneqq \max\left(\left\{J, K\right\}\right)$, then

$$\begin{aligned} p\left(q+r\right) &= \left(\sum_{i=0}^{I} a_i X^i\right) \left(\sum_{j=0}^{M} \left(b_j + c_j\right) X^j\right) \\ &\coloneqq \sum_{i=0}^{I} \sum_{j=0}^{M} \left[a_i \left(b_j + c_j\right)\right] X^{i+j}. \end{aligned}$$

In this expression, we have used the same index name j to index both q and r simultaneously. To that end, we have combined their upper limit into $M \coloneqq \max\left(\left\{J, K\right\}\right)$. This does not change anything: J, for example, was the largest index such that b_j was nonzero. That means that all b_j for $j > J$ are zero, and it doesn't hurt if we include "extra" terms $0 = b_j X^j$ when j is between J and M for notational convenience. Likewise for $k > K$, if it so happens that $K > J$.

Using the distributivity of the coefficients in R and the laws of module addition and scalar multiplication, this simplifies to

$$\begin{aligned} &\sum_{i=0}^{I} \sum_{j=0}^{M} \left[\left(a_i b_j\right) X^{i+j} + \left(a_i c_j\right) X^{i+j}\right] \\ &= \left[\sum_{i=0}^{I} \sum_{j=0}^{M} \left(a_i b_j\right) X^{i+j}\right] + \left[\sum_{i=0}^{I} \sum_{k=0}^{M} \left(a_i c_k\right) X^{i+k}\right] \\ &= \left(pq\right) + \left(pr\right). \end{aligned}$$

Finally, it is associative, as the same module/ring laws show:

$$\begin{aligned}
(pq)\,r &= \left[\sum_{i=0}^{I}\sum_{j=0}^{J}(a_ib_j)\,X^{i+j}\right]\left[\sum_{k=0}^{K}c_kX^k\right] \\
&= \sum_{i=0}^{I}\sum_{j=0}^{J}\sum_{k=0}^{K}\left[(a_ib_j)\,c_k\right]X^{i+j+k} \\
&= \sum_{i=0}^{I}\sum_{j=0}^{J}\sum_{k=0}^{K}\left[a_iX^i\right]\left[(b_jc_k)\,X^{j+k}\right] \\
&= \left[\sum_{i=0}^{I}a_iX^i\right]\left[\sum_{j=0}^{J}\sum_{k=0}^{K}(b_jc_k)\,X^{j+k}\right] \\
&= p\,(qr)\,.
\end{aligned}$$

However, this naive definition of polynomial multiplication is not the most computationally-convenient. The product pq is itself a tuple of infinite length, and Equation (3.1) doesn't help us find a particular entry (the coefficient of a given power) in that tuple very easily. To do so, we have to loop over two large-ish sets of indices, many of which are redundant. To address that, let's try to turn Equation (3.1) into a single sum. First, simply let $\ell = i + j$, and rewrite the formula,

$$pq = \sum\left\{(a_ib_j)\,X^\ell \;\middle|\; i,j \in \{0,1,\ldots,\max\left(\{I,J\}\right)\},\, i+j=\ell\right\}.$$

With this new expression for pq, it's easier to read off what the ℓ^{th} entry of pq is; by definition, it's the coefficient of X^ℓ:

$$(pq)_\ell = \sum\left\{(a_ib_j) \mid i,j \in \{0,1,\ldots,\max\left(\{I,J\}\right)\},\, i+j=\ell\right\}.$$

Notice that we won't be considering any i or j greater than ℓ, since both are nonnegative and we must have $i + j = \ell$. As a result, this can be simplified to

$$(pq)_\ell = \sum\left\{a_ib_j \mid i,j \in \{0,1,\ldots,\ell\},\, i+j=\ell\right\}.$$

Leave i alone in this expression, but solve for j in terms of i and ℓ to get $j = \ell - i$. Since ℓ is fixed, i ranges from 0 to ℓ, and j is uniquely determined by those, we can simply replace j by $\ell - i$ without any loss of fidelity:

$$(pq)_\ell = \sum\left\{a_ib_{\ell-i} \mid i \in \{0,1,\ldots,\ell\}\right\} = \sum_{i=0}^{\ell}a_ib_{\ell-i}. \tag{3.2}$$

This new expression contains only one summation, and tells us what the ℓ^{th} coordinate of pq is. Let's check Equation (3.2) using SageMath for two quadratic polynomials p and q:

```
sage: a0,a1,a2 = SR.var('a0,a1,a2')
sage: b0,b1,b2 = SR.var('b0,b1,b2')
sage: a = [a0,a1,a2,0,0]
sage: b = [b0,b1,b2,0,0]
sage: p = a[0] + a[1]*x + a[2]*x^2
sage: q = b[0] + b[1]*x + b[2]*x^2
sage: expected = (p*q).expand()
sage: expected
a2*b2*x^4 + a2*b1*x^3 + a1*b2*x^3 + a2*b0*x^2 + a1*b1*x^2 +
a0*b2*x^2 + a1*b0*x + a0*b1*x + a0*b0
sage: def coeff(l):
....:     return sum( a[i]*b[l - i] for i in range(l+1) )
sage: [ bool(coeff(l) == expected.coefficient(x,l))
....:   for l in range(5) ]
[True, True, True, True, True]
```

Do we need to show that this new formula is commutative, associative, and distributive? It can be done directly, but we have already shown that Equations (3.1) and (3.2) are equivalent definitions, and the first one satisfies all of the properties we need.

Chapter 4

Linear Algebra

4.1 Linear operators, matrix representation

Every vector space has a basis, and all bases for a given vector space have the same cardinality (these are not easy things to prove). A vector space is said to be *finite-dimensional* if some/every basis for that vector space is finite. The cardinality of the basis is referred to as the dimension of the vector space. All of our vector spaces will be finite-dimensional: this makes things a lot easier.

Definition 32. If $(V, \mathbb{F})$ and $(W, \mathbb{F})$ are vector spaces and if $L : V \to W$ is a function, then we say that L is a *linear operator* from V to W if

$$\forall x, y \in V, \forall \alpha \in \mathbb{F} : L(\alpha x + y) = \alpha L(x) + L(y).$$

The set of all linear operators from V to W is denoted by $\mathcal{B}(V, W)$.

Exercise 2. *Show that $\mathcal{B}(V, W)$ is a vector space over $\mathbb{F}$ if V and W are.*

There is a straightforward connection between linear operators and matrices: a matrix is simply a representation of a linear operator with respect to a particular basis. For example, suppose V has a basis $\{e_1, e_2, \ldots, e_n\}$ and that $x \in V$. Then we can write $x = x_1 e_1 + x_2 e_2 \cdots + x_n e_n$ in terms of that basis. Now suppose $L \in \mathcal{B}(V)$. Then in particular, $L(e_1)$, and $L(e_2)$, and so on, are back in V and we can write them in terms of our basis:

$$\begin{aligned} L(e_1) &= \ell_{11} e_1 + \ell_{21} e_2 + \cdots + \ell_{n1} e_n \\ L(e_2) &= \ell_{12} e_1 + \ell_{22} e_2 + \cdots + \ell_{n2} e_n \\ &\vdots \\ L(e_n) &= \ell_{1n} e_1 + \ell_{2n} e_2 + \cdots + \ell_{nn} e_n. \end{aligned}$$

It turns out that knowing the scalars $\{\ell_{ij} \mid 1 \leq i, j \leq n\}$ is completely equivalent to knowing L itself. Since any $x \in V$ can be written as $x = x_1 e_1 + x_2 e_2 \cdots + x_n e_n$, we have

$$L(x) = x_1 L(e_1) + x_2 L(e_2) + \cdots x_n L(e_n),$$

and of course knowing the ℓ_{ij} tells us what L does to each e_j. Matrices arise from the following realization: if knowing the scalars $x_1, x_2, \ldots, x_n$ is equivalent to knowing x, and if knowing the ℓ_{ij} is equivalent to knowing L, then why don't we just arrange those scalars in a way that lets us compute with them? Matrix multiplication is defined how it is precisely so that

$$\begin{bmatrix} \ell_{11} & \ell_{12} & \cdots & \ell_{1n} \\ \ell_{21} & \ddots & & \ell_{2n} \\ \vdots & & \ddots & \vdots \\ \ell_{n1} & \ell_{n2} & \cdots & \ell_{nn}. \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \text{ the coordinate representation of } L(x).$$

SageMath is happy to let you define a linear transformation in terms of its action on a basis, and it can tell you the resulting matrix:

```
sage: V = VectorSpace(QQ,3)
sage: e1,e2,e3 = V.basis()
sage: L_of_e1 = -e1 + 2*e2 + e3
sage: L_of_e2 = e1 + e2 - e3
sage: L_of_e3 = e2
sage: images = [L_of_e1, L_of_e2, L_of_e3]
sage: L = linear_transformation(V,V,images)
sage: L
Vector space morphism represented by the matrix:
[-1  2  1]
[ 1  1 -1]
[ 0  1  0]
Domain: Vector space of dimension 3 over Rational Field
Codomain: Vector space of dimension 3 over Rational Field
```

Definition 33. If V is a finite-dimensional vector space over the field $\mathbb{F}$ with basis $\mathbf{b}$, then the coordinate vector of $x \in V$ with respect to $\mathbf{b}$ will be written $\mathbf{b}(x) \in \mathbb{F}^{n\times 1}$, and the coordinate matrix of $L \in \mathcal{B}(V)$ will be written similarly, as $\mathbf{b}(L) \in \mathbb{F}^{n\times n}$. We use function notation for this operation to emphasize that it acts very much like a homomorphism; matrix multiplication is defined precisely so that $\mathbf{b}(L(x)) = \mathbf{b}(L)\,\mathbf{b}(x)$.

Proposition 16. *If V is a vector space and if $\mathbf{b} = \{b_1, b_2, \ldots, b_n\}$ is a basis for V, then the (block) matrix representation of $L \in \mathcal{B}(V)$ with respect to $\mathbf{b}$ is,*

$$\mathbf{b}(L) \coloneqq \begin{bmatrix} | & | & & | \\ \mathbf{b}(L(b_1)) & \mathbf{b}(L(b_2)) & \cdots & \mathbf{b}(L(b_n)) \\ | & | & & | \end{bmatrix}.$$

Proof. Recall that $\mathbf{b}(L)$ should be the matrix satisfying $\mathbf{b}(L)\mathbf{b}(x) = \mathbf{b}(L(x))$ for all $x \in V$. If $x \in V$ is arbitrary with $\mathbf{b}$-coordinates $\mathbf{b}(x) = (x_1, x_2, \ldots, x_n)^T$, then $x = x_1 b_1 + x_2 b_2 + \cdots x_n b_n$, and using the linearity of L,

$$\mathbf{b}(L(x)) = \mathbf{b}(x_1 L(b_1) + x_2 L(b_2) + \cdots + x_n L(b_n)).$$

Now using the linearity of $\mathbf{b}()$, this is just

$$x_1 \mathbf{b}(L(b_1)) + x_2 \mathbf{b}(L(b_2)) + \cdots + x_2 \mathbf{b}(L(b_n)),$$

which, by the definition of (block) matrix multiplication, is

$$\begin{bmatrix} | & | & & | \\ \mathbf{b}(L(b_1)) & \mathbf{b}(L(b_2)) & \cdots & \mathbf{b}(L(b_n)) \\ | & | & & | \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \qquad \square$$

Exercise 4 (matrix of transpose operator). Let $V = \mathbb{R}^{2\times 2}$ be the vector space of 2-by-2 matrices with real entries over the scalar field $\mathbb{R}$. We can define a function L on V by

$$\begin{aligned} L &: V \to V \\ L &= A \mapsto A^T, \end{aligned}$$

so that L is the "transpose operator."

First show that L is linear, so that $L \in \mathcal{B}(V)$. Then choose a basis for the vector space $V = \mathbb{R}^{2\times 2}$, and find the matrix of L with respect to your basis.

It's possible to have more than one basis in play at the same time, which is when things really get confusing. (And God forbid if your vector space is $\mathbb{R}^n$ so that the matrix of a linear operator with respect to the standard basis looks exactly like itself). We'll do one example of a "change of basis" for linear operators, since it's so useful.

Example 21 (change of basis)**.** Suppose you have two bases $\mathbf{e} = \{e_1, e_2, \ldots, e_n\}$ and $\mathbf{b} = \{b_1, b_2, \ldots, b_n\}$ for a vector space V, and that $L \in \mathcal{B}(V)$ is some linear operator. How are $\mathbf{e}(L)$ and $\mathbf{b}(L)$ related? Can you compute one easily from the other? From Proposition 16, we can say immediately that

$$\mathbf{e}(L) = \begin{bmatrix} | & | & & | \\ \mathbf{e}(L(e_1)) & \mathbf{e}(L(e_2)) & \cdots & \mathbf{e}(L(e_n)) \\ | & | & & | \end{bmatrix}, \text{ and}$$

$$\mathbf{b}(L) = \begin{bmatrix} | & | & & | \\ \mathbf{b}(L(b_1)) & \mathbf{b}(L(b_2)) & \cdots & \mathbf{b}(L(b_n)) \\ | & | & & | \end{bmatrix}.$$

Theorem 2.2 of Roman says that we can completely specify a linear operator by its action on a basis, so let $A \in \mathcal{B}(V)$ be the map that sends e_i to b_i. We can then substitute $b_i = A(b_i)$ in the second equation to get

$$\begin{bmatrix} | & | & & | \\ \mathbf{b}(LA(e_1)) & \mathbf{b}(LA(e_2)) & \cdots & \mathbf{b}(LA(e_n)) \\ | & | & & | \end{bmatrix}.$$

Note now that A is invertible, and that A^{-1} sends b_i to e_i. Thus for any $x = x_1 b_1 + x_2 b_2 + \cdots x_n b_n \in V$, we have $A^{-1}(x) = x_1 e_1 + x_2 e_2 + \cdots x_n e_n$. It follows that $\mathbf{e}\left(A^{-1}(x)\right) = \mathbf{b}(x)$ for all x in V. By taking $x = LA(e_i)$ for $i = 1, 2, \ldots, n$ in the expression above and substituting $\mathbf{e}\left(A^{-1}(x)\right)$ for $\mathbf{b}(x)$, we finally arrive at

$$\begin{aligned} \mathbf{b}(L) &= \begin{bmatrix} | & | & & | \\ \mathbf{e}\left(A^{-1}LA(e_1)\right) & \mathbf{e}\left(A^{-1}LA(e_2)\right) & \cdots & \mathbf{e}\left(A^{-1}LA(e_n)\right) \\ | & | & & | \end{bmatrix} \\ &= \mathbf{e}\left(A^{-1}LA\right). \end{aligned}$$

Now by the "homomorphism" property of basis representation,

$$\mathbf{b}(L) = \mathbf{e}\left(A^{-1}LA\right) \iff \mathbf{b}(L) = \mathbf{e}\left(A^{-1}\right)\mathbf{e}(L)\,\mathbf{e}(A),$$

showing that we can obtain $\mathbf{b}(L)$ from $\mathbf{e}(L)$ by conjugating it.

For the most part, people choose a standard orthonormal basis, and the space of matrices is isometric to (essentially the same as) the space of linear operators. Thus, nobody really distinguishes them. Matrices are easy to compute with, but choosing a coordinate system (that is, a basis) is a bit arbitrary and can obscure what's going on.

Proposition 17. *If V and W are two finite-dimensional vector spaces, then $\mathcal{B}(V, W)$ is also finite-dimensional and has dimension* $\dim(V)\dim(W)$.

Axler, Proposition 3.20

Proof. Let $\{a_1, a_2, \ldots, a_m\}$ be a basis for V and $\{b_1, b_2, \ldots, b_n\}$ be a basis for W. Define the following family of linear operators, where the x_k denote scalars:

$$L_{ij} \coloneqq \left(\sum_{k=1}^{m} x_k a_k\right) \mapsto x_i b_j.$$

It is fairly easy to see using linearity that any element of $\mathcal{B}(V, W)$ can be written as a linear combination of these L_{ij}. Likewise, it is easy to show that the set $\{L_{ij} \mid i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n\}$ is linearly-independent. As a result, that set is a basis for the vector space $\mathcal{B}(V, W)$, and it contains $m \cdot n = \dim(V)\dim(W)$ elements. □

Corollary 7. *If V is finite-dimensional, then* $\dim(\mathcal{B}(V)) = \dim(V)^2$.

4.2 Eigenvalues and self-adjoint operators

Probably the most important concept that we're going to study with regards to linear operators is that of eigenvalues/eigenvectors. Here we recall some familiar facts from basic linear algebra. They will become extremely important later when we're studying Euclidean Jordan algebras: the one trick in our bag will be to convert Jordan-algebraic problems into standard linear algebra problems, and to analyze those instead.

Definition 34. If $(V, \mathbb{F})$ is a vector space and if $L \in \mathcal{B}(V)$, then we say that $\lambda \in \mathbb{F}$ is an *eigenvalue* of L if there exists a nonzero $x \in V$ such that $L(x) = \lambda x$. In that case, x is called an *eigenvector* of L corresponding to λ.

Eigenvalues are important because they make it easy to understand what a linear operator does. If L sends x to λx, then by linearity, we know how L acts on all of $\operatorname{span}(\{x\})$. Thus it suffices to understand how L acts on things perpendicular to x. And if $y \perp x$, and if y is also an eigenvector... then we can repeat the process, breaking down L into a bunch of simple scaling operations (on the eigenvectors) plus whatever's left over (which is usually more complicated, but not as bad as when we started).

When can we decompose a linear operator L completely in terms of its eigenvalues/eigenvectors? This question has a nice answer. Recall that if $A \in \mathbb{R}^{n\times n}$ is a matrix, then the function $\lambda \mapsto \det(\lambda I - A)$ is a real polynomial function of degree n on $\mathbb{R}$. Now is a good time to define that function.

Definition 35. Suppose R is a commutative ring and that $A \in R^{n\times n}$ is a matrix with entries $A_{i,j} \in R$. If S_n is the permutation group on $\{1, 2, \ldots, n\}$ and if $\operatorname{par}(\rho)$ denotes the parity of the permutation ρ, then

Axler 10.25; Roman, Corollary 14.20

$$\begin{aligned} &\det : R^{n\times n} \to R \\ &\det \coloneqq A \mapsto \sum_{\rho\in S_n} \operatorname{par}(\rho)\, A_{p(1),1} A_{p(2),2} \cdots A_{p(n),n}. \end{aligned}$$

is the *determinant* of the matrix A.

The function $\lambda \mapsto \det(\lambda I - A)$ first constructs a matrix $\lambda I - A$ whose entries are all of the form $\delta_{ij}\lambda - A_{ij}$ where $\delta_{ij} \in \{0, 1\}$. And the parity of a permutation is either 1 or -1. Thus $\det(\lambda I - A)$, which consists of products and sums of those entries and the parities, consists of just more products and sums involving real numbers and λ. As a result, the entire expression is a big product/sum of terms involving only real numbers and λ; that is, a polynomial in λ. A 3-by-3 example should get the idea across. Here we have used the letter X instead of λ for unrelated technical reasons.

```
sage: a11,a12,a13 = SR.var('a11,a12,a13')
sage: a21,a22,a23 = SR.var('a21,a22,a23')
sage: a31,a32,a33 = SR.var('a31,a32,a33')
sage: A = matrix(SR, [ [a11,a12,a13],
....:                  [a21,a22,a23],
....:                  [a31,a32,a33] ])
sage: X = SR.var('X')
sage: I = matrix.identity(SR,3)
sage: (X*I - A).determinant().expand()
X^3 - X^2*a11 - X*a12*a21 - X^2*a22 + X*a11*a22 -
X*a13*a31 + a13*a22*a31 - a12*a23*a31 - a13*a21*a32 -
X*a23*a32 + a11*a23*a32 - X^2*a33 + X*a11*a33 +
a12*a21*a33 + X*a22*a33 - a11*a22*a33
```

Since $\lambda \mapsto \det(\lambda I - A)$ is a real polynomial function, it is safe to say by Theorem 7 that it is the unique real polynomial function associated with some $\det(\Lambda I - A) \in \mathbb{R}[\Lambda]$, where here the determinant operation is interpreted formally as a series of multiplications and sums of polynomial objects (specifically, one like the expression in the SageMath example above). We will adopt this more-convenient formalism from now on.

There is a slightly more useful formula for the determinant that doesn't require us to compute the signs of a bunch of permutations.

Definition 36 (cofactors)**.** Suppose that R is a commutative ring, and that $R^{n\times n}$ and $R^{(n-1)\times(n-1)}$ are two matrix spaces with respective standard bases $E = \{E_{ij} \mid i,j \in \{1,2,\ldots,n\}\}$ and $F = \{F_{ij} \mid i,j \in \{1,2,\ldots,n-1\}\}$. Then since we're in a free module (see Chapter 5 of Roman) we can define a linear transformation $M_{\ell k} : R^{n\times n} \to R^{(n-1)\times(n-1)}$ by its action on E,

$$M_{\ell k}(E_{ij}) \coloneqq \begin{cases} 0 & \text{if } i = \ell \text{ or } j = k \\ F_{ij} & \text{otherwise} \end{cases}.$$

When acting on matrices, the transformation $M_{\ell k}$ has the effect of "deleting" the ℓ^{th} row and k^{th} column. We can now define the $(\ell,k)^{th}$ *cofactor* of $A \in R^{n\times n}$,

$$\begin{aligned} &\text{cofactor}(\ell,k,\cdot) : R^{n\times n} \to R \\ &\text{cofactor}(\ell,k,A) = (-1)^{\ell+k} \det(M_{\ell k}(A)). \end{aligned}$$

Essentially, $\text{cofactor}(\ell,k,A)$ is just (plus or minus) the determinant of the matrix you would get if you deleted the ℓ^{th} row and k^{th} column of A.

Theorem 14 (Laplace cofactor expansion)**.** *If R is a commutative ring, if*

$A \in R^{n\times n}$ is a matrix with entries A_{ij}, and if we fix $i \in \{1, 2, \ldots, n\}$, then

$$\det(A) = \sum_{j=1}^{n} A_{ij} \operatorname{cofactor}(i, j, A).$$

Likewise, if we fix $j \in \{1, 2 \ldots, n\}$, then

$$\det(A) = \sum_{i=1}^{n} A_{ij} \operatorname{cofactor}(i, j, A).$$

The cofactor expansion allows us to define the determinant recursively. We know what the determinant of a 1-by-1 matrix should be, and then the determinant of a 2-by-2 matrix is defined in terms of that. So on for bigger matrices.

Example 22. Consider the real symmetric matrix

$$A \coloneqq \begin{bmatrix} 1 & 2 & 3 \\ 2 & 0 & 4 \\ 3 & 4 & 5 \end{bmatrix} \in \mathcal{S}^3.$$

The minimal polynomial of A is $\Lambda^3 - 6\Lambda^2 - 24\Lambda - 12 \in \mathbb{R}[\Lambda]$ from which we can deduce that $\det(A) = 12$. Let's fix $i = 3$, and use its cofactor expansion:

$$\begin{gathered} A_{31} \cdot \operatorname{cofactor}(3, 1, A) + A_{32} \cdot \operatorname{cofactor}(3, 2, A) + A_{33} \cdot \operatorname{cofactor}(3, 3, A) \\ = \\ 3(-1)^4 \det\left(\begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}\right) + 4(-1)^5 \det\left(\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\right) + 5(-1)^6 \det\left(\begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\right) \\ = \\ 3 \cdot 8 + 4 \cdot 2 + 5 \cdot (-4) = 12. \end{gathered}$$

Here we have implicitly used the fact that

$$\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc,$$

which of course follows itself from another cofactor expansion.

The cofactor expansion also makes it easy to see that the determinant of A comes from some multivariate polynomial evaluated on the entries of A. It's trivially true for 1-by-1 matrices, and if it holds for $(n-1)$-by-$(n-1)$ matrices, then the cofactor expansion is a sum/product of polynomials in the entries of A. So, it's true by induction on n.

Ok, why do we care? The determinant can be used to solve systems of linear equations.

Theorem 15 (Cramer's rule)**.** *If R is a ring, if $b \in R^n$, and if $A \in R^{n\times n}$ with $\det(A) \neq 0$, then the system $Ax = b$ has a unique solution for $x \in R^n$ given by*

$$x = (x_1, x_2, \ldots, x_n)^T \text{ with } x_i = \frac{\det(A_{i\to b})}{\det(A)},$$

where $A_{i\to b}$ denotes the matrix A but with its i^{th} column replaced by b.

Proof. Define a function $L_A : R^n \to R^n$ by

$$L_A\left(\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}\right) \coloneqq \frac{1}{\det(A)} \begin{bmatrix} \det(A_{1\to x}) \\ \det(A_{2\to x}) \\ \vdots \\ \det(A_{n\to x}) \end{bmatrix}$$

The determinant function is linear in the columns (and rows, see Corollary 14.20 in Roman) of its argument, so for a fixed A, the function L_A is linear in its argument x. Now see what happens if we apply L_A to each column A_i of A itself. The entries of $L_A(A_i)$ look like

$$L_A(A_i)_k = \frac{\det(A_{k\to A_i})}{\det(A)} = \begin{cases} \frac{\det(A)}{\det(A)} = 1 & \text{if } k = i \\ 0 & \text{otherwise} \end{cases},$$

since adding a second copy of A_i in a non-i position makes the matrix singular. Thus we conclude that

$$L_A(A_i) = e_i,$$

the i^{th} standard basis vector. However, the inverse of A acts the same way, as can be seen if we write both A^{-1} and A itself in block form,

$$\begin{aligned} A^{-1}A &= \begin{bmatrix} A^{-1} \end{bmatrix} \begin{bmatrix} A_1 & A_2 & \cdots & A_n \end{bmatrix} \\ &= \begin{bmatrix} A^{-1}A_1 & A^{-1}A_2 & \cdots & A^{-1}A_n \end{bmatrix} \\ &= I \\ &= \begin{bmatrix} e_1 & e_2 & \cdots & e_n \end{bmatrix}. \end{aligned}$$

Since the columns of A form a basis for R^n (it's a free module, see Chapter 5 of Roman), and since L_A and A^{-1} agree on that basis, they must be the same linear transformation. Now we simply substitute L_A for A^{-1} in

$$x = A^{-1}b \iff x = L_A(b),$$

and look at the i^{th} component:

$$x_i = (L_A(b))_i = \frac{\det(A_{i\to b})}{\det(A)}.$$ □

Another reason to care about the determinant is that $\det(\Lambda I - A) \in \mathbb{R}[\Lambda]$ is a polynomial, and the roots of the function $[\det(\Lambda I - A)]\restriction_{\mathbb{R}}$ are the eigenvalues of A, since that expression comes directly from the eigenvalue equation $Ax = \lambda x$. Therefore, by the fundamental theorem of algebra, if $\mathbb{F}$ is the complex numbers, we can find n complex roots/eigenvalues, some of which may be repeated. However, we want to know what happens in *real* vector spaces. First let's recall the adjoint of a linear operator.

Definition 37. If $(V, \langle\cdot,\cdot\rangle_V)$ and $(W, \langle\cdot,\cdot\rangle_W)$ are two finite-dimensional real inner-product spaces and if $L \in \mathcal{B}(V, W)$, then there exists a unique $L^* \in \mathcal{B}(W, V)$ called the *adjoint* of L such that

$$\forall x \in V, \forall y \in W : \langle L(x), y\rangle_W = \langle x, L^*(y)\rangle_V .$$

If $L \in \mathcal{B}(V)$ and if $L^* = L$, then L is called *self-adjoint*. Note that the idea of self-adjoint doesn't make sense unless $W = V$ above.

The existence of an adjoint in finite-dimensional spaces is discussed in Axler's Chapter 6, or in Roman's Theorem 10.1. The general case (more general even than what we claim here) is covered in the uncharacteristically-readable Theorem 4.10 in *Functional Analysis*, by Walter Rudin [14].

In an inner product space, the "isomorphisms" are isometries—linear maps that preserve the inner product.

Definition 38. If $(V, \langle\cdot,\cdot\rangle_V)$ and $(W, \langle\cdot,\cdot\rangle_W)$ are two finite-dimensional real inner-product spaces and if $L \in \mathcal{B}(V, W)$ satisfies

Axler, Chapter 7

$$\forall x \in V : \|x\|_V = \|L(x)\|_W ,$$

then L is an *isometry* between V and W.

Theorem 16. *If $(V, \langle\cdot,\cdot\rangle_V)$ and $(W, \langle\cdot,\cdot\rangle_W)$ are two finite-dimensional real inner-product spaces and if $L \in \mathcal{B}(V, W)$, then L is an isometry if and only if $\forall x, y \in V : \langle x, y\rangle_V = \langle L(x), L(y)\rangle_W$.*

Axler, 7.36; Roman, 9.6

Thus isometries preserve not only norms, but also inner products. Since the theorem above is an equivalence, it doesn't really matter which one you choose as your definition: Chapter 9 of Roman defines isometries as preserving inner products. Literally, though, "isometry" means "same distance," so we side with Axler on this one.

Exercise 5 (isometry between finite-dimensional spaces). Suppose that V and W are two real, n-dimensional Hilbert spaces. Each therefore has a basis consisting of n elements. Prove Theorem 1: show that V and W are *isometric* by demonstrating an isometry between them.

Hint: take both bases, and cite some linear algebra result that says that you can orthonormalize them. Prove (or cite someone again to show) that you can define a linear operator on a vector space by specifying its action on a basis. Finally, define your isometry by deciding what it should do on an orthonormal basis for V, and prove that it preserves inner-products and/or norms.

If A is a real matrix that represents L with respect to some orthonormal basis, then its transpose A^T represents L^* with respect to the same basis. If A is complex, then its conjugate-transpose A^* (sometimes written A^H) represents L^* instead.

Proposition 18. *If $(V, \mathbb{F}, \langle\cdot,\cdot\rangle)$ is a finite-dimensional inner-product space with orthonormal basis $\mathbf{b}$, then $L \in \mathcal{B}(V)$ is self-adjoint if and only if the matrix of L with respect to $\mathbf{b}$ is Hermitian.*

Proof. Since $\mathbf{b}$ is orthonormal, then the basis representation map $b_i \mapsto e_i$ from V to $\mathbb{F}^n$ (where n is the dimension of V) is an isometry: $\mathbf{b}(b_i) = e_i$, and both b_i and e_i have unit norm. This holds for the entire orthonormal basis $\mathbf{b}$, and thus for all of V: any $v \in V$ can be written as a linear combination $\sum_{i=1}^n \alpha_i b_i$ of the elements of $\mathbf{b}$; then using $\|x\|^2 \coloneqq \langle x, x\rangle$ and the orthonormality of both bases, we have

$$\|v\|_V^2 = \left\|\sum_{i=1}^n \alpha_i b_i\right\|_V^2 = \sum_{i=1}^n \sum_{j=1}^n \alpha_i \alpha_j \langle b_i, b_j\rangle_V = \sum_{i=1}^n \alpha_i^2 \|b_i\|_V^2 = \sum_{i=1}^n \alpha_i^2$$

$$\|\mathbf{b}(v)\|_{\mathbb{F}^n}^2 = \left\|\mathbf{b}\left(\sum_{i=1}^n \alpha_i b_i\right)\right\|_{\mathbb{F}^n}^2 = \sum_{i=1}^n \sum_{j=1}^n \alpha_i \alpha_j \langle e_i, e_j\rangle_{\mathbb{F}^n} = \sum_{i=1}^n \alpha_i \|e_i\|_{\mathbb{F}^n}^2 = \sum_{i=1}^n \alpha_i^2.$$

Thus $\mathbf{b}$ is an isometry when considered as a linear operator from V to $\mathbb{F}^n$. And since $\mathbf{b}$ is an isometry, it is in particular an invertible linear operator. Keep that in mind for a second, because...

$$\begin{gathered}
\forall y, z \in V : \langle L(y), z\rangle_V = \langle y, L(z)\rangle_V \\
\iff \\
\forall y, z \in V : \langle \mathbf{b}(L(y)), \mathbf{b}(z)\rangle_{\mathbb{F}^n} = \langle \mathbf{b}(y), \mathbf{b}(L(z))\rangle_{\mathbb{F}^n} \\
\iff \\
\forall y, z \in V : \langle \mathbf{b}(L)\,\mathbf{b}(y), \mathbf{b}(z)\rangle_{\mathbb{F}^n} = \langle \mathbf{b}(y), \mathbf{b}(L)\,\mathbf{b}(z)\rangle_{\mathbb{F}^n}.
\end{gathered}$$

Here we can use the invertibility of $\mathbf{b}$, to create the correspondences

$$\begin{aligned}
p = \mathbf{b}(y) &\iff \mathbf{b}^{-1}(p) = y \\
q = \mathbf{b}(z) &\iff \mathbf{b}^{-1}(q) = z,
\end{aligned}$$

and use them to change where the "for all" takes place. The result is,

$$\begin{gathered}
\dots \\
\iff \\
\forall p, q \in \mathbb{F}^n : \langle \mathbf{b}(L)\,p, q\rangle_{\mathbb{F}^n} = \langle p, \mathbf{b}(L)\,q\rangle_{\mathbb{F}^n}.
\end{gathered}$$

This chain of equivalences starts with the self-adjointness of L, and end with its matrix $\mathbf{b}(L)$ being Hermitian. So, those two things are equivalent. □

Example 23. In $\mathbb{R}^{n\times 1}$, the inner product $\langle x, y\rangle$ can be written as simply $y^T x$. Thus $\langle Ax, y\rangle = y^T Ax$, and if A is self-adjoint, then

$$y^T Ax = \langle Ax, y\rangle = \langle x, Ay\rangle = \langle Ay, x\rangle = x^T Ay.$$

Theorem 17. *If $(V, \mathbb{C})$ is an inner-product space and if $L \in \mathcal{B}(V)$ is self-adjoint, then all of the eigenvalues of L are real.* *Axler, Proposition 7.1*

Proof. Suppose that $x \in V$ is an eigenvector of L with $L(x) = \lambda x$. We want to show that $\overline{\lambda} = \lambda$, from which we conclude that $\lambda \in \mathbb{R}$:

$$\lambda \|x\|^2 = \langle \lambda x, x \rangle = \langle L(x), x \rangle = \langle x, L(x) \rangle = \langle x, \lambda x \rangle = \overline{\lambda} \|x\|^2 .$$

Since $x \neq 0$ because it was an eigenvector, we can divide both sides by $\|x\|^2 > 0$ to conclude that $\overline{\lambda} = \lambda$. □

How do we apply the previous theorem to real vector spaces?

Proposition 19. *If $A \in \mathbb{R}^{n \times n}$ is symmetric, then the real polynomial function $\lambda \mapsto \det(\lambda I - A)$ has n real roots.*

Roman, Theorem, 10.11

Proof. Consider the matrix $\widetilde{A} \in \mathbb{C}^{n \times n}$ having the same entries as A. In that setting, $\widetilde{A}$ is Hermitian, because the conjugate-transpose of a matrix with real entries is the regular transpose, and A was symmetric. Thus, the eigenvalues of $\widetilde{A}$ are real by Theorem 17, and we conclude that the polynomial function $\lambda \mapsto \det\left(\lambda I - \widetilde{A}\right)$ has n real roots. Now we simply note that

$$\forall \lambda \in \mathbb{R} : \det\left(\lambda I - \widetilde{A}\right) = \det(\lambda I - A),$$

from which the conclusion follows. □

We won't call this next theorem "the fundamental theorem of linear algebra," but only because that name is already taken. This is *the* practical reason why symmetry of matrices is so important.

Theorem 18 (spectral theorem for linear algebra)**.** *If $(V, \mathbb{R})$ is a real inner-product space of dimension n and if $L \in \mathcal{B}(V)$, then the following are equivalent:*

Axler, Chapter 7; or Roman, Theorem 10.19

- *L is self-adjoint.*
- *V has an orthonormal basis consisting of eigenvectors of L.*
- *There exists some orthogonal matrix U that diagonalizes the matrix A of L; that is, such that $UAU^T = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ where (without loss of generality) the λ_i are the eigenvalues of L.*
- *There exists a unique set of pairs $\{(\lambda_1, P_1), (\lambda_2, P_2), \ldots, (\lambda_k, P_k)\}$ consisting of real numbers $\lambda_i \in \mathbb{R}$ and operators $P_i \in \mathcal{B}(V)$ such that*
  - *The real numbers λ_1 through λ_k are all non-zero and distinct; likewise, the operators P_1 through P_k are all non-zero and distinct.*
  - *$P_i^2 = P_i$ and $P_i^* = P_i$. In other words, each P_i is a* projection.
  - *P_i is the projection onto the eigenspace $\ker(\lambda_i \operatorname{id}_V - L)$ of L corresponding to the non-zero eigenvalue λ_i.*
  - *$\sum_{i=1}^k P_i = \operatorname{id}_V$ and thus $\sum_{i=1}^k \lambda_i P_i = L$.*
  - *$P_i P_j = 0$ for $i \neq j$ (the projections are onto orthogonal subspaces).*

The last item involving the projections doesn't appear in the cited theorems, but can be deduced afterwards from Axler's Proposition 5.21.

Warning 5: Zeros invalidate uniqueness

It's hard to find the unique decomposition written down anywhere correctly. The fact that there *exist* spectral projectors and eigenvalues is fairly easy to deduce, but the uniqueness is not. The caveat is that the zero operator satisfies the definition of a projection, and the zero eigenvalue is also a legitimate eigenvalue. You can add in extra zero projectors to any decomposition to make it non-unique without affecting the answer. And if $\lambda = 0$ is an eigenvalue of your operator, then you can pair it with any projection P in $\lambda P = 0$ to make the decomposition non-unique. Thus we have restricted our statement to nonzero projectors and eigenvalues.

The spectral theorem is *incredibly useful* because the mapping $X \mapsto UXU^T$ is an isometry on the space of matrices. Thus if we can write $A = UDU^T$ for a diagonal matrix D, then we know precisely how A is isometric to a diagonal matrix. And diagonal matrices are *easy* to reason about.

Example 24. [inverse of a symmetric matrix] Suppose that $A \in \mathbb{R}^{n\times n}$ is symmetric. Using the spectral theorem for linear algebra, we can write

$$A = U^T \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)\, U.$$

If any of the λ_i are zero, then A is not invertible. On the other hand, if all of the λ_i are nonzero, then the inverse of A is

$$A^{-1} = U^T \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)\, U^{-1} = U^T \operatorname{diag}\left(\frac{1}{\lambda_1}, \frac{1}{\lambda_2}, \ldots, \frac{1}{\lambda_n}\right) U,$$

as can easily be verified by matrix multiplication using the fact that $UU^T = U^TU = I$.

Example 25 (spectral norm of a symmetric matrix)**.** The *operator norm* or *spectral norm* of a matrix $A \in \mathbb{R}^{n\times n}$ is the maximum amount that it can stretch a vector,

$$\|A\| \coloneqq \sup\left(\left\{\frac{\|Ax\|}{\|x\|} \;\middle|\; x \in \mathbb{R}^n, x \neq 0\right\}\right) = \max\left(\{\|Ay\| \mid y \in \mathbb{R}^n, \|y\| = 1\}\right).$$

The second equality is obtained by letting $y = x/\|x\|$. The set of all $y \in \mathbb{R}^n$ with $\|y\| = 1$ is closed and bounded, and is therefore compact in $\mathbb{R}^n$ by Theorem 3.

As a result, the continuous function $y \mapsto \|Ay\|$ achieves its supremum on said set by Theorem 4.

But what is this norm? If A is symmetric, then we write $A = U^T DU$ where $D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ by the spectral theorem for linear algebra. Then

$$\|A\| = \max\left(\left\{\left\|U^T DUy\right\| \;\middle|\; y \in \mathbb{R}^n, \|y\| = 1\right\}\right),$$

and since U and U^T are invertible isometries, we can let $Uy = z$ and substitute,

$$\begin{aligned}\|A\| &= \max\left(\left\{\left\|U^T Dz\right\| \;\middle|\; z \in \mathbb{R}^n, \|z\| = 1\right\}\right) \\ &= \max\left(\{\|Dz\| \mid z \in \mathbb{R}^n, \|z\| = 1\}\right).\end{aligned}$$

Intuitively, the way to maximize this is to put a "1" in the component of z that corresponds to the largest entry of D. Without loss of generality, suppose that $D_{11} = \lambda_1$ is the largest entry in absolute value. Then it easy to see that

$$\|A\| = \|De_1\| = |\lambda_1|.$$

Thus the spectral/operator norm of A is its largest eigenvalue, in absolute value:

$$\|A\| = \max\left(\{|\lambda_1|, |\lambda_2|, \ldots, |\lambda_n|\}\right).$$

The maximum eigenvalue of *any* matrix A is called its spectral radius and is written $\rho(A)$. Thus in the special case of a symmetric matrix, the operator norm is the same as the spectral radius.

Example 26 (condition number of a symmetric matrix)**.** In numerical computations, solving the system $Ax = b$ in $\mathbb{R}^n$ using floating-point arithmetic will produce an innacurate solution. The *condition number* $\kappa(A)$ of the matrix $A \in \mathbb{R}^{n\times n}$ provides an upper bound on the error associated with that solution. In terms of the operator norm,

$$\kappa(A) = \frac{\|A\|}{\|A^{-1}\|}.$$

Therefore, if A is symmetric, then by Example 25 we can simply compute

$$\kappa(A) = \frac{|\lambda_{\max}|}{|\lambda_{\min}|},$$

where $\lambda_{\max}$ and $\lambda_{\min}$ are the largest/smallest eigenvalues of A, in absolute value, respectively.

Example 27. [exponential of a symmetrix matrix] The matrix exponential of $A \in \mathbb{R}^{n\times n}$ is defined to be

$$\exp(A) \coloneqq \sum_{k=0}^{\infty} \frac{1}{k!} A^k,$$

and this always converges thanks to the factorial in the denominator. Ok, but how do we compute it? If A is symmetric, we write $A = U^T DU$ where $D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ as usual. Then

$$\exp(A) = \sum_{k=0}^{\infty} \frac{1}{k!} \underbrace{U^T DUU^T DUU^T DU \cdots}_{k \text{ times}},$$

and using the fact that $UU^T = I$, we arrive at

$$\begin{aligned}
\exp(A) &= \sum_{k=0}^{\infty} \frac{1}{k!} U^T D^k U \\
&= U^T \left(\sum_{k=0}^{\infty} \frac{1}{k!} D^k \right) U \\
&= U^T \operatorname{diag}\left(e^{\lambda_1}, e^{\lambda_2}, \ldots, e^{\lambda_n}\right) U.
\end{aligned}$$

Exercise 6 (eigenvalues of powers). Let $A \in \mathbb{R}^{n \times n}$ be symmetric with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{R}$. Use the spectral decomposition of A to show that the eigenvalues of A^k are $\lambda_1^k, \lambda_2^k, \ldots, \lambda_n^k$.

Exercise 7 (eigenspaces of transpose operator). Let $V = \mathbb{R}^{2 \times 2}$ and recall the "transpose operator" L from Exercise 4 that takes a matrix $A \in V$ and returns A^T. In this problem, we will want to talk about orthogonality in V, and that requires an inner product. The inner product of two matrices B and C is usually defined to be

$$\langle B, C \rangle \coloneqq \operatorname{trace}\left(BC^T\right), \tag{4.2}$$

and we will use that as our inner product on V. Thus when we talk about matrices $B, C \in V$ being orthogonal, we mean that

$$\langle B, C \rangle \coloneqq \operatorname{trace}\left(BC^T\right) = 0.$$

First, find all eigenvalues of L, using either your solution to Exercise 4 or the fact that $L(L(A)) = \left(A^T\right)^T = A$. For each eigenvalue $\lambda_i \in \mathbb{R}$ that you find, there should be a corresponding eigenspace $V_i \subseteq V$ such that

$$\forall x \in V_i : L(x) = \lambda_i x.$$

Find these eigenspaces and their dimensions, and show that V is an orthogonal direct sum of them,

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k,$$

where the elements of V_i and V_j are orthogonal when $i \neq j$.

4.3 Positive semi-definite operators

The cone of positive-semidefinite matrices (in the ambient space of symmetric matrices) is going to come up frequently. We recall the definition, which gives us a good example of why the spectral theorem is so useful.

Definition 39 (positive-semidefinite)**.** If $(V, \mathbb{F})$ is an inner-product space and if $L \in \mathcal{B}(V)$, then L is *positive-semidefinite* or *PSD* if

$$\forall x \in V : \langle L(x), x \rangle \geq 0.$$

Proposition 20. *If $A \in \mathbb{R}^{n \times n}$ is symmetric, then A is positive-semidefinite if and only if every eigenvalue of A is nonnegative.*

Proof. Use the spectral theorem for linear algebra to write $A = UDU^T$ with the eigenvalues of A on the diagonal of D and all other entries of D zero. Then

$$\langle Ax, x \rangle = \left\langle UDU^T x, x \right\rangle = \left\langle D\left(U^T x\right), U^T x \right\rangle.$$

Since U is an isometry on V, we have $V = \left\{ U^T x \;\middle|\; x \in V \right\}$. Thus we can let $y = U^T x$ above and conclude that

$$\forall x \in V : \langle Ax, x \rangle \geq 0 \iff \forall y \in V : \langle Dy, y \rangle \geq 0.$$

Now simply consider $y = (1, 0, \ldots)^T$, $y = (0, 1, \ldots)^T$, et cetera to see that this is equivalent to the diagonal entries of D (the eigenvalues of A) being nonnegative:

$$\langle De_i, e_i \rangle = \lambda_i \geq 0.$$

□

Warning 6: Positive-semidefinite isn't self-adjoint

Some authors define a positive-semidefinite operator to be self-adjoint (so that its matrix is symmetric or Hermitian). When you're working over the complex numbers, this kind-of makes sense, because in that case the condition in Definition 39 implies that the operator is self-adjoint. In particular, when we write $\langle L(x), x \rangle \geq 0$, we mean that the inner product is *real*. On a complex vector space, that can only happen when L is self-adjoint.

Example 28. If $(V, \mathbb{C})$ is an inner-product space and if $L \in \mathcal{B}(V)$ is *not* self-adjoint, then there exists some $x \in V$ such that

$$\langle L(x), x \rangle \neq \langle x, L(x) \rangle \iff \langle L(x), x \rangle \neq \overline{\langle L(x), x \rangle}.$$

Clearly this means that $\langle L(x), x \rangle$ is not real.

However, over the real numbers, symmetry and positive-semidefiniteness don't come as a package.

Example 29. Let $A \in \mathbb{R}^{2\times 2}$ and an arbitrary $x \in \mathbb{R}^{2\times 1}$ be given by

$$A = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \text{ and } x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

Clearly, A is not symmetric. And yet,

$$\langle Ax, x\rangle = \left\langle \begin{bmatrix} x_1 + x_2 \\ -x_1 + x_2 \end{bmatrix}, \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \right\rangle = x_1^2 + x_2^2 \geq 0,$$

showing that A is positive-semidefinite.

4.4 Characteristic and minimal polynomials

The utility of results like Proposition 19 might not be immediately clear; however, the polynomial it refers to is quite important. Refer to Section 3.3 and specifically Example 18 if the notation needs explaining.

Theorem 19. *The polynomial* $\det(\Lambda I - A) \in \mathbb{R}[\Lambda]$ *is the characteristic polynomial of* $A \in \mathbb{R}^{n\times n}$. *Axler, Theorem 10.17*

The polynomial object in Theorem 19 is computed according to Definition 35. Since the determinant involves only addition and multiplication, and since $\mathbb{R}[\Lambda]$ is a ring, the end result is back in that same ring; that is, $\det(\Lambda I - A) \in \mathbb{R}[\Lambda]$.

Recall that the characteristic polynomial of a *complex* matrix A is usually defined as

$$(\Lambda - \lambda_1)^{m_1}(\Lambda - \lambda_2)^{m_2}\cdots(\Lambda - \lambda_k)^{m_k} \in \mathbb{C}[\Lambda], \tag{4.3}$$

where the k real numbers $\lambda_1, \ldots, \lambda_k$ are the distinct (complex) eigenvalues of A, and the exponent m_i is the dimension of $\ker(\lambda_i I - A)$. You can find it in SageMath, although the default is to output a lowercase x for the polynomial indeterminate:

```
sage: A = matrix.hilbert(3); A
[  1 1/2 1/3]
[1/2 1/3 1/4]
[1/3 1/4 1/5]
sage: A.characteristic_polynomial()
x^3 - 23/15*x^2 + 127/720*x - 1/2160
```

Proposition 21. *The exponents* $m_1, \ldots, m_k$ *in Equation (4.3) sum to* n. *Axler, Proposition 8.18*

Thus, the characteristic polynomial of a complex n-by-n matrix is always of degree n. The real-matrix case is rather more annoying; you can consult Chapter 9 in Axler for the details. However, things are just as nice for real *symmetric* matrices, because their eigenvalues are all real.

Proposition 22. *If $A \in \mathbb{R}^{n\times n}$ is symmetric, then the characteristic polynomial of A is*

$$(\Lambda - \lambda_1)^{m_1} (\Lambda - \lambda_2)^{m_2} \cdots (\Lambda - \lambda_k)^{m_k} \in \mathbb{R}[\Lambda],$$

where the k real numbers $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of A, the exponents m_i are the dimensions of the $\ker(\lambda_i I - A)$, and $\sum_i m_i = n$.

Proof. Since A is symmetric, we cite Proposition 19 and Theorem 19 to conclude that

$$\det(\Lambda I - A) \in \mathbb{R}[\Lambda]$$

is the characteristic polynomial of A. It follows from the definition of determinant that the whole thing is a polynomial of degree n, and since the corresponding function $[\det(\Lambda I - A)]\restriction_{\mathbb{R}}$ has n roots, it factors into the stated form. □

Exercise 8 (characteristic polynomial of transpose operator). The characteristic polynomial of a linear operator is defined to be the characteristic polynomial of its matrix representation with respect to any basis. Let L be the "transpose" operator on $V = \mathbb{R}^{2\times 2}$ that sends a matrix A to its transpose, A^T. Use your solutions to Exercise 4 and/or Exercise 7 to show that L is self-adjoint, and then use either its matrix representation or Proposition 22 to find its characteristic polynomial.

Exercise 9 (axiomatic determinant). Suppose that $A \in \mathbb{R}^{n\times n}$ is a symmetric matrix. In Proposition 19 (and thus in Proposition 22), we have relied upon the fact that the roots of $\gamma_A\restriction_{\mathbb{R}}$ are the eigenvalues of A. This is based on the belief that there are nontrivial solutions $\lambda \in \mathbb{R}$ to the equation $(\lambda I - A)\, x = 0$ if and only if $(\lambda I - A)$ is singular if and only if $\det(\lambda I - A) = 0$. From Definition 35, it's not obvious that the determinant has that property.

For reasons like that, an axiomatic definition of the determinant is often used instead. For example, if R is a commutative ring, then the determinant is the *unique* function from $R^{n\times n}$ to R satisfying the following four properties:

1. $\det(I) = 1_R$, where $I = 1_{R^{n\times n}}$ is the identity matrix in $R^{n\times n}$.
2. If you fix any $n-1$ rows of A, then det is linear in the remaining row. For example, if the rows of A are $A_1, A_2, \ldots, A_n$, then

$$\det(A) \coloneqq \det\left(\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{bmatrix}\right),$$

and the linearity that we refer to is (for example, in the first row),

$$\det\left(\begin{bmatrix}\alpha A_1 + B\\ A_2\\ \vdots\\ A_n\end{bmatrix}\right) = \alpha\det\left(\begin{bmatrix}A_1\\ A_2\\ \vdots\\ A_n\end{bmatrix}\right) + \det\left(\begin{bmatrix}B\\ A_2\\ \vdots\\ A_n\end{bmatrix}\right).$$

3. If two adjacent rows of A are equal, then $\det(A) = 0$.

From those three properties it follows that $\det(AB) = \det(A)\det(B)$. Take the three properties (and the one consequence) as your definition of the determinant, and use the spectral decomposition of the symmetric matrix $A \in \mathbb{R}^{n\times n}$ to show directly that

$$\gamma_A = \det(\Lambda I - A) = (\Lambda - \lambda_1)(\Lambda - \lambda_2)\cdots(\Lambda - \lambda_n) \in \mathbb{R}[\Lambda],$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the (possibly repeated) eigenvalues of A. In other words, re-prove Proposition 22 using an axiomatic definition of the determinant.

Hint: this is easier than it sounds. First use the spectral theorem for linear algebra to diagonalize A. Use one of the properties to eliminate the orthogonal matrices. Then all that remains is to find the determinant of a diagonal matrix using the given properties.

The next theorem looks pretty innocent, but we'll use it over and over again.

Axler, Theorems 8.20 and 9.20

Theorem 20 (Cayley-Hamilton Theorem)**.** *If $A \in \mathbb{R}^{n\times n}$ and if p is the characteristic polynomial of A, then the associated function $p\restriction_{\mathbb{R}^{n\times n}} : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ satisfies $p\restriction_{\mathbb{R}^{n\times n}}(A) = 0$.*

The Cayley-Hamilton theorem tells us something surprising: we know that $\mathbb{R}^{n\times n}$ is a vector space of dimension n^2, right? So let $A \in \mathbb{R}^{n\times n}$ be given, and consider the set of powers,

$$\left\{A^0, A^1, A^2, \ldots, A^{(n^2)}\right\}.$$

How many powers do we need before this set becomes linearly-dependent? In the worst case, we might expect the answer to be n^2, because that's the dimension of the ambient space.

Definition 40. The minimal polynomial of $A \in \mathbb{R}^{n\times n}$ is the monic polynomial $p \in \mathbb{R}[\Lambda]$ of smallest degree such that the associated function $p\restriction_{\mathbb{R}^{n\times n}} : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ satisfies $p\restriction_{\mathbb{R}^{n\times n}}(A) = 0$.

Recall that if the set $\left\{A^0, A^1, \ldots, A^{m-1}\right\}$ is linearly-independent but the set $\left\{A^0, A^1, \ldots, A^m\right\}$ is linearly-*dependent*, then we can write A^m as a unique linear combination of the lower powers $A^0, A^1, \ldots, A^{m-1}$. It's not obvious, but this gives us a way to find the minimal polynomial of a matrix. But for sure, it

gives us a polynomial function that evaluates to zero on A, since

$$A^m = a_0 A^0 + a_1 A^1 + \cdots + a_{(m-1)} A^{m-1}$$
$$\iff$$
$$A^m - a_0 A^0 - a_1 A^1 - \cdots - a_{(m-1)} A^{m-1} = 0.$$

To prove that this is indeed the minimal polynomial of $A \in \mathbb{R}^{n \times n}$ takes a bit of work. We omit the proof of the next proposition because we give a more general proof in Proposition 34 that actually applies to any finite-dimensional power-associative unital algebra, and in particular to the associative algebra of matrices under matrix multiplication (we showed that this is an associative algebra in the algebra of linear operators).

Proposition 23. *If $A \in \mathbb{R}^{n \times n}$ for $n \geq 1$, then the minimal polynomial of A is*

$$\mu_A = \Lambda^d - a_0 \Lambda^0 - a_1 \Lambda^1 - \cdots - a_{(d-1)} \Lambda^{d-1} \in \mathbb{R}\left[\Lambda\right],$$

where $d \geq 1$ is first power of A that can be expressed as a linear combination of lower powers, and where the coefficients $\{a_0, a_1, \ldots, a_{d-1}\}$ are the coordinates of A^d with respect to $\left\{A^0, A^1, \ldots, A^{d-1}\right\}$ in span $\left(\left\{A^0, A^1, \ldots, A^{d-1}\right\}\right)$.

So, asking how many linearly-independent powers we can get is equivalent to asking the degree of the minimal polynomial. The importance of the Cayley-Hamilton theorem is that it shows that the minimal polynomial of any matrix must divide its characteristic polynomial (the "minimal" is with respect to the "divides" ordering that we'll meet in Example 40). And the characteristic polynomial is always degree n in $\mathbb{R}^{n \times n}$, as we just showed. Thus, even though we might expect to need n^2 powers, it turns out that we only need the *much* smaller number n. SageMath can also find minimal polynomials:

```
sage: A = matrix(ZZ, [[4,0,0],
....:                 [0,2,2],
....:                 [0,2,2]])
sage: p = A.characteristic_polynomial(); p
x^3 - 8*x^2 + 16*x
sage: m = A.minimal_polynomial(); m
x^2 - 4*x
sage: m.divides(p)    # by Cayley-Hamilton
True
```

We're going to reinvent all of these concepts later, in the setting of a Euclidean Jordan algebra, so it's important that you have some intuition for the minimal/characteristic polynomials and why they're useful.

Theorem 21. *The determinant of a symmetric matrix $A \in \mathbb{R}^{n\times n}$ is the product of its eigenvalues, and the trace of A is the sum of its eigenvalues.*

Proof. Use the spectral theorem for linear algebra to write $A = UDU^T$ where U is orthogonal (so $U^T = U^{-1}$). Then

$$\det(A) = \det\left(UDU^{-1}\right) = \det(U)\det(D)\det\left(U^{-1}\right) = \det(D),$$

and since the eigenvalues of A are on the diagonal of D and the rest of D contains zeros, the only non-zero term in $\det(D)$ is the product of the eigenvalues of A.

For the trace, the same trick works:

$$\operatorname{trace}(A) = \operatorname{trace}\left(UDU^{-1}\right) = \operatorname{trace}\left(DU^{-1}U\right) = \operatorname{trace}(D).$$

Now the trace of D is the sum of its diagonal entries, the eigenvalues of A. □

This theorem holds also for asymmetric matrices, but it's harder to prove when you can't use the spectral theorem to diagonalize the matrix.

Corollary 8. *The determinant of a symmetric matrix $A \in \mathbb{R}^{n\times n}$ is $(-1)^n$ times the constant (zeroth) term in its characteristic polynomial, and the trace of A is (-1) times the coefficient of the penultimate term.*

Proof. Consider the argument zero to the real function $p\restriction_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ associated with the characteristic polynomial $p \in \mathbb{R}[\Lambda]$ of A. By Proposition 22,

$$\begin{aligned} p\restriction_{\mathbb{R}}(0) &= (-\lambda_1)^{m_1}\left(-\lambda_2^{m_2}\right)\cdots\left(-\lambda_k^{m_k}\right) \\ &= (-1)^{(m_1+m_2+\cdots+m_k)}\lambda_1^{m_1}\lambda_2^{m_2}\cdots\lambda_k^{m_k} \\ &= (-1)^n\lambda_1^{m_1}\lambda_2^{m_2}\cdots\lambda_k^{m_k}. \end{aligned}$$

is the constant term in the characteristic polynomial because all others go away when apply the function to 0. It is also $(-1)^n$ times the product of the eigenvalues of A, which Theorem 21 shows is the determinant of A.

For the trace, consider the polynomial of degree n,

$$p = (\Lambda - \sigma_1)(\Lambda - \sigma_2)\cdots(\Lambda - \sigma_n) \in \mathbb{R}[\Lambda],$$

where $\sigma_i \in \mathbb{R}$. We claim that the coefficient of Λ^{n-1} in this polynomial is $-\sum_{i=1}^n \sigma_i$, and can prove it by induction. The result is clearly true for $n = 1$, where $p = \Lambda^1 - \sigma_1$ and σ_1 is the coefficient of $\Lambda^{n-1} = \Lambda^0$. So, assume that it holds for polynomials of degree $n-1$, and reconsider

$$p = (\Lambda - \sigma_1)\underbrace{(\Lambda - \sigma_2)\cdots(\Lambda - \sigma_n)}_{q} = \Lambda q - \sigma_1 q$$

where now we have introduced a polynomial $q \in \mathbb{R}[\Lambda]$ of degree $n-1$. The coefficient of Λ^{n-1} in p must be the coefficient of Λ^{n-1} in Λq minus the coefficient of Λ^{n-1} in $\sigma_1 q$. But within q, the induction hypothesis applies, and we see that

in q, the coefficient of Λ^{n-2} must be $-\sum_{i=2}^{n}\sigma_i$. Thus in Λq, the coefficient of Λ^{n-1} is also $-\sum_{i=2}^{n}\sigma_i$. Moreover, in q, the coefficient of Λ^{n-1} is one (it's a monic polynomial), so the coefficient of Λ^{n-1} in $\sigma_1 q$ is simply σ_1. Subtracting the two, we get

$$\left(-\sum_{i=2}^{i=n}\sigma_i\right)-\sigma_1=-\sum_{i=1}^{n}\sigma_i,$$

and the statement is proved. To turn this into a statement about the trace, simply apply it to the characteristic polynomial in Proposition 22, whence the coefficient of Λ^{n-1} is $-\sum_k \lambda_k m_k$, or negative the sum of the eigenvalues of A, including repeats, that we showed in Theorem 21 was the trace. □

Exercise 10 (inverse via Cayley-Hamilton). Suppose that $A\in\mathbb{R}^{n\times n}$ is symmetric and has characteristic polynomial

$$\gamma_A=a_0+a_1\Lambda+a_2\Lambda^2+\cdots+\Lambda^n\in\mathbb{R}\left[\Lambda\right].$$

Recall that the inverse of A is the unique matrix B such that $AB=BA=I$, where $I\in\mathbb{R}^{n\times n}$ denotes the identity matrix, and use the Cayley-Hamilton Theorem to find a formula for the inverse of A when $\det(A)\neq 0$.

4.5 Solutions to exercises

Solution to Exercise 4 (matrix of transpose operator). The transpose is linear on any real matrix space. Two matrices are equal if their entries are equal, and

$$\left((\alpha A+B)^T\right)_{ij}=(\alpha A+B)_{ji}=\alpha\left(A^T\right)_{ij}+\left(B^T\right)_{ij}=\left(\alpha A^T+B^T\right)_{ij}.$$

For a basis of V, the obvious choice is $\mathbf{b}=\{b_1,b_2,b_3,b_4\}$ where

$$b_1=\begin{bmatrix}1&0\\0&0\end{bmatrix},\quad b_2=\begin{bmatrix}0&1\\0&0\end{bmatrix},\quad b_3=\begin{bmatrix}0&0\\1&0\end{bmatrix},\quad b_4=\begin{bmatrix}0&0\\0&1\end{bmatrix}.$$

This spans the space, since for any $\alpha,\beta,\gamma,\delta\in\mathbb{R}$, we have

$$\begin{bmatrix}\alpha&\beta\\\gamma&\delta\end{bmatrix}=\alpha b_1+\beta b_2+\gamma b_3+\delta b_4. \tag{4.1}$$

Moreover Equation (4.1) shows that $\mathbf{b}$ is linearly-independent, since

$$\alpha b_1+\beta b_2+\gamma b_3+\delta b_4=\begin{bmatrix}0&0\\0&0\end{bmatrix}$$
$$\iff$$
$$\alpha=\beta=\gamma=\delta=0.$$

So $\mathbf{b}$ is in fact a basis for V. To find the matrix of L, we just use the formula,

$$\begin{aligned}
\mathbf{b}(L) &= \begin{bmatrix} \mathbf{b}(L(b_1)) & \mathbf{b}(L(b_2)) & \mathbf{b}(L(b_3)) & \mathbf{b}(L(b_4)) \end{bmatrix} \\
&= \begin{bmatrix} \mathbf{b}(b_1) & \mathbf{b}(b_3) & \mathbf{b}(b_2) & \mathbf{b}(b_4) \end{bmatrix} \\
&= \begin{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.
\end{aligned}$$

Solution to Exercise 5 (isometry between finite-dimensional spaces). Let $\mathbf{a} = \{a_1, a_2, \ldots, a_n\}$ be a basis for V and $\mathbf{b} = \{b_1, b_2, \ldots, b_n\}$ be a basis for W. Since V, W are both n-dimensional, the two bases contain the same number of elements. By the Gram-Schmidt orthonormalization process (Roman, Theorem 9.11), there also exist two *orthonormal* bases

$$\begin{aligned}
\hat{\mathbf{a}} &= \{\hat{a_1}, \hat{a_2}, \ldots \hat{a_n}\}, \text{ and} \\
\hat{\mathbf{b}} &= \left\{\hat{b_1}, \hat{b_2}, \ldots \hat{b_n}\right\}
\end{aligned}$$

of V and W, respectively, obtained from the originals. Theorem 2.2 in Roman says that we can define a linear transformation by specifying its action on a basis, so we define

$$L(\hat{a_i}) = \hat{b_i},$$

and its linear extension should be an isometry. To see this, let $x, y \in V$ be arbitrary. We can represent them uniquely in terms of our orthonormal basis,

$$\begin{aligned}
x &= x_1\hat{a_1} + x_2\hat{a_2} + \cdots + x_n\hat{a_n} \\
y &= y_1\hat{a_1} + y_2\hat{a_2} + \cdots + y_n\hat{a_n},
\end{aligned}$$

and simply compute. First in V,

$$\begin{aligned}
\langle x, y\rangle_V &= \sum_{i=1}^{n}\sum_{j=1}^{n} \langle x_i\hat{a_i}, y_j\hat{a_j}\rangle_V \\
&= \sum_{i=1}^{n} \langle x_i\hat{a_i}, y_i\hat{a_i}\rangle_V \qquad \text{(since the basis } \hat{\mathbf{a}} \text{ is orthogonal)} \\
&= \sum_{i=1}^{n} x_i y_i \left\|\hat{a_i}\right\|_V^2 \\
&= \sum_{i=1}^{n} x_i y_i \qquad \text{(since the basis } \hat{\mathbf{a}} \text{ is normal).}
\end{aligned}$$

and then in W, using our definition of L and its linearity:

$$\begin{aligned}
\langle L(x), L(y)\rangle_W &= \sum_{i=1}^{n}\sum_{j=1}^{n}\left\langle x_i\hat{b_i}, y_j\hat{b_j}\right\rangle_W \\
&= \sum_{i=1}^{n}\left\langle x_i\hat{b_i}, y_i\hat{b_i}\right\rangle_W \qquad \text{(since the basis } \hat{\mathbf{b}} \text{ is orthogonal)} \\
&= \sum_{i=1}^{n} x_i y_i \left\|\hat{b_i}\right\|_W^2 \\
&= \sum_{i=1}^{n} x_i y_i \qquad \text{(since the basis } \hat{\mathbf{b}} \text{ is normal).}
\end{aligned}$$

Solution to Exercise 6 (eigenvalues of powers). Use the spectral theorem for linear algebra to write $A = UDU^T$. Then,

$$A^k = \underbrace{UDU^TUDU^T\cdots UDU^T}_{k \text{ times}} = UD^kU^T,$$

since all of the U^TU terms in the middle cancel. Now

$$D^k = \operatorname{diag}\left(\lambda_1^k, \lambda_2^k, \ldots, \lambda_n^k\right),$$

and the only question that remains is, why should those be the eigenvalues of UD^kU^T? Suppose that

$$UD^kU^Tx = \lambda x,$$

where $x \neq 0$, and then let $U^Tx = y$ which is also non-zero because U^T is an isometry. We can also multiply on the left by $U^T = U^{-1}$ to obtain,

$$\begin{gathered}
U^TUD^kU^Tx = \lambda U^Tx \\
\Longleftrightarrow \\
D^ky = \lambda y \\
\Longleftrightarrow \\
\begin{bmatrix} \lambda_1^k y_1 \\ \lambda_2^k y_2 \\ \vdots \\ \lambda_n^k y_n \end{bmatrix} = \begin{bmatrix} \lambda y_1 \\ \lambda y_2 \\ \vdots \\ \lambda y_n \end{bmatrix}.
\end{gathered}$$

The vector y was nonzero, so some particular coordinate y_j is non-zero. If λ is *not* equal to *any* of the λ_i^k, then in particular $\lambda \neq \lambda_j^k$. But then the equation above is false in the jth row. So, it must be the case that λ is contained in the set $\left\{\lambda_i^k \;\middle|\; i = 0, 1, \ldots, n\right\}$.

On the other hand, by choosing $x = Ue_1, Ue_2, \ldots, Ue_n$ successively, where e_i is the ith standard basis vector, we see that each λ_i^k is indeed an eigenvalue of UD^kU^T. So the set $\left\{\lambda_i^k \;\middle|\; i = 0, 1, \ldots, n\right\}$ is precisely its set of eigenvalues.

Solution to Exercise 7 (eigenspaces of transpose operator). Suppose that $A \in \mathbb{R}^{2\times 2}$ is an eigenvector of L corresponding to the eigenvalue $\lambda \in \mathbb{R}$, so that $L(A) = \lambda A$. Then

$$L(L(A)) = \lambda L(A) = \lambda^2 A.$$

But we also know that

$$L(L(A)) = A,$$

since taking the transpose twice gives us back the original matrix. Combining these two equations and using the fact that $A \neq 0$ (from the definition of an eigenvector) gives us $\left(\lambda^2 - 1\right) = 0$. This quadratic equation has two solutions, $\lambda = 1$ and $\lambda = -1$.

The eigenspace corresponding to $\lambda = 1$ consists of the symmetric matrices,

$$V_1 \coloneqq \left\{ \begin{bmatrix} \alpha & \beta \\ \beta & \gamma \end{bmatrix} \;\middle|\; \alpha, \beta, \gamma \in \mathbb{R} \right\}$$

since those are the matrices that are left unchanged by the "transpose" operation. The other eigenspace, corresponding to $\lambda = -1$, consists of *skew-symmetric* matrices,

$$V_2 \coloneqq \left\{ \begin{bmatrix} 0 & \beta \\ -\beta & 0 \end{bmatrix} \;\middle|\; \beta \in \mathbb{R} \right\}.$$

Let $\mathbf{b} = \{b_1, b_2, b_3, b_4\}$ be the basis of $\mathbb{R}^{2\times 2}$ that we used in our solution to Exercise 4, namely

$$b_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad b_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad b_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

This basis is in fact orthonormal:

```
sage: b1 = matrix(QQ,[[1,0],
....:                 [0,0]])
sage: b2 = matrix(QQ,[[0,1],
....:                 [0,0]])
sage: b3 = matrix(QQ,[[0,0],
....:                 [1,0]])
sage: b4 = matrix(QQ,[[0,0],
....:                 [0,1]])
sage: b = [b1,b2,b3,b4]
sage: [ (b[i]*b[j].transpose()).trace()
....:   for i in range(4)
....:   for j in range(4)
....:   if i == j ]
[1, 1, 1, 1]
sage: [ (b[i]*b[j].transpose()).trace()
....:   for i in range(4)
....:   for j in range(4)
....:   if i != j ]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

As a result, the set $\{b_1, b_2 + b_3, b_4\}$ forms a basis for the (three-dimensional) subspace V_1 of symmetric matrices; and likewise, the set $\{b_2 - b_3\}$ forms a basis for the (one-dimensional) subspace V_2 of skew-symmetric matrices. It is straightforward to show that these are indeed bases for their respective spaces, and that the two subspaces are orthogonal to one another in the sense of Equation (4.2) by using the fact that the elements of $\mathbf{b}$ are orthonormal. For example, $\langle b_2 - b_3, b_4\rangle = \langle b_2, b_4\rangle - \langle b_3, b_4\rangle = 0 - 0$. And since $1 = \dim(V_2)$ and $3 = \dim(V_1)$ sum to $4 = \dim(V)$, the direct sum of V_1 and V_2 must be V itself.

Solution to Exercise 8 (characteristic polynomial of transpose operator). In Exercise 4 we found that

$$\mathbf{b}(L) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

with respect to the basis $\mathbf{b} = \{b_1, b_2, b_3, b_4\}$ whose elements are

$$b_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad b_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad b_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Then, in Exercise 7 we showed that $\mathbf{b}$ is an orthonormal basis for V. We can therefore apply Proposition 18 to conclude that L is self-adjoint because the matrix $\mathbf{b}(L)$ is symmetric. We also showed in Exercise 7 that V is an

orthogonal direct sum of two eigenspaces V_1 and V_2 of L. By combining two unit norm-bases of V_1 and V_2, we obtain an orthonormal basis for V consisting of eigenvectors of L—which by the spectral theorem for linear algebra also shows that L is self-adjoint.

We can compute the characteristic polynomial of L directly from its matrix:

```
sage: R = PolynomialRing(QQ,'X')
sage: X = R.gen()
sage: L = matrix(R, [[1,0,0,0],
....:                [0,0,1,0],
....:                [0,1,0,0],
....:                [0,0,0,1]])
sage: I = identity_matrix(R,4)
sage: (X*I - L).determinant().factor()
(X + 1) * (X - 1)^3
```

We could also apply Proposition 22 here, since in Exercise 7 we proved that $\dim(V_1) = 3$ and $\dim(V_2) = 1$ are the dimensions of the eigenspaces corresponding to $\lambda = 1$ and $\lambda = -1$ respectively.

Solution to Exercise 9 (axiomatic determinant). Let $R \coloneqq \mathbb{R}[\Lambda]$ and note that $\Lambda I - A$ lives in the space $R^{n\times n}$. The symbol I therefore necessarily denotes the identity matrix in $R^{n\times n}$.

Use the spectral theorem for linear algebra to write $A = UDU^T$, and substitute that into the formula for the characteristic polynomial:

$$\begin{aligned}\gamma_A &= \det\left(\Lambda I - UDU^T\right)\\ &= \det\left(U\left(\Lambda U^T IU - D\right)U^T\right)\\ &= \det\left(U\left(\Lambda I - D\right)U^T\right).\end{aligned}$$

Using the fact that $\det(AB) = \det(A)\det(B)$, we have

$$\det\left(U\left(\Lambda I - D\right)U^T\right) = \det(U)\det\left(\Lambda I - D\right)\det\left(U^T\right).$$

Now, from $\det(I) = 1_R$, we deduce that

$$\det(I) = \det\left(UU^T\right) = \det(U)\det\left(U^T\right) = 1_R,$$

and thus,

$$\det(U)\det\left(\Lambda I - D\right)\det\left(U^T\right) = \det\left(\Lambda I - D\right).$$

If $D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$, then in block form,

$$\Lambda I - D = \begin{bmatrix} (\Lambda - \lambda_1)\, e_1 \\ (\Lambda - \lambda_2)\, e_2 \\ \vdots \\ (\Lambda - \lambda_n)\, e_n \end{bmatrix},$$

where e_i denotes the ith standard basis vector, which is the ith row of the identity matrix. Using the row-linearity property, we can pull these out one at a time,

$$\det(\Lambda I - D) = \det\left(\begin{bmatrix} (\Lambda - \lambda_1)\, e_1 \\ (\Lambda - \lambda_2)\, e_2 \\ \vdots \\ (\Lambda - \lambda_n)\, e_n \end{bmatrix}\right) = (\Lambda - \lambda_1) \det\left(\begin{bmatrix} e_1 \\ (\Lambda - \lambda_2)\, e_2 \\ \vdots \\ (\Lambda - \lambda_n)\, e_n \end{bmatrix}\right),$$

until eventually we're left with

$$(\Lambda - \lambda_1)(\Lambda - \lambda_2) \cdots (\Lambda - \lambda_n) \det(I).$$

Use the fact that $\det(I) = 1_R$ one more time, and we're done.

Solution to Exercise 10 (inverse via Cayley-Hamilton). The Cayley-Hamilton Theorem says that

$$\gamma_A\restriction_{\mathbb{R}^{n\times n}}(A) = a_0 I + a_1 A + a_2 A^2 + \cdots + A^n = 0.$$

Move the identity to the other side, and factor out an A:

$$A\left(a_1 I + a_2 A + \cdots + A^{n-1}\right) = -a_0 I.$$

From Corollary 8, we know that $a_0 = (-1)^n \det(A)$. If $\det(A) \neq 0$, then $a_0 \neq 0$, and we can solve

$$A\left[\frac{a_1 I + a_2 A + \cdots + A^{n-1}}{-a_0}\right] = I.$$

Since powers of a matrix commute, the same thing holds on the other side,

$$\left[\frac{a_1 I + a_2 A + \cdots + A^{n-1}}{-a_0}\right] A = I,$$

and thus we've found the inverse of A.

Chapter 5

Convex geometry

The goal of mathematical optimization problem is minimize or maximize something. Minimization and maximization require you to have some idea of bigness and smallness, and as a result, we tend to do optimization over the real numbers. Typically the thing we minimize or maximize is a function into the real numbers; given $f : V \to \mathbb{R}$, we might be asked to

$$\begin{gathered}\text{minimize } f(x) \\ \Longleftrightarrow \\ \text{find } x^* \in V \text{ such that } f(x^*) = \inf\{f(x) \mid x \in V\}.\end{gathered}$$

Our use of the infimum here provides another reason to work in the real number system: we want that inf to exist. Now, people thought this looked too easy, so they started to impose extra conditions. One natural constraint would be to restrict x to a subset of the domain, one that is defined by a list of functions. If we choose a bunch of real functions $g_1, g_2, \ldots, g_m$ that are also defined on V, then we can reformulate the problem,

$$\begin{aligned}\text{minimize } & f(x) \\ \text{subject to } & g_1(x) \leq 0 \\ & g_2(x) \leq 0 \\ & \vdots \\ & g_m(x) \leq 0.\end{aligned}$$

By choosing the functions g_i carefully, this approach can be used to impose all kinds of constraints on the problem. In fact, the g_i are called constraint functions, and the whole problem above is called a constrained optimization problem.

5.1 Convex sets

The good/bad news is, without knowing more about f or the constraint functions g_i, we have very little idea how to solve these problems. The main reason we study convex sets and functions is because we can actually solve constrained optimization problems when the functions and sets are both convex.

Definition 41. If x and y are elements of a real vector space, then a *convex combination* of x y is any sum $\alpha x + (1-\alpha)\, y$ where $\alpha \in [0,1]$.

The set of all convex combinations of x and y forms the line segment between x and y. You can think of this in one of two ways. First, you can think of α as being a parameter that ranges from one (none of the way) to zero (all of the way), and represents how far along the segment from x to y we are. When $\alpha = 0$, we're at y, and when $\alpha = 1$, we're at x. Between those two extremes, it varies linearly. The other way to think of it is to rewrite

$$\alpha x + (1-\alpha) = y + \alpha\,(x-y)\,,$$

where now we can think of $x - y$ as being the distance from y to x, and the parameter α as indicating the portion of that distance that we've "traveled."

Definition 42. A set X in a real vector space V is a *convex set* if

$$\forall x, y \in V : [\forall \alpha \in [0,1] : \alpha x + (1-\alpha)\, y \in V]\,.$$

In other words, a set is convex if any convex combination of two of its elements is back in the set.

The line segment between any two points in a convex set is thus completely contained in that set.

Example 30. Every vector space is convex, somewhat obviously.

Example 31. If V is a normed vector space and if $x \in V$, then any ball centered at x is convex. To see this, let its radius be r, so that the ball is given by

Boyd, 2.2.2 and 2.2.3

$$B_r(x) = \{x + y \mid y \in V, \|y\| < r\}\,.$$

Now suppose $z_1 = x + y_1$ and $z_2 = x + y_2 \in B_r(x)$, so that $\|y_1\| < r$ and $\|y_2\| < r$. We will let $z_3 = x + y_3$ be any point on the segment that joins z_1 and z_2. Thus we will assume that

$$\exists \alpha \in [0,1] : z_3 = x + y_3 = \alpha\,(x + y_1) + (1-\alpha)\,(x + y_2)\,,$$

and our goal is to show that $\|y_3\| < r$, allowing us to conclude that $z_3 \in B_r(x)$ as well. This is not hard: factor out the x terms above to obtain,

$$\begin{gathered} x + y_3 = [\alpha + (1-\alpha)]\, x + \alpha y_1 + (1-\alpha)\, y_2 \\ \iff \\ y_3 = \alpha y_1 + (1-\alpha)\, y_2. \end{gathered}$$

Now take norms on both sides, and use the triangle inequality:

$$\|y_3\| \leq \alpha \|y_1\| + (1-\alpha) \|y_2\| \leq \alpha r + (1-\alpha) r = r.$$

Definition 43. If X is a nonempty subset of a real vector space V, then the *convex hull* of X is

$$\operatorname{conv}(X) \coloneqq \left\{ \sum_{i=1}^{m} \alpha_i x_i \;\middle|\; m \in \mathbb{N}, x_i \in X, \alpha_i \geq 0, \sum_{i=1}^{m} \alpha_i = 1 \right\}.$$

We have already defined a convex combination of two points; the convex hull extends that concept to three or more points. Analogous to how $\operatorname{conv}(\{x, y\})$ is the line segment between x and y, we can think of $\operatorname{conv}(\{x, y, z\})$ as being the "triangle" bounded by x, y, and z.

Perhaps the best way to think of $\operatorname{conv}(X)$ is as "the convex set generated by X." This is a familiar idea: $\operatorname{span}(X)$ is the vector space generated by X, for example, and is obtained by starting with X and then adding in all of the things that have to be there to satisfy the definition of a vector space. In exactly the same way, $\operatorname{conv}(X)$ is defined as if we started with X, and then we added in everything else that needs to be there to make a convex set. In that regard, it should not be surprising that $\operatorname{conv}(X)$ is the smallest convex set containing X.

Proposition 24. *If V is a real vector space and if $X, Y \subseteq V$ are convex, then $X \cap Y$ is convex.* *Boyd, 2.3.1*

Proof. Pick any two points in $X \cap Y$; they both live in X and they both live in Y, by definition. Thus the line segment between them lives in both X and Y, and so it lives in their intersection as well. □

5.2 Convex cones

So we've seen convex functions and general convex sets, and we know why they're nice to have. But the most important convex sets we will encounter are convex *cones*. The optimization algorithms we focus on will all have feasible sets that are (slices of) convex cones.

Definition 44. If X is a nonempty subset of a real vector space V and if

$$\forall x \in X, \forall \alpha \geq 0 : \alpha x \in X,$$

then X is a *cone*.

Thus a cone is simply a subset of a real vector space that is closed under nonnegative scaling.

Example 32. Any vector space is a cone, in a fairly obvious way.

Example 33. If you take any nonempty subset X of a real vector space and generate all nonnegative multiples of it, then the result $K \coloneqq \{\alpha x \mid x \in X, \alpha \geq 0\}$ must be a cone.

Cones are alright, but convex cones are better.

Definition 45. A *convex cone* is a cone that also happens to be convex. Likewise, a *closed convex cone* is a convex cone that just happens to be a closed set (relative to the ambient vector space).

Just like we did with convex combinations, we can define "conic combinations," and use them to construct "conic hulls."

Definition 46. If X is a nonempty subset of a real vector space V, then the *conic hull* of X is

$$\operatorname{cone}(X) \coloneqq \left\{ \sum_{i=1}^{m} \alpha_i x_i \;\middle|\; m \in \mathbb{N}, x_i \in X, \alpha_i \geq 0 \right\}.$$

This should look a lot like the definition of a convex hull, because it is. The only difference is that we don't require the coefficients in the conic hull to sum to one—any collection of nonnegative coefficients will do. For identical reasons, we think of $\operatorname{cone}(X)$ as being "the cone generated by X," and $\operatorname{cone}(X)$ is also the smallest cone that contains X. It's also worth noting that $\operatorname{cone}(X)$ is nothing other than all nonnegative multiples of $\operatorname{conv}(X)$.

Exercise 11 (cone convexity characterization). Assume that K is a cone in some finite-dimensional real vector space V, and show that

$$K \text{ is convex} \iff \forall x, y \in K : x + y \in K.$$

There are a few other "special" types of cones that you'll encounter. Let's get the names out of the way.

Definition 47. Let V be a real, finite-dimensional vector space. A convex cone K in V is *solid* if $\operatorname{span}(K) = V$, and *pointed* if $-K \cap K = \{0\}$. A pointed, solid, and closed convex cone is *proper*.

Alizadeh, Chapter 2 Definition 1; Boyd, 2.4.1

Limiting your attention to proper cones can make life easier. A non-solid cone can be thought of as a solid cone (in a subspace) embedded in a space that's too large. A non-pointed cone is the sum of a vector subspace and some other pointed cone. In both cases, that extra vector space can kind-of be factored out, and usually isn't very interesting.

Let's see some non-trivial examples of convex cones.

Example 34 (nonnegative orthant)**.** The *nonnegative orthant* $\mathbb{R}^n_+$ in the real vector space $\mathbb{R}^n$ is

$$\mathbb{R}^n_+ \coloneqq \{x \in \mathbb{R}^n \mid \forall i \in \{1, 2, \ldots, n\} : x_i \geq 0\}.$$

In other words, $\mathbb{R}^n_+$ is the set of all vectors whose entries are all nonnegative. It is a cone, because if $x \in \mathbb{R}^n_+$ and if $\alpha \geq 0$, then every component of αx looks

like $\alpha x_i \geq 0$, so $\alpha x \in \mathbb{R}^n_+$. It is also convex, since if $x, y \in \mathbb{R}^n_+$ and $\alpha \in [0,1]$, then $\alpha x + (1-\alpha)\, y$ is the sum of two vectors with nonnegative entries, and thus has nonnegative entries itself. It is solid, since if $\{e_1, e_2, \ldots, e_n\}$ is the standard basis then $V = \operatorname{span}(\{e_1, e_2, \ldots, e_n\}) \subseteq \operatorname{span}\left(\mathbb{R}^n_+\right)$ because each $e_i \in \mathbb{R}^n_+$. It is pointed, since if x and $-x$ are both in $\mathbb{R}^n_+$, then they both have nonnegative entries. This implies that $x = 0$, showing that $-\mathbb{R}^n_+ \cap \mathbb{R}^n_+ = \{0\}$. Finally, $\mathbb{R}^n_+$ is closed as a subset of $\mathbb{R}^n$: this is the hardest property to prove. Recall that the intersection of closed sets is closed, and write

$$\mathbb{R}^n_+ = \bigcap_{i=1}^{n} H_i$$

where

$$H_i = \{x \in \mathbb{R}^n \mid x_i \geq 0\}$$

is the half-space corresponding to the ith dimension. If we can show that each H_i is closed, then Proposition 24 will tell us that $\mathbb{R}^n_+$ is, too. So, we have merely punted to showing that H_i is closed, but this is more tractable. One can verify that

$$H_i = f_i^{-1}([0, \infty])$$

where

$$\begin{aligned} f_i &: \mathbb{R}^n \to \mathbb{R} \\ f_i &= x \mapsto \langle x, e_i \rangle \end{aligned}$$

is pretty obviously continuous (it's linear). Since we know that $[0, \infty]$ is closed, the preimage definition of continuity tells us that H_i is, too.

Example 35 (Lorentz cone)**.** The *Lorentz cone* in the real vector space $\mathbb{R}^n$ is Boyd, Example 2.3

$$\mathcal{L}^n_+ \coloneqq \left\{ x \in \mathbb{R}^n \;\middle|\; x_1 \geq 0, \sqrt{x_2^2 + x_3^2 + \cdots + x_n^2} \leq x_1 \right\}.$$

You will also encounter this written in block-form,

$$\mathcal{L}^n_+ \coloneqq \left\{ (t, x) \in \left(\mathbb{R}_+, \mathbb{R}^{n-1}\right) \;\middle|\; \|x\| \leq t \right\}.$$

and with the name "ice cream cone" or "second-order cone." They all mean the same thing. The name "ice cream cone" is perhaps the most descriptive: if you think of t as being the height, then the condition that $\|x\| \leq t$ describes a disc of radius t. As t gets bigger (as we go higher up in the cone), the radius of the disc gets wider and wider. The resulting set looks just like an ice cream cone, so long as we agree to call the first coordinate the "up/down" direction.

Exercise 3. *Verify that $\mathcal{L}^n_+$ is a proper cone in $\mathbb{R}^n$. Use the sequential definition of a closed set if that makes things easier.* *Boyd, 2.2.3*

Example 36 (PSD cone)**.** Let $\mathcal{S}^n$ denote the subspace of symmetric matrices within the larger real vector space $\mathbb{R}^{n\times n}$. The positive-semidefinite (PSD) cone $\mathcal{S}^n_+$ in the real vector space $\mathcal{S}^n$ is Boyd, 2.2.5

$$\mathcal{S}^n_+ \coloneqq \{A \in \mathcal{S}^n \mid A \text{ is positive-semidefinite}\}.$$

We will leverage Proposition 20 to show that this is a proper cone. First note that if $A \in \mathcal{S}^n_+$ and if $\alpha \geq 0$, then the eigenvalues of A are nonnegative and of course the eigenvalues of αA are too (you just multiply the eigenvalues of A by α to get those of αA). Thus $\mathcal{S}^n_+$ is a cone. To see that it is convex, suppose that $A, B \in \mathcal{S}^n_+$, and apply the definition of positive-semidefiniteness to the convex combination $\alpha A + (1-\alpha) B$ with $\alpha \in [0,1]$:

$$\langle [\alpha A + (1-\alpha) B] x, x\rangle = \alpha \langle Ax, x\rangle + (1-\alpha)\langle Bx, x\rangle \geq 0.$$

Thus $\mathcal{S}^n_+$ is a convex cone. It is pointed because if A and $-A$ both belong to $\mathcal{S}^n_+$, then by Proposition 20 the eigenvalues of A are all zero; that is, $A = 0$. To see that it is solid, consider the following set,

$$\mathbf{b} = \left\{E_{ij} \coloneqq e_i e_j^T + e_i e_i^T + e_j e_j^T + e_j e_j^T \mid i, j \in \{1, 2, \ldots, n\}\right\}.$$

Each element of this set is positive-semidefinite:

$$\begin{aligned}
\langle E_{ij} x, x\rangle &= \langle e_i, x\rangle \langle e_i, x\rangle + 2\langle e_i, x\rangle \langle e_j, x\rangle + \langle e_j, x\rangle \langle e_j, x\rangle \\
&= x_i^2 + 2x_i x_j + x_j^2 \\
&= (x_i + x_j)^2 \\
&\geq 0.
\end{aligned}$$

The set $\mathbf{b}$ also spans $\mathcal{S}^n$. To see this, note that when $i = j$, the matrix $E_{ii} = 4e_i e_i^T$ is diagonal and is a scalar multiple of the standard basis element $e_i e_i^T$ for $\mathcal{S}^n$. When $i \neq j$, then

$$E_{ij} - E_{ii}/4 - E_{jj}/4 = e_i e_j^T + e_j e_i^T$$

gives us the off-diagonal standard basis elements for $\mathcal{S}^n$. Thus, the standard basis for $\mathcal{S}^n$ is contained in span $(\mathbf{b})$, and we have

$$\text{span}\left(\mathcal{S}^n_+\right) \supseteq \text{span}\,(\mathbf{b}) = \mathcal{S}^n$$

because every element of $\mathbf{b}$ was in $\mathcal{S}^n_+$.

Finally, $\mathcal{S}^n_+$ is closed. For any $x \in \mathbb{R}^n$, define

$$\begin{aligned}
f_x &: \mathcal{S}^n \to \mathbb{R} \\
f_x &= A \mapsto \langle Ax, x\rangle
\end{aligned}$$

and consider the set $f_x^{-1}([0,\infty])$. The function f_x is linear and thus continuous for all x, so this set is closed, and if we take the intersection over all $x \in \mathbb{R}^n$, we obtain (from the definition of positive-semidefinite)

$$\mathcal{S}^n_+ = \bigcap_{x\in\mathbb{R}^n} f^{-1}([0,\infty]).$$

The arbitrary intersection of closed sets is closed; thus $\mathcal{S}^n_+$ is closed.

Another approach is to use the fact that the function $\lambda : \mathcal{S}^n \to \mathbb{R}^n$ that takes a symmetric matrix to its vector of eigenvalues (in decreasing order, say) is continuous. Its continuity follows from the fact that the eigenvalues are roots of a characteristic polynomial function, and those roots depend continuously on the coefficients of the polynomial (which themselves depend continuously on the entries of the matrix) by Theorem 9. If you believe that, then we have already shown that $\mathbb{R}^n_+$ is closed in $\mathbb{R}^n$, and Proposition 20 says that $\mathcal{S}^n_+ = \lambda^{-1}\left(\mathbb{R}^n_+\right)$ from which it follows that $\mathcal{S}^n_+$ is closed.

The next definition is one of the most fundamental, even though it looks quite arbitrary at first.

Definition 48. If K is a subset of V, then the *dual cone* K^* of K is given by

$$K^* \coloneqq \{y \in V \mid \langle x, y\rangle \geq 0 \text{ for all } x \in K\}.$$

Alizadeh, Chapter 2 Definition 2; Boyd, 2.6.1

Here are a few useful facts about dual cones.

- The dual K^* is a closed convex cone for any subset $K \subseteq V$.
- If K is a convex cone, then $(K^*)^* = \operatorname{cl}(K)$.
- A subset $K \subseteq V$ is a closed convex cone in V if and only if $(K^*)^* = K$.
- A closed convex cone K is polyhedral if and only if its dual K^* is polyhedral.

It will take some experimentation to get a feel for the dual cone. It generally points "in the same direction" as the original cone; the bigger the original cone is, the smaller the dual is, and vice-versa. All vector subspaces are closed convex cones, and the dual of a vector subspace is its orthogonal complement. So, in a sense, the dual operation on cones generalizes the "perp" operation on subspaces.

Exercise 4. *Let W be a subspace of a finite-dimensional real inner-product space V. Prove that W is a closed convex cone in V, and that $W^* = W^\perp$.*

To understand why the dual is useful, imagine we are in the middle of an optimization algorithm, moving through some set defined by constraint functions, and sitting at the point x_0. Those constraint functions (if they are nice!), give rise to a convex cone K of feasible directions in which we can move. But what will happen to the value of the function f if we move in those directions? If $\nabla f(x_0)$ lies in K^*, then we can be sure that, at least locally, the function value will increase no matter what direction d we choose, because $\langle \nabla f(x_0), d\rangle \geq 0$ for all $d \in K$. If we're trying to minimize f, that means we found a local optimum!

Example 37. Recall the nonnegative orthant $\mathbb{R}^n_+$ from Example 34. This cone is *self-dual*, meaning that its dual cone is equal to itself. To demonstrate this, we will show that $x \in \left(\mathbb{R}^n_+\right)^*$ if and only if $x \in \mathbb{R}^n_+$.

First, suppose that $x \in \mathbb{R}^n_+$. Then for any $y \in \mathbb{R}^n_+$, we have $\langle x, y\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n \geq 0$, since each individual term x_iy_i is the product of two nonnegative real numbers. And since $\langle x, y\rangle \geq 0$ for all $y \in \mathbb{R}^n_+$, we have $x \in \left(\mathbb{R}^n_+\right)^*$ by definition.

On the other hand, suppose that $x \notin \mathbb{R}^n_+$, so that $x_i < 0$ for some i. Then we can choose $y = e_i \in \mathbb{R}^n_+$, the ith standard basis vector in $\mathbb{R}^n$, to show that $x \notin \left(\mathbb{R}^n_+\right)^*$. Specifically, we have $\langle x, y\rangle = \langle x, e_i\rangle = x_i < 0$ which would be nonnegative if x were in $\left(\mathbb{R}^n_+\right)^*$. So, it isn't.

SageMath can perform dual cone computations for us, so long as your cone is polyhedral.

```
sage: K = Cone([(1,0,0),(0,1,0),(0,0,1)])
sage: K.dual().rays()
M(1, 0, 0),
M(0, 1, 0),
M(0, 0, 1)
in 3-d lattice M
sage: K.dual().is_isomorphic(K)
True
```

Another fundamental example to keep in mind is the dual cone to a subspace, which turns out to be its orthogonal complement.

Example 38. Suppose that W is a subspace of a finite-dimensional real inner-product space V. Then W somewhat-obviously forms a closed convex cone, and it has a dual cone.

If $y \in W^\perp$, then clearly $\langle y, x\rangle = 0$ for all $x \in W$, and thus $y \in W^*$. This shows that $W^\perp \subseteq W^*$.

On the other hand, if $y \in W^*$, then

$$\begin{gathered}\forall x \in W : (\langle y, x\rangle \geq 0) \wedge (\langle y, -x\rangle \geq 0) \\ \iff \\ \forall x \in W : \langle y, x\rangle = 0\end{gathered}$$

where we have used the fact that $-x \in W$ as well whenever $x \in W$. This last statement says that $y \in W^\perp$, showing that $W^* \subseteq W^\perp$. Combining the two set inclusions gives us $W^* = W^\perp$.

Since all vector subspaces are closed convex cones, and since the dual cone of a vector subspace is its orthogonal complement, closed convex cones and their duals generalize subspaces and orthogonal complemenents. This is just one more way to think about closed convex cones.

5.3 Partially-ordered vector spaces

One important property of convex cones is that (under some additional constraints) they allow us to generalize the notion of an ordering, like "greater than or equal to." You may already have seen this used, for example, in $\mathbb{R}^n$, where $x \geq 0$ means that all components of the vector $x \in \mathbb{R}^n$ are individually nonnegative. That only works well because the set of vectors in $\mathbb{R}^n$ whose components are all nonnegative forms a particular type of convex cone.

Boyd 2.4.1; Roman, Preliminaries

Definition 49. A *partially-ordered set*, or *poset*, is a set P and a binary relation "$\preccurlyeq$" defined on P that satisfies three properties:

- Reflexivity: $\forall x \in P : x \preccurlyeq x$.
- Antisymmetry: $\forall x, y \in P : x \preccurlyeq y$ and $y \preccurlyeq x$ implies $x = y$.
- Transitivity: $\forall x, y, z \in P : x \preccurlyeq y$ and $y \preccurlyeq z$ implies $x \preccurlyeq z$.

A *partially-ordered vector space* is a real vector space $(V, \mathbb{R})$ along with a partial order $\preccurlyeq$ on V that satisfies two additional properties:

- Translation invariance: $\forall x, y, z \in V : x \preccurlyeq y \implies x + z \preccurlyeq y + z$.
- Scaling invariance: $\forall x, y \in V, \forall \alpha \in \mathbb{R} : x \preccurlyeq y$ and $\alpha \geq 0$ implies $\alpha x \preccurlyeq \alpha y$.

In either case, we define the "greater than or equal to" version by $y \succcurlyeq x \iff x \preccurlyeq y$.

Example 39. Let $X = \{1, 2, 3\} \subseteq \mathbb{N}$. The *powerset* of X is the set of all subsets of X,

$$\mathcal{P}(X) = \{\emptyset, \{1\}\{1,2\}, \{1,3\}, \{1,2,3\}, \{2\}, \{2,3\}, \{3\}, X\}.$$

The "is a subset of" relation forms a partial order on the powerset of X:

- Reflexivity: if $A \subseteq X$, then clearly $A \subseteq A$.
- Antisymmetry: if $A, B \subseteq X$ and if both $A \subseteq B$ and $B \subseteq A$, then $A = B$ from basic set theory.
- Transitivity: if $A, B, C \subseteq X$ and if $A \subseteq B$ and $B \subseteq C$, then again, from basic set theory, we know that $A \subseteq C$.

Example 40. Suppose that $\mathbb{F}$ is a field, and let $R \subseteq \mathbb{F}[X]$ be the set of all nonzero monic polynomials in $\mathbb{F}[X]$.

We say that a polynomial $p \in R$ divides another polynomial $s \in R$ and we write $p \mid s$ if and only if there exists some $q \in R$ such that $s = pq$. This relation is a partial order on the set R. Note that the multiplicative identity X^0 of $\mathbb{F}[X]$ also belongs to R. For clarity, we will write $1_R \coloneqq X^0$ when referring to it inside the set R.

For reflexivity, note that $p \mid p$ holds, since letting $q = 1_R$ gives $p = pq$.

For antisymmetry, suppose that both $p \mid s$ and $s \mid p$, so there exist some $q_1, q_2 \in R$ such that $s = pq_1$ and $p = sq_2$. Substituting the second identity into the first, we find that

$$s = sq_2q_1 \iff s(1_R - q_2q_1) = 0.$$

The fact that $\mathbb{F}$ is a field makes $\mathbb{F}[X]$ an integral domain by Theorem 10. In an integral domain, two non-zero elements cannot multiply to zero. Thus from $s(1_R - q_2q_1) = 0$ we infer that $q_2q_1 = 1_R$. Since $\deg(q_1q_2)$ is greater than or equal to the degree of either factor, we infer that $\deg(q_1) = \deg(q_2) = 0$. In other words, they consist of only one "constant" term each, and those two terms must be unity because both polynomials are monic. Thus, $q_1 = q_2 = 1_R$, and it follows that $s = pq_1 = p$. Antisymmetry is proved.

For transitivity, suppose that both $p \mid s$ and $s \mid t$. Then there exist $q_1, q_2 \in R$ such that $s = pq_1$ and $t = sq_2$. But then if we substitute the first identity into the second, we get $t = pq_1q_2$. Now we recall that the product of two monic polynomials is monic, so we have expressed t as a monic multiple of p.

Theorem 22. *If V is a finite-dimensional real vector space, then every proper cone K in V induces a vector-space ordering on V by $x \preccurlyeq_K y \iff y - x \in K$.*

Example 41. The usual notation $x \leq y$ for two vectors $x, y \in \mathbb{R}^n$ derives from a cone ordering. By definition, $x \leq y$ if and only if $0 \leq y - x$, or $y - x \geq 0$. But this is equivalent to $y - x \in \mathbb{R}^n_+$. Thus, the component-wise ordering is the cone ordering with $K = \mathbb{R}^n_+$:

$$x \leq y \iff x \preccurlyeq_{\mathbb{R}^n_+} y.$$

Exercise 12 (partiality of cone ordering). The ordering in Theorem 22 is, in general, only partial. That means that there exists some cone K in an appropriate vector space and two vectors x, y such that neither $x \preccurlyeq_K y$ nor $y \preccurlyeq_K x$. Find an example of this situation.

Exercise 13 (proof of cone ordering). Prove Theorem 22. Let V be a finite-dimensional real inner-product space, and let K be a pointed closed convex cone in V. Show that the relation $\preccurlyeq_K$ defined on $V \times V$ by

$$x \preccurlyeq_K y \iff y - x \in K$$

has the properties of reflexivity, antisymmetry, transitivity, translation invariance, and scaling invariance. This suffices to prove the theorem.

Next, prove that if $(x, y)_i$ is a sequence in $V \times V$ converging to $(\bar{x}, \bar{y})$, and if

$$x_i \preccurlyeq_K y_i \text{ for } i = 1, 2, \ldots$$

then $\bar{x} \preccurlyeq_K \bar{y}$. This last property shows that inequality holds if we "pass to the limit." These are all nice properties that we've come to expect from the usual "less than or equal to" ordering on $\mathbb{R}$.

In Exercise 13, you may have noticed that we did not require the cone K to be solid. When the cone has a nonempty interior, it can be used to define a strict version of the cone inequality via $x \prec_K y \iff y - x \in \operatorname{int}(K)$. This is another "nice to have" property of the ordering—and one possessed by the componentwise ordering induced by $\mathbb{R}^n_+$—but it isn't strictly (ha ha) necessary.

While we are on the topic of partially-ordered sets, it is an opportune time to introduce the concept of minimality, a notion that is central to optimization.

Definition 50. If P is a partially-ordered set under the relation $\preccurlyeq$, then $p \in P$ is a *minimal element* of P if and only if there does not exist a $q \in P$ such that both $q \neq p$ and $q \preccurlyeq p$.

If you have never seen the definition of "minimal" before, you might think that it means the same thing as "minimum." Au contraire, a minimal element is simply not bigger than anything else. For example, if no two distinct elements in the poset are related, then every element is minimal, because we never have $p \preccurlyeq q$ when $q \neq p$. A *minimum element* on the other hand, has to be smaller than *every* other element.

5.4 Solutions to exercises

Solution to Exercise 11 (cone convexity characterization). If K is convex, then

$$\forall x, y \in K : x + y = \frac{1}{2} \cdot 2x + \frac{1}{2} \cdot 2y \in \operatorname{conv}(\{2x, 2y\}) \subseteq \operatorname{conv}(K) = K.$$

On the other hand, if $x, y \in K$ implies that $x + y \in K$, then for any $\alpha \in [0, 1]$ we have

$$\underbrace{\alpha x}_{\in K} + \underbrace{(1 - \alpha)\, y}_{\in K} \in K.$$

Solution to Exercise 12 (partiality of cone ordering). The set $K = \{0\}$ forms a pointed closed convex cone in $\mathbb{R}^2$. The ordering associated with this cone is

$$x \preccurlyeq_K y \iff y - x \in \{0\} \iff y - x = 0 \iff x = y.$$

In $\mathbb{R}^2$, the standard basis vectors $e_1 = (1, 0)^T$ and $e_2 = (0, 1)^T$ are not equal; therefore neither $e_1 \preccurlyeq_K e_2$ nor $e_2 \preccurlyeq_K e_1$.

Solution to Exercise 13 (proof of cone ordering).

- Reflexivity: $x \preccurlyeq_K x \iff x - x \in K$, but $x - x = 0$ belongs to every cone: cones are nonempty by definition, which means that they contain at least one element z, and we can thus take $\alpha = 0$ in Definition 44 of a cone to conclude that $0z = 0 \in K$.

- Antisymmetry: if $x \preccurlyeq_K y$ and $y \preccurlyeq_K x$, then $y - x \in K$ and $x - y = -(y - x) \in K$, or $y - x \in -K$. Since K is pointed, the fact that $y - x \in -K \cap K$ implies that $y - x = 0$, or that $y = x$.

- Transitivity: If $x \preccurlyeq_K y$ and $y \preccurlyeq_K z$, then $y - x \in K$ and $z - y \in K$. Using the result from Exercise 11, we know that $z - x = (y - x) + (z - y)$ is back in K, since K is a convex cone.

- Translation invariance: if $x \preccurlyeq_K y$, then $y - x \in K$. However, $y - x = (y + z) - (x + z)$, so the result follows immediately.

- Scaling invariance: if $x \preccurlyeq_K y$ and if $\alpha \geq 0$, then $y - x \in K$ implies that $\alpha(y - x) \in K$, since K is a cone. But $\alpha(y - x) = \alpha y - \alpha x \in K$ means that $\alpha x \preccurlyeq_K \alpha y$.

- Ability to pass to the limit: suppose that $(x, y)_i$ is a sequence in $V \times V$ converging to $(\bar{x}, \bar{y})$, and that $x_i \preccurlyeq_K y_i$ for all $i \in \mathbb{N}$. From this we conclude that the components x_i and y_i of the pairs $(x, y)_i$ must converge individually to $\bar{x}$ and $\bar{y}$. (This is justified by the "Pythagorean theorem" in product spaces, which we discuss prior to Example 46 in a later chapter.)

  Now, let $s : V \times V \to V$ be the "subtract from" function defined by $s((a, b)) = b - a$. This function is always continuous in a finite-dimensional real space by Proposition 2, or by Theorem 1 because subtraction is continuous on $\mathbb{R}^n$.

  We can define a new sequence $(z)_i$ by $z_i := y_i - x_i = s((x_i, y_i))$. Note that each z_i belongs to K since $y_i \preccurlyeq_K x_i$. Thus if we take the limit,

$$\left(\lim_{i \to \infty} z_i\right) \in K,$$

  because K is a closed set. However, using the fact that the function s is continuous, we also have

$$\lim_{i \to \infty} z_i = \lim_{i \to \infty} s((x_i, y_i)) = s\left(\lim_{i \to \infty} (x_i, y_i)\right) = s((\bar{x}, \bar{y})) = \bar{y} - \bar{x},$$

  showing that $\bar{y} - \bar{x} \in K$. Or in other words, that $\bar{x} \preccurlyeq_K \bar{y}$.

Part II

Euclidean Jordan Algebras

Chapter 6

What are Euclidean Jordan algebras?

Definition 51. The algebra $(V, \mathbb{F}, \circ)$ is a *Jordan algebra* if $\mathbb{F}$ is not of characteristic two, and if the multiplication satisfies the two conditions,

- Commutativity: $\forall x, y \in V : x \circ y = y \circ x$, and
- The Jordan identity: $\forall x, y \in V : x \circ ((x \circ x) \circ y) = (x \circ x) \circ (x \circ y)$.

In that case, the algebra multiplication is called a *Jordan product*.

Warning 7: Jordan algebras are not associative

In general, Jordan algebras are *not* associative. There usually exist some elements x, y and z in the algebra such that $x \circ (y \circ z) \neq (x \circ y) \circ z$.

The "characteristic two" in Definition 51 is a technicality that prevents our algebra from being junk. In practice, we will always have $\mathbb{F} = \mathbb{R}$. And we'll be working in a more specific structure than Jordan algebras, namely a "formally-real Jordan algebra" or a "Euclidean Jordan algebra." These are the same thing, even though you will see both terms used with seemingly-different definitions.

Definition 52. A *formally-real* Jordan algebra $(V, \mathbb{R}, \circ)$ is a Jordan algebra over the reals where $(x \circ x) + (y \circ y) = 0$ implies that both $x = 0$ and $y = 0$.

Baes, Definition 2.2.9; Koecher, Section VI.4

Note that if we write $x \circ x$ as x^2, then the condition $x^2 + y^2 = 0 \implies x = y = 0$ is a condition that holds when x, y are real numbers but not when x, y are complex. This is where the name "formally-real" comes from.

Definition 53. A *Euclidean Jordan algebra*, or *EJA*, is a triple $(V, \circ, \langle \cdot, \cdot \rangle)$ consisting of a finite-dimensional Jordan algebra $(V, \mathbb{R}, \circ)$ over the real numbers, and an inner product that satisfies

Faraut and Korányi, Section III.1

$$\forall x, y, z \in V : \langle x \circ y, z \rangle = \langle y, x \circ z \rangle , \tag{6.1}$$

and a multiplicative unit element 1_V such that

$$\forall x \in V : 1_V \circ x = x = x \circ 1_V .$$

Some comments on this definition are in order. Historically, formally-real Jordan algebras were investigated first for their connection to quantum mechanics (see Section 6.1). But it turns out that every finite-dimensional formally-real Jordan algebra must have a unit element—this was proven back in 1934.

Theorem 23. *Every finite-dimensional formally-real Jordan algebra possesses a unit element.*

Theorem 5 of Jordan, von Neumann, and Wigner

It was later discovered that you can put a compatible inner-product on a finite-dimensional formally-real Jordan algebra, turning it into a Euclidean Jordan algebra and vice-versa.

Theorem 24. *A finite-dimensional real unital Jordan algebra is formally-real if and only if there exists some inner-product on it that satisfies Equation (6.1).*

Faraut and Korányi, Section III.1 and Proposition VIII.4.2

Our Definition 53 of a Euclidean Jordan algebra is thus "retconned" to include things that a finite-dimensional formally-real Jordan algebra must ultimately possess, without doing any of the work to prove it. This simplifies the presentation greatly. We have also included "finite-dimensional" in our definition of a Euclidean Jordan algebra. This is not entirely standard, but we make several excuses for our behavior:

1. If we don't impose finite-dimensionality, then the existence of a unit element is not clear, so we shouldn't include that either. From then on we would have to say "finite-dimensional unital Euclidean Jordan algebra" everywhere, which is objectionable from an aesthetic point of view.

2. The name "Euclidean"refers to a Euclidean space, which generally means a finite-dimensional real inner-product space. Insofar as is possible, we would like the name of a thing to describe what it is.

3. It's what all of our friends (particularly Faraut and Korányi) are doing. This argument would not convince your mother, but it's something.

Simplification 4: All EJAs are finite-dimensional

Any n-dimensional Euclidean Jordan algebra is also a finite-dimensional real inner-product space, and is therefore isometric to $\mathbb{R}^n$ by Theorem 1. As a result, continuity and sequences in Euclidean Jordan algebras work the same way that they do in $\mathbb{R}^n$. In particular, the Jordan multiplication $(x, y) \mapsto x \circ y$ will always be continuous by Proposition 5.

From now on, we will work only with Euclidean Jordan algebras as they are defined in Definition 53. Some of our results hold in a more general Jordan algebra, but for pedagogical reasons, we will always work in the simpler setting.

6.1 History

In 1932, the physicist Pascual Jordan (NOT Camille Jordan) set out to find an algebraic setting for quantum mechanics. Back then, the "Copenhagen model" said that physical observables are represented by Hermitian (or self-adjoint) matrices. The problem was, that many operations on Hermitian matrices turn out not to be observable; that is, they don't give you back a Hermitian matrix! For example, multiplication by an imaginary scalar:

$$\begin{aligned} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^* &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ \left(i \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right)^* &= \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \neq i \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{aligned}$$

Or matrix multiplication:

$$\begin{aligned} \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}^T \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^T \\ \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} &\neq \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}^T. \end{aligned} \tag{6.2}$$

So, Jordan tried to come up with an axiomatic system wherein doing things to observables was also observable. The big idea was that most operations of interest could be expressed in terms of quasi-multiplication that preserves

symmetry,

$$(A, B) \mapsto \frac{AB + BA}{2}.$$

For sure, if A, B are symmetric, then

$$\left(\frac{AB + BA}{2}\right)^T = \frac{(AB)^T + (BA)^T}{2} = \frac{B^T A^T + A^T B^T}{2} = \frac{BA + AB}{2}.$$

This product turns out not to be associative, but it does satisfy the "weak associativity" that we called the "Jordan identity," namely $x \circ \left(\left(x^2\right) \circ y\right) = \left(x^2\right) \circ (x \circ y)$, where we have taken the liberty of writing $x \circ x$ as x^2. So, Jordan made the weaker property one of the axioms of his system.

Another property that Jordan noticed is that, if you take the Hermitian matrices with the symmetriced product, then $X \circ X = X^2$, where the latter is squaring with respect to matrix multiplication. Thus $X^2 + Y^2 = 0$ can only be solved as $X^2 = -Y^2$. If, without loss of generality, the X^2 term is nonzero, then there is some vector v such that $X^2 v \neq 0$, and in particular $Xv \neq 0$. It follows that $\left\langle X^2 v, v \right\rangle = -\left\langle Y^2 v, v \right\rangle \iff \|Xv\|^2 = -\|Yv\|^2$ which is impossible because the left-hand side is strictly positive and the right-hand side is nonpositive, whatever it is. Thus, $X^2 = -Y^2 = 0$. This algebra is formally-real!

Jordan and his colleagues continued to study formally-real Jordan algebras. In 1934, Jordan, Wigner, and von Neumann proved that all finite-dimensional formally-real Jordan algebras (that is, Euclidean Jordan algebras) are constructed from only five basic building blocks. Only one of these does not come from an associative algebra equipped with the symmetrized product, and those are the kind that physicists were interested in. Moreover, the one good candidate only has dimension 27, and that's too small for quantum mechanics. This was disappointing: it means that—if we stick to finite dimensions—Jordan algebras weren't powerful enough to do the thing they were invented to do! Almost 50 years later, Efim Zel'manov (who won a related Fields medal) proved that there are no other simple "exceptional" Jordan algebras. So much for that.

All was not lost, however. In the early 1990s, barrier functions were becoming big deal in optimization because they led to efficient interior-point methods. Osman Güler at UMBC showed that certain nice barrier functions were intrinsic to symmetric cones [6], and recalled that every symmetric cone comes from a Euclidean Jordan algebra. Thus, Jordan algebras came back into the spotlight.

6.2 Fundamental examples

Example 42 (Hadamard EJA)**.** Let x and y be elements of the real vector space $\mathbb{R}^n$ with the standard basis and usual inner product. The *Hadamard product* of

x and y is defined by,

$$x \circ y = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \circ \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 y_1 \\ x_2 y_2 \\ \vdots \\ x_n y_n \end{bmatrix}.$$

In other words, it is the component-wise product of the entries of x and y.

The Hadamard product is bilinear and commutative, because multiplication of real numbers is bilinear and commutative, and we're doing that component-wise, which is also how equality is defined. It is associative for the same reason, and associativity implies that the "Jordan identity" holds. The condition in Equation (6.1) is easy to verify using the standard inner product on $\mathbb{R}^n$,

$$\langle x \circ y, z \rangle = \sum_{i=1}^{n} (x_i y_i) z_i = \sum_{i=1}^{n} y_i (x_i z_i) = \langle y, x \circ z \rangle .$$

Finally, the unit element 1_V in this algebra is $(1, 1, \ldots, 1)^T$, since

$$1_V \circ x = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \circ \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 1x_1 \\ 1x_2 \\ \vdots \\ 1x_n \end{bmatrix} = x,$$

regardless of what x is. So, $(\mathbb{R}^n, \circ, \langle \cdot, \cdot \rangle_{\mathbb{R}^n})$ is a Euclidean Jordan algebra.

Example 43 (Jordan Spin EJA)**.** Let x and y be elements of the real vector space $\mathbb{R}^n$ with the standard basis and usual inner product. For convenience, we will represent x and y in block form,

$$x = \begin{bmatrix} x_1 \\ \bar{x} \end{bmatrix}, \quad y = \begin{bmatrix} y_1 \\ \bar{y} \end{bmatrix},$$

with x_1, y_1 denoting the first components of x, y as usual, and $\bar{x}, \bar{y}$ denoting the remaining components. With that out of the way, we can define the product of x and y to be

$$x \circ y \coloneqq \begin{bmatrix} x_1 \\ \bar{x} \end{bmatrix} \circ \begin{bmatrix} y_1 \\ \bar{y} \end{bmatrix} = \begin{bmatrix} \langle x, y \rangle_{\mathbb{R}^n} \\ y_1 \bar{x} + x_1 \bar{y} \end{bmatrix}.$$

For example, in R^4, if we let $x = (1, 2, 3, 4)^T$ and $y = (1, 0, 1, 0)^T$, then, in block notation

$$x_1 = 1 \quad , \quad y_1 = 1,$$

$$\bar{x} = \begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix} \quad , \quad \bar{y} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix},$$

$$x \circ y \coloneqq \begin{bmatrix} \langle x, y \rangle_{\mathbb{R}^n} \\ y_1 \bar{x} + x_1 \bar{y} \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix} + 1 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \\ 4 \\ 4 \end{bmatrix}.$$

It's not hard to see that this multiplication is bilinear, and that along with $\langle \cdot, \cdot \rangle_{\mathbb{R}^n}$ it satisfies the three additional properties of a Euclidean Jordan algebra. The only difficulty is in the bookeeping of expressions like

$$x \circ x = \begin{bmatrix} \langle x, x \rangle \\ x_1 \bar{x} + x_1 \bar{x} \end{bmatrix} = \begin{bmatrix} \|x\|^2 \\ 2x_1 \bar{x} \end{bmatrix}$$

and

$$(x \circ x) \circ y = \begin{bmatrix} \left\langle \begin{bmatrix} \|x\|^2 \\ 2x_1 \bar{x} \end{bmatrix}, \begin{bmatrix} y_1 \\ \bar{y} \end{bmatrix} \right\rangle \\ y_1 \left(2x_1 \bar{x}\right) + \|x\|^2 \bar{y} \end{bmatrix} = \begin{bmatrix} \|x\|^2 y_1 + 2x_1 \langle \bar{x}, \bar{y} \rangle \\ y_1 \left(2x_1 \bar{x}\right) + \|x\|^2 \bar{y} \end{bmatrix}.$$

This Euclidean Jordan algebra is known as the *Jordan spin algebra*.

Exercise 14 (spin algebra unit). Let $(V, \circ, \langle \cdot, \cdot \rangle)$ be the Jordan Spin EJA, so that $V = \left(\mathbb{R}^{n-1} \times \mathbb{R}\right) \cong \mathbb{R}^n$ and $\langle \cdot, \cdot \rangle$ is the usual inner product. Find an element $e \in V$ such that for all $x \in V$, we have $x \circ e = e \circ x = x$. Conclude that $1_V = e$.

Exercise 15 (spin algebra properties).
Let $(V, \circ, \langle \cdot, \cdot \rangle)$ be the Jordan Spin EJA, and prove that the Jordan multiplication on V satisfies the four properties in Definitions 17, 51 and 53 necessary for $(V, \circ, \langle \cdot, \cdot \rangle)$ to form a Euclidean Jordan algebra:

1. Bilinearity,
2. Commutativity,
3. The Jordan identity $x \circ ((x \circ x) \circ y) = (x \circ x) \circ (x \circ y)$,
4. The inner-product compatibility condition $\langle x \circ y, z \rangle = \langle y, x \circ z \rangle$.

Example 44 (Real Symmetric EJA)**.** In the real vector space of real symmetric n-by-n matrices, the usual matrix product does not constitute an algebra product because multiplying two symmetric matrices may not give you back a symmetric matrix (see Inequality (6.2), for example). However, the "symmetrized product,"

$$X \circ Y \coloneqq \frac{XY + YX}{2},$$

does. This multiplication along with the inner product

$$\langle X, Y \rangle_{\mathcal{S}^n} \coloneqq \operatorname{trace}(XY)$$

forms a Euclidean Jordan algebra. To verify that claim, we have to check all of the properties. First, it is commutative:

$$X \circ Y = \frac{XY + YX}{2} = \frac{YX + XY}{2} = Y \circ X.$$

We check bilinearity after checking commutativity so that it need only be checked on one side:

$$\begin{aligned}(\alpha X + Y) \circ Z &= \frac{(\alpha X + Y) Z + Z (\alpha X + Y)}{2} \\ &= \frac{\alpha XZ + YZ + \alpha ZX + ZY}{2} \\ &= \alpha \frac{XZ + ZX}{2} + \frac{YZ + ZY}{2} \\ &= \alpha (X \circ Z) + (Y \circ Z).\end{aligned}$$

The Jordan identity is also satisfied:

$$\begin{aligned}X^2 \circ (X \circ Y) &= \frac{X^2 (X \circ Y) + (X \circ Y) X^2}{2} \\ &= \frac{X^2 (XY + YX) + (XY + YX) X^2}{4} \\ &= \frac{X^3Y + X^2YX + XYX^2 + YX^3}{4}, \\ X \circ \left(X^2 \circ Y\right) &= \frac{X \left(X^2 \circ Y\right) + \left(X^2 \circ Y\right) X}{2} \\ &= \frac{X \left(X^2Y + YX^2\right) + \left(X^2Y + YX^2\right) X}{4} \\ &= \frac{X^3Y + XYX^2 + X^2YX + YX^3}{4}.\end{aligned}$$

Finally, the inner-product condition in Equation (6.1) holds:

$$\begin{aligned}\langle X \circ Y, Z \rangle_{\mathcal{S}^n} &= \frac{\langle XY, Z \rangle_{\mathcal{S}^n} + \langle YX, Z \rangle_{\mathcal{S}^n}}{2} = \frac{\operatorname{trace}(XYZ) + \operatorname{trace}(YXZ)}{2}, \\ \langle Y, X \circ Z \rangle_{\mathcal{S}^n} &= \frac{\langle Y, XZ \rangle_{\mathcal{S}^n} + \langle Y, ZX \rangle_{\mathcal{S}^n}}{2} = \frac{\operatorname{trace}(YXZ) + \operatorname{trace}(YZX)}{2}.\end{aligned}$$

These expressions are in fact equal. By cancelling $\operatorname{trace}(YXZ)$ from both sides, it obviously comes down to showing that $\operatorname{trace}(XYZ) = \operatorname{trace}(YZX)$. This is a well-known trace identity, but it can now be deduced from something much more fundamental. If we let $YZ = A$, then all we're trying to show is that $\operatorname{trace}(AX) = \operatorname{trace}(XA)$. If you recall Theorem 21, the trace of a matrix is simply the sum of its eigenvalues. The set of eigenvalues (that is, the *spectrum*) of XA and AX are *always* the same (see for example Exercise 11 in Chapter 5 of Axler). Thus if we add them up, we also get the same thing.

Finally, we mention the somewhat-obvious fact that the unit element in this algebra is the identity matrix $I \in \mathcal{S}^n$, since

$$I \circ X = \frac{IX + XI}{2} = X = \frac{XI + IX}{2} = X \circ I.$$

Exercise 16 (nonassociativity of Real Symmetric EJA). Show that Jordan multiplication in the Real Symmetric EJA is not associative by finding an $n \in \mathbb{N}$ and three real symmetric matrices $X, Y, Z \in \mathcal{S}^n$ such that

$$(X \circ Y) \circ Z \neq X \circ (Y \circ Z).$$

A somewhat less fundamental example is the trivial Euclidean Jordan algebra. This algebra is fairly useless on its own, but it acts as a convenient sanity check on our definitions.

Example 45 (Trivial EJA)**.** Take $0 \in \mathbb{R}$ and construct the real zero-dimensional vector space $V = \{0\}$ on which we define the following:

$$\begin{aligned} \circ &= \text{const}_0, \\ \langle \cdot, \cdot \rangle &= \text{const}_0 . \end{aligned}$$

These two functions obviously satisfy the laws of a Euclidean Jordan algebra, because every element/product in the algebra is equal to every other element/product in the algebra, and they're all the real number zero. The same is true of the inner-products, so for example to check bilinearity we compute

$$\forall \alpha \in \mathbb{R}, \forall x, y, z \in V : (\alpha x + y) \circ z \coloneqq 0 = 0 \cdot 0 + 0 =: \alpha \, (x \circ z) + (y \circ z) \, .$$

Likewise for commutativity,

$$\forall x, y \in V : (x \circ y) \coloneqq 0 =: (y \circ x) \, ,$$

The inner-product compatibility condition,

$$\forall x, y \in V : \langle x \circ y, x \rangle \coloneqq 0 =: \langle y, x \circ z \rangle \, ,$$

and the Jordan identity:

$$\forall x, y \in V : x \circ ((x \circ x) \circ y) \coloneqq 0 =: (x \circ x) \circ (x \circ y).$$

Moreover, since $x = 0$ is the only element of V,

$$(0 \circ x) \coloneqq 0 = x = 0 =: (x \circ 0) \, ,$$

for all elements x of the algebra. Thus, $0 \in V$ serves as the unit element for this algebra. The structure $(\{0\}, \text{const}_0, \text{const}_0)$ is therefore an example of a Euclidean Jordan algebra, called the *trivial Euclidean Jordan algebra*.

One of the most important ways to construct a Euclidean Jordan algebra is as the Cartesian product of two other Euclidean Jordan algebras. But first let's talk about Cartesian products of inner-product spaces. If $(V, \mathbb{F})$ and $(W, \mathbb{F})$ are two vector spaces over the same field $\mathbb{F}$, then the Cartesian product $V \times W$ forms a vector space in an obvious way. If 0_V and 0_W are the zero elements in V and W respectively, then the zero vector in $V \times W$ is $(0_V, 0_W)^T$. Addition and scalar multiplication are defined component-wise. We have written addition and

scaling in V, W, and $V \times W$ all the same way, but keep in mind that they're all different things. If $\alpha \in \mathbb{F}$,

$$\begin{bmatrix} v_1 \\ w_1 \end{bmatrix} + \begin{bmatrix} v_2 \\ w_2 \end{bmatrix} \coloneqq \begin{bmatrix} v_1 + v_2 \\ w_1 + w_2 \end{bmatrix},$$
$$\alpha \begin{bmatrix} v \\ w \end{bmatrix} \coloneqq \begin{bmatrix} \alpha v \\ \alpha w \end{bmatrix}.$$

Equality in $V \times W$ is determined componentwise, and since the addition and scaling operations are both defined componentwise, the properties of a vector space are automatically fulfilled by this construction. If, in addition, there are two inner-products $\langle \cdot, \cdot \rangle_V$ and $\langle \cdot, \cdot \rangle_W$ defined on V and W, then we can use them to define an inner-product on $V \times W$, too:

$$\left\langle \begin{bmatrix} v_1 \\ w_1 \end{bmatrix}, \begin{bmatrix} v_2 \\ w_2 \end{bmatrix} \right\rangle_{V \times W} \coloneqq \langle v_1, v_2 \rangle_V + \langle w_1, w_2 \rangle_W .$$

The fact that this works is less obvious, but we can check that it works. First, it is linear in the first component:

$$\left\langle \alpha \begin{bmatrix} v_1 \\ w_1 \end{bmatrix} + \begin{bmatrix} v_2 \\ w_2 \end{bmatrix}, \begin{bmatrix} v_3 \\ w_3 \end{bmatrix} \right\rangle_{V \times W} \coloneqq \langle \alpha v_1 + v_2, v_3 \rangle_V + \langle \alpha w_1 + w_2, w_3 \rangle_W .$$

Now expanding and regrouping, we see that this is equal to

$$\begin{gathered} \alpha \langle v_1, v_3 \rangle_V + \langle v_2, v_3 \rangle_V + \alpha \langle w_1, w_3 \rangle_W + \langle w_2, w_3 \rangle_W \\ = \\ (\alpha \langle v_1, v_3 \rangle_V + \alpha \langle w_1, w_3 \rangle_W) + (\langle v_2, v_3 \rangle_V + \langle w_2, w_3 \rangle_W) \\ = \\ \alpha \left\langle \begin{bmatrix} v_1 \\ w_1 \end{bmatrix}, \begin{bmatrix} v_3 \\ w_3 \end{bmatrix} \right\rangle_{V \times W} + \left\langle \begin{bmatrix} v_2 \\ w_2 \end{bmatrix}, \begin{bmatrix} v_3 \\ w_3 \end{bmatrix} \right\rangle_{V \times W} . \end{gathered}$$

This proposed inner-product is also positive-definite. If $(v, w) \in V \times W$ is non-zero, then one of its components is non-zero. Thus, in

$$\left\langle \begin{bmatrix} v \\ w \end{bmatrix}, \begin{bmatrix} v \\ w \end{bmatrix} \right\rangle_{V \times W} \coloneqq \langle v, v \rangle_V + \langle w, w \rangle_W ,$$

one of the terms $\langle v, v \rangle_V$ or $\langle w, w \rangle_W$ must be non-zero (because those we know are inner-products, and thus are positive-definite). Finally, we check conjugate

symmetry:

$$\begin{aligned}\left\langle \begin{bmatrix} v_2 \\ w_2 \end{bmatrix}, \begin{bmatrix} v_1 \\ w_1 \end{bmatrix} \right\rangle_{V \times W} &\coloneqq \langle v_2, v_1 \rangle_V + \langle w_2, w_1 \rangle_W \\ &= \overline{\langle v_1, v_2 \rangle_V} + \overline{\langle w_1, w_2 \rangle_W} \\ &= \overline{\langle v_1, v_2 \rangle_V + \langle w_1, w_2 \rangle_W} \\ &= \overline{\left\langle \begin{bmatrix} v_1 \\ w_1 \end{bmatrix}, \begin{bmatrix} v_2 \\ w_2 \end{bmatrix} \right\rangle_{V \times W}}.\end{aligned}$$

Again this property holds in $V \times W$ because it held in V and W separately.

This inner-product has the additional nice property that it supplies a version of the Pythagorean theorem on the product space:

$$\left\| \begin{bmatrix} v \\ w \end{bmatrix} \right\|^2 = \left\langle \begin{bmatrix} v \\ w \end{bmatrix}, \begin{bmatrix} v \\ w \end{bmatrix} \right\rangle = \langle v, v \rangle_V + \langle w, w \rangle_W = \|v\|_V^2 + \|w\|_W^2 .$$

The method described above is the standard way to define inner-products on Cartesian product spaces. For example, the real numbers form a vector space over themselves (feel free to check this), and $\langle x, y \rangle_{\mathbb{R}} \coloneqq xy$ defines an inner-product on that space. We can see now that the usual inner-product on $\mathbb{R}^n$ is nothing other than n copies of the inner-product space $\mathbb{R}$, since, for example,

$$\left\langle \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \right\rangle_{\mathbb{R}^2} = x_1 y_1 + x_2 y_2 = \langle x_1, y_1 \rangle_{\mathbb{R}} + \langle x_2, y_2 \rangle_{\mathbb{R}} .$$

This technique can also be used to define a Cartesian product Euclidean Jordan algebra where the Jordan product is performed componentwise.

Example 46 (Cartesian Product EJA)**.** If $\left(V_1, \circ, \langle \cdot, \cdot \rangle_{V_1}\right)$ and $\left(V_2, \bullet, \langle \cdot, \cdot \rangle_{V_2}\right)$ are two Euclidean Jordan algebras, then we can define a Cartesian product algebra $(W, \star, \langle \cdot, \cdot \rangle_W)$ on the set $W \coloneqq V_1 \times V_2$ by,

$$\begin{aligned}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \star \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} &\coloneqq \begin{bmatrix} x_1 \circ y_1 \\ x_2 \bullet y_2 \end{bmatrix}, \\ \left\langle \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \right\rangle_W &\coloneqq \langle x_1, y_1 \rangle_{V_1} + \langle x_2, y_2 \rangle_{V_2} .\end{aligned}$$

The unit element in W is $1_W = (1_{V_1}, 1_{V_2})^T$.

Exercise 17 (Cartesian Product EJA properties). Give a heuristic argument why the multiplication in a Cartesian Product EJA should be bilinear, commutative, and satisfy the Jordan identity. Prove that the inner-product compatibility condition holds.

The Cartesian product algegras are some of the most important examples because it will turn out that every Euclidean Jordan algebra is isometric to some Cartesian product algebra where the factors can be of only five "simple" types. In fact, the Hadamard EJA on $\mathbb{R}^n$ is nothing more than a Cartesian product of n Jordan spin algebras where each spin algebra is on $\mathbb{R}$.

Definition 54. If $(V, \circ)$ is a Jordan algebra and if $x \in V$, then we define

$$\begin{aligned} L_x &: V \to V \\ L_x &= y \mapsto x \circ y \end{aligned}$$

to be the "left multiplication by x" operator.

Some people write $L(x)$ instead of L_x, but that leads to too many parentheses in some situations. In a more general setting, we would also need a "right multiplication by x" operator; however Definition 51 says that left-multiplication-by-x is the same thing as right-multiplication-by-x. So, we can get away with only one.

Proposition 25. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then L_x is a self-adjoint linear operator on V. Moreover, for any $\alpha \in \mathbb{R}$ and $x, y \in V$, we have $L_{(x+\alpha y)} = L_x + \alpha L_y$; the map $x \mapsto L_x$ is linear.*

Proof. In an algebra, the "multiplication" operation is always bilinear. Thus, L_x is linear,

$$L_x(\alpha y + z) \coloneqq x \circ (\alpha y + z) = \alpha (x \circ y) + x \circ z = \alpha L_x(y) + L_x(z),$$

and the fact that L_x is self-adjoint is an axiom stated in Equation (6.1).

To show that $L_{(x+\alpha y)} = L_x + \alpha L_y$ for any $\alpha \in \mathbb{R}$ and $x, y \in V$, we apply it to an arbitrary $z \in V$ and use the bilinearity of the multiplication:

$$L_{(x+\alpha y)}(z) \coloneqq (x + \alpha y) \circ z = x \circ z + \alpha (y \circ z) = L_x(z) + \alpha L_y(z).$$

In the algebra of functions $\mathcal{B}(V)$, this means that $L_{(x+\alpha y)} = L_x + \alpha L_y$. □

Corollary 9. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra with orthonormal basis $\mathbf{b}$ and if $x \in V$, then the matrix of L_x with respect to $\mathbf{b}$ is symmetric.*

Proof. Follows directly from Proposition 25 and Proposition 18. □

Example 47. In the Jordan identity, we can write

$$\begin{aligned} (x \circ y) &= L_x(y), \\ (x \circ x) \circ (x \circ y) &= L_{x^2}(L_x(y)) \end{aligned}$$

and

$$\begin{aligned} (x \circ x) \circ y &= L_{x^2}(y) \\ x \circ ((x \circ x) \circ y) &= L_x(L_{x^2}(y)) \end{aligned}$$

to conclude that

$$\forall y \in V : L_{x^2}\left(L_x\left(y\right)\right) = L_x\left(L_{x^2}\left(y\right)\right)$$
$$\iff$$
$$L_{x^2}L_x = L_xL_{x^2} \text{ as functions.}$$

Thus the Jordan identity is really only saying that two particular linear operators commute in the algebra of linear operators (Example 8), where the "multiplication" is function composition.

Here, and from now on, we denote the composition of linear operators by juxtaposition (putting them next to each other). This is to avoid confusion between the usual composition symbol and the Jordan product.

The use of L_x to denote left-multiplication by a fixed element x makes it easier for us to study another type of commutativity in Euclidean Jordan algebras, one that we're not always guaranteed to have.

Definition 55. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, then we say that $x, y \in V$ *operator-commute* if $L_xL_y = L_yL_x$.

In Example 47, we have thus shown that x and x^2 operator-commute.

Warning 8: The meaning of commutativity

Beware that some authors say only "x and y commute" instead of "x and y operator-commute" when they mean that $L_xL_y = L_yL_x$. That is far too easy to confuse with the Jordan-product commutativity guaranteed by Definition 51, however; so we will always say "operator-commute" when referring to the commutativity of the operators.

Exercise 18 (center of an EJA). If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, then the *center of the algebra* is denoted by $Z\left(V\right)$ and is the set of elements that operator-commute with everything else,

$$Z\left(V\right) \coloneqq \left\{z \in V \mid \forall x \in V : L_zL_x = L_xL_z\right\}.$$

To gain some familiarity with working in Euclidean Jordan algebras, let's prove a few easy facts about the center of an algebra.

1. First suppose that $z \in Z\left(V\right)$ that $u, v \in V$, and show that $u \circ \left(z \circ v\right) = z \circ \left(u \circ v\right)$.

2. Next suppose that $z \in Z(V)$ and that $u, v \in V$, and show that $v \circ (z \circ u) = z \circ (u \circ v)$.

3. Combine the previous two items to show that if $z \in Z(V)$ then we have $L_{(u \circ z)} = L_u L_z$.

4. Show that Jordan multiplication is associative on $Z(V)$ by picking any $x, y, z \in Z(V)$ and showing that $x \circ (y \circ z) = (x \circ y) \circ z$.

Another important practical fact is that we can apply our knowledge of linear algebra to compute the Jordan product.

Proposition 26. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra, then its multiplication is completely described by a set of n matrices, each of which has size $n \times n$.*

Proof. Let $\{e_1, e_2, \ldots, e_n\}$ be a basis for V. Definition 17 tells us that the Jordan product $\circ$ is bilinear, so in the expression $x \circ y$, we can express x and y in terms of our basis and then expand using bilinearity:

$$x \circ y = \left(\sum_{i=1}^{n} x_i e_i \right) \circ \left(\sum_{j=1}^{n} y_j e_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j (e_i \circ e_j) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j L_{e_i}(e_j).$$

Now each L_{e_i} for $i \in \{1, 2, \ldots, n\}$ is a linear operator on V, and thus has a representation as an $n \times n$ matrix with respect to the given basis. And there are of course n such operators/matrices. □

Thus we can compute the Jordan product fairly easily, assuming that we know its "multiplication table" consisting of the matrices $\{L_{e_i} \mid i = 1, 2, \ldots, n\}$. The same trick actually works for any algebra, not just a Jordan algebra.

Example 48. In the Hadamard EJA with the standard basis,

$$e_i \circ e_j = \begin{cases} e_i & \text{if i = j,} \\ 0 & \text{otherwise.} \end{cases}$$

and we can use this to compute the "multiplication table" from Proposition 26:

$$L_{e_i} = e_i e_i^T \text{ for } i = 1, 2, \ldots, n.$$

SageMath makes it pretty easy to implement these finite-dimensional algebras where we know how to multiply basis elements. It's not strictly necessary, but to emphasize Proposition 26 we will define the multiplication using the table above.

```
sage: class HadamardR3(CombinatorialFreeModule):
....:     def __init__(self):
....:         cat = FiniteDimensionalAlgebrasWithBasis(QQ)
....:         gens = range(3)
....:         super(HadamardR3,self).__init__(QQ,
....:                                         gens,
....:                                         category=cat)
....:     def product_on_basis(self,i,j):
....:         ei = self.monomial(i).to_vector()
....:         ej = self.monomial(j).to_vector()
....:         Lei = ei.column()*ei.row()
....:         return self.from_vector(Lei*ej)
sage: J = HadamardR3()
sage: x = J.from_vector(vector([1,3,8]))
sage: y = J.from_vector(vector([5,2,1]))
sage: (x*y).to_vector()
(5, 6, 8)
```

The incomprehensible stuff here is mostly boilerplate. We're creating a class that happens to be a free module, and then telling SageMath that it's also a finite-dimensional algebra by way of specifying the category. We use the field of rational numbers instead of the reals because real numbers and computers don't mix. But after that, we just tell it how to multiply basis elements, and we can convert coordinate vectors to algebra elements and multiply them.

Exercise 5. *Compute the multiplication table for the Jordan Spin EJA on $\mathbb{R}^3$. Write a function in your favorite programming language that performs Jordan multiplication based on a multiplication table (list of matrices), and use it to test your answer.*

What we've just done will be a major theme for the rest of the course. If we need to prove a theorem or define a concept in a Jordan algebra, we'll first either translate to, or reason by analogy with, basic linear algebra. Then when we've got what we want, we'll convert back to the Jordan algebraic setting.

6.3 Solutions to exercises

Solution to Exercise 14 (spin algebra unit). If we try to solve $x \circ e = x$ for all x, then we arrive at a system of equations in the n variables $e_1, e_2, \ldots, e_n$:

$$\begin{bmatrix} \langle x, e \rangle \\ x_1 \bar{e} + e_1 \bar{x} \end{bmatrix} = \begin{bmatrix} x_1 \\ \bar{x} \end{bmatrix}.$$

In particular this holds for $x = (1, 0, 0, \ldots, 0)^T$, and substituting that choice into the system gives

$$\begin{bmatrix} e_1 \\ \bar{e} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

A quick check shows that $e = (1, 0, 0, \ldots, 0)^T$ is indeed a unit element for this algebra.

Solution to Exercise 15 (spin algebra properties). First we note that the multiplication is commutative, because then it's easier to show bilinearity. We need only the fact that $\langle x, y \rangle = \langle y, x \rangle$ in $\mathbb{R}^n$, and the commutativity of vector addition:

$$x \circ y \coloneqq \begin{bmatrix} \langle x, y \rangle \\ x_1 \bar{y} + y_1 \bar{x} \end{bmatrix} = \begin{bmatrix} \langle y, x \rangle \\ y_1 \bar{x} + x_1 \bar{y} \end{bmatrix} =: y \circ x.$$

Now we show that the multiplication is bilinear. Suppose that $\alpha \in \mathbb{R}$. By definition,

$$(\alpha x + y) \circ z \coloneqq \begin{bmatrix} \langle \alpha x + y, z \rangle \\ z_1 \overline{(\alpha x + y)} + (\alpha x + y)_1 \bar{z} \end{bmatrix}$$

Since indexing is a linear operation on $\mathbb{R}^n$; that is, since $(\alpha x + y)_i = \alpha x_i + y_i$, we have for example

$$\overline{(\alpha x + y)}_i = (\alpha x + y)_{i+1} = \alpha x_{i+1} + y_{i+1} = \alpha \bar{x}_i + \bar{y}_i.$$

Thus the "bar" operation is linear too. It follows that

$$(\alpha x + y) \circ z = \begin{bmatrix} \alpha \langle x, z \rangle + \langle y, z \rangle \\ \alpha z_1 \bar{x} + z_1 \bar{y} + \alpha x_1 \bar{z} + y_1 \bar{z} \end{bmatrix} = \alpha (x \circ z) + (y \circ z).$$

Since we have already shown that our multiplication is commutative, linearity in the second argument follows from linearity in the first.

The inner-product compatibility condition is straightforward,

$$\begin{aligned}
\langle x \circ y, z \rangle = \left\langle \begin{bmatrix} \langle x, y \rangle \\ x_1 \bar{y} + y_1 \bar{x} \end{bmatrix}, \begin{bmatrix} z_1 \\ \bar{z} \end{bmatrix} \right\rangle &= z_1 \langle x, y \rangle + \langle x_1 \bar{y} + y_1 \bar{x}, \bar{z} \rangle \\
&= z_1 \langle x, y \rangle + x_1 \langle \bar{y}, \bar{z} \rangle + y_1 \langle \bar{x}, \bar{z} \rangle \\
&= x_1 y_1 z_1 + z_1 \langle \bar{x}, \bar{y} \rangle + x_1 \langle \bar{y}, \bar{z} \rangle + y_1 \langle \bar{x}, \bar{z} \rangle; \\
\langle y, x \circ z \rangle = \left\langle \begin{bmatrix} y_1 \\ \bar{y} \end{bmatrix}, \begin{bmatrix} \langle x, z \rangle \\ x_1 \bar{z} + z_1 \bar{x} \end{bmatrix} \right\rangle &= y_1 \langle x, z \rangle + \langle \bar{y}, x_1 \bar{z} + z_1 \bar{x} \rangle \\
&= y_1 \langle x, z \rangle + x_1 \langle \bar{y}, \bar{z} \rangle + z_1 \langle \bar{y}, \bar{x} \rangle \\
&= y_1 x_1 z_1 + y_1 \langle \bar{x}, \bar{z} \rangle + x_1 \langle \bar{y}, \bar{z} \rangle + z_1 \langle \bar{y}, \bar{x} \rangle.
\end{aligned}$$

Finally, we check the Jordan identity using the inner-product compatibility

condition and the identity $\langle x, y\rangle = x_1 y_1 + \langle \bar{x}, \bar{y}\rangle$:

$$
\begin{aligned}
x \circ x &\coloneqq \begin{bmatrix} \|x\|^2 \\ 2x_1\bar{x} \end{bmatrix} \\
(x \circ x) \circ y &\coloneqq \begin{bmatrix} \langle x \circ x, y\rangle \\ 2y_1x_1\bar{x} + \|x\|^2 \bar{y} \end{bmatrix} \\
x \circ ((x \circ x) \circ y) &\coloneqq \begin{bmatrix} \langle x, (x \circ x) \circ y\rangle \\ \left(\|x\|^2 y_1 + 2x_1 \langle \bar{x}, \bar{y}\rangle\right) \bar{x} + x_1 \left(2y_1x_1\bar{x} + \|x\|^2 \bar{y}\right) \end{bmatrix} \\
&= \begin{bmatrix} \langle (x \circ x) \circ x, y\rangle \\ \|x\|^2 y_1\bar{x} + 2x_1 \langle \bar{x}, \bar{y}\rangle \bar{x} + 2x_1^2 y_1\bar{x} + x_1 \|x\|^2 \bar{y} \end{bmatrix} \\
(x \circ x) \circ (x \circ y) &\coloneqq \begin{bmatrix} \langle x \circ x, x \circ y\rangle \\ \|x\|^2 (x_1\bar{y} + y_1\bar{x}) + \langle x, y\rangle 2x_1\bar{x} \end{bmatrix} \\
&= \begin{bmatrix} \langle x \circ (x \circ x), y\rangle \\ \\ \|x\|^2 x_1\bar{y} + y_1 \|x\|^2 \bar{x} + 2x_1^2 y_1\bar{x} + 2x_1 \langle \bar{x}, \bar{y}\rangle \bar{x}. \end{bmatrix}
\end{aligned}
$$

Solution to Exercise 16 (nonassociativity of Real Symmetric EJA).

```
sage: def jp(A,B):
....:   return (A*B + B*A)/2
sage: X = matrix([ [0,0],
....:              [0,1] ])
sage: Y = matrix([ [ 0,-1],
....:              [-1,-1] ])
sage: Z = matrix([ [0, 1],
....:              [1, 0] ])
sage: jp(jp(X,Y),Z)
[-1/2 -1/2]
[-1/2 -1/2]
sage: jp(X,jp(Y,Z))
[   0 -1/4]
[-1/4   -1]
```

Solution to Exercise 17 (Cartesian Product EJA properties). Scalar multiplication, addition, and equality are all defined componentwise in a Carte-

sian product space. So, for example, asking if

$$\begin{aligned}\alpha\left(\begin{bmatrix}x_1\\x_2\end{bmatrix}+\begin{bmatrix}y_1\\y_2\end{bmatrix}\right)\star\begin{bmatrix}z_1\\z_2\end{bmatrix} &= \begin{bmatrix}\alpha\left(x_1+y_1\right)\circ z_1\\ \alpha\left(x_2+y_2\right)\bullet z_2\end{bmatrix}\\ &= \alpha\left(\begin{bmatrix}x_1\\x_2\end{bmatrix}\star\begin{bmatrix}z_1\\z_2\end{bmatrix}\right)+\left(\begin{bmatrix}y_1\\y_2\end{bmatrix}\star\begin{bmatrix}z_1\\z_2\end{bmatrix}\right)\\ &= \alpha\begin{bmatrix}x_1\circ z_1\\x_2\bullet z_2\end{bmatrix}+\begin{bmatrix}y_1\circ z_1\\y_2\bullet z_2\end{bmatrix}\end{aligned}$$

is quite literally just asking if both $\circ$ and $\bullet$ are linear in the first component—which of course they are, because they're the algebra multiplication operations in two Euclidean Jordan algebras. Likewise, the commutativity and weak associativity will be satisfied automatically because you would check them componentwise, and they hold componentwise. The only thing that needs to be checked is the inner-product compatibility condition:

$$\begin{aligned}\left\langle\begin{bmatrix}x_1\\x_2\end{bmatrix}\star\begin{bmatrix}y_1\\y_2\end{bmatrix},\begin{bmatrix}z_1\\z_2\end{bmatrix}\right\rangle_W &\coloneqq \left\langle x_1\circ y_1, z_1\right\rangle_{V_1}+\left\langle x_2\bullet y_2, z_2\right\rangle_{V_2}\\ &= \left\langle y_1, x_1\circ z_1\right\rangle_{V_1}+\left\langle y_2, x_2\bullet z_2\right\rangle_{V_2}\\ &= \left\langle\begin{bmatrix}y_1\\y_2\end{bmatrix},\begin{bmatrix}x_1\\x_2\end{bmatrix}\star\begin{bmatrix}z_1\\z_2\end{bmatrix}\right\rangle_W,\end{aligned}$$

where the innermost equality holds because the inner-product compatibility condition is satisfied separately for $\circ$ in V_1 and for $\bullet$ in V_2.

Solution to Exercise 18 (center of an EJA).

1. Apply the definition of L_u and L_z and use the fact that they commute:

$$u\circ(z\circ v)=L_u\left(L_z\left(v\right)\right)=L_z\left(L_u\left(v\right)\right)=z\circ(u\circ v).$$

2. Same trick. Apply the definitions, and use the fact that L_z and L_v commute,

$$v\circ(z\circ u)=L_v\left(L_z\left(u\right)\right)=L_z\left(L_v\left(u\right)\right)=z\circ(v\circ u).$$

3. In the first item we found

$$u\circ(z\circ v)=z\circ(u\circ v),$$

but multiplication is commutative in a Euclidean Jordan algebra, so this is equivalent to

$$u\circ(z\circ v)=z\circ(v\circ u).$$

Now in the second item, we showed that

$$v\circ(z\circ u)=z\circ(v\circ u).$$

Since the right-hand sides of these equations are the same, the left-hand sides are too. Thus,

$$u \circ (z \circ v) = v \circ (z \circ u).$$

Rearranging once more using the commutativity of the Jordan multiplication, we wind up with,

$$u \circ (z \circ v) = (u \circ z) \circ v,$$

which says (in other words) that

$$L_u L_z (v) = L_{(u \circ z)} (v).$$

Since that holds for an arbitrary $v \in V$, the two linear operators $L_u L_z$ and $L_{(u \circ z)}$ are equal.

4. Again this follows from the commutativity of x, y, z and L_x, L_y, L_z:

$$\begin{aligned} x \circ (y \circ z) &= x \circ (z \circ y) \\ &= L_x L_z (y) \\ &= L_z L_x (y) \\ &= z \circ (x \circ y) \\ &= (x \circ y) \circ z. \end{aligned}$$

Chapter 7

Power-associativity and polarization

The big problem we face in a Jordan algebra is that it's just really hard to do anything without associativity. For example, we've used the notation $x^2 \coloneqq x \circ x$ to denote the Jordan product of x with itself. You might think it's safe to write x^3 to mean $x \circ x \circ x$, but a priori the expression $x \circ x \circ x$ is meaningless! It could be either $x \circ (x \circ x)$ or $(x \circ x) \circ x$, and they may not be the same thing. Thus the parentheses are required, and we can't even write a simple power like x^3 using what we know now. This causes some problems:

- Nilpotent operators are defined in terms of powers of themselves.
- Minimal and characteristic polynomials are all about powers of operators.
- Generalized eigenvalues involve powers of their operator.

Et cetera. And all we have to work with is the Jordan identity, which is equivalent to $L_x L_{x^2} = L_{x^2} L_x$. How can we leverage this? Fortunately, the left-multiplication operators are linear, and this lets us do some tricks.

7.1 Polarization identities

Proposition 27. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra, then*

$$\forall x, y \in V : 2L_x L_{(x \circ y)} + L_y L_{x^2} = 2L_{(x \circ y)} L_x + L_{x^2} L_y. \tag{7.1}$$

Koecher, Chapter III; Faraut and Korányi, Proposition II.1.1.i; Baes, Section 2.2.3

Proof. Let $z = x + ty$ for some $t \in \mathbb{R}$, and substitute into the Jordan identity:

$$\begin{gathered} \forall z \in V : L_z L_{z^2} = L_{z^2} L_z \\ \iff \\ \forall x, y \in V, \forall t \in \mathbb{R} : L_{(x+ty)} L_{(x+ty)^2} = L_{(x+ty)^2} L_{(x+ty)}. \end{gathered}$$

Now use Proposition 25 to expand,

$$\begin{aligned} L_{(x+ty)} &= L_x + tL_y \\ L_{(x+ty)^2} &= L_{(x^2+2t(x\circ y)+t^2y^2)} = L_{x^2} + 2tL_{(x\circ y)} + t^2L_{y^2}, \end{aligned}$$

and to get (for all x, y and t)

$$\begin{gathered} \left(L_x + tL_y\right)\left(L_{x^2} + 2tL_{(x\circ y)} + t^2L_{y^2}\right) = \left(L_{x^2} + 2tL_{(x\circ y)} + t^2L_{y^2}\right)\left(L_x + tL_y\right) \\ \iff \\ L_xL_{x^2} + 2tL_xL_{(x\circ y)} + t^2L_xL_{y^2} + tL_yL_{x^2} + 2t^2L_yL_{(x\circ y)} + t^3L_yL_{y^2} \\ = \\ L_{x^2}L_x + 2tL_{(x\circ y)}L_x + t^2L_{y^2}L_x + tL_{x^2}L_y + 2t^2L_{(x\circ y)}L_y + t^3L_{y^2}L_y. \end{gathered}$$

Are we having fun yet? We can now cancel $L_xL_{x^2} = L_{x^2}L_x$ and $t^3L_yL_{y^2} = t^3L_{y^2}L_y$ from both sides using the Jordan identity, which leaves

$$\begin{gathered} 2tL_xL_{(x\circ y)} + t^2L_xL_{y^2} + tL_yL_{x^2} + 2t^2L_yL_{(x\circ y)} \\ = \\ 2tL_{(x\circ y)}L_x + t^2L_{y^2}L_x + tL_{x^2}L_y + 2t^2L_{(x\circ y)}L_y. \end{gathered}$$

If we group by the coefficients t and t^2, this is the same thing as

$$\begin{gathered} \forall x, y \in V, \forall t \in \mathbb{R} : \\ t\left(2L_xL_{(x\circ y)} + L_yL_{x^2} - 2L_{(x\circ y)}L_x - L_{x^2}L_y\right) \\ = \\ -t^2\left(2L_yL_{(x\circ y)} + L_xL_{y^2} - 2L_{(x\circ y)}L_y - L_{y^2}L_x\right). \end{gathered}$$

If our conclusion is false, then there exist some $\tilde{x}, \tilde{y}$ that make it false. But then we could take norms on both sides—that is, we could set,

$$\begin{aligned} n_1 &\coloneqq \left\|2L_{\tilde{x}}L_{(\tilde{x}\circ\tilde{y})} + L_{\tilde{y}}L_{\tilde{x}^2} - 2L_{(\tilde{x}\circ\tilde{y})}L_{\tilde{x}} - L_{\tilde{x}^2}L_{\tilde{y}}\right\| \\ n_2 &\coloneqq \left\|2L_{\tilde{y}}L_{(\tilde{x}\circ\tilde{y})} + L_{\tilde{x}}L_{\tilde{y}^2} - 2L_{(\tilde{x}\circ\tilde{y})}L_{\tilde{y}} - L_{\tilde{y}^2}L_{\tilde{x}}\right\| \end{aligned}$$

and conclude that

$$\forall t \in \mathbb{R} : tn_1 = t^2n_2$$

where $n_1 \neq 0$ if our conclusion is false. By choosing two particular values ($t = 1$ and $t = 2$) of t, we can easily see that this is impossible:

$$\begin{aligned} n_1 &= n_2 \quad (\text{for } t = 1) \\ 2n_1 &= 4n_2 \ (\text{for } t = 2). \end{aligned}$$

Thus we must have $n_1 = 0$, and the conclusion follows. □

Proposition 28. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, then for all $x, y, z \in V$ we have*

$$L_xL_{(z\circ y)} + L_zL_{(x\circ y)} + L_yL_{(x\circ z)} = L_{(z\circ y)}L_x + L_{(x\circ y)}L_z + L_{(x\circ z)}L_y. \tag{7.2}$$

Faraut and Korányi, Proposition II.1.1.ii; Baes, Section 2.3.3

Proof. Replace x by $(x+z)$ in Proposition 27,

$$\forall x,y,z \in V : 2L_{(x+z)}L_{((x+z)\circ y)} + L_y L_{(x+z)^2} = 2L_{((x+z)\circ y)}L_{(x+z)} + L_{(x+z)^2}L_y$$

and expand,

$$\begin{gathered}2L_xL_{(x\circ y)} + 2L_xL_{(z\circ y)} + 2L_zL_{(x\circ y)} + 2L_zL_{(z\circ y)} + L_yL_{x^2} + 2L_yL_{(x\circ z)} + L_yL_{z^2} \\ = \\ 2L_{(x\circ y)}L_x + 2L_{(z\circ y)}L_x + 2L_{(x\circ y)}L_z + 2L_{(z\circ y)}L_z + L_{x^2}L_y + 2L_{(x\circ z)}L_y + L_{z^2}L_y\end{gathered}$$

There are a few terms above that only involve two variables; cancel them using Equation (7.1) (and divide everything by two) to obtain

$$L_xL_{(z\circ y)} + L_zL_{(x\circ y)} + L_yL_{(x\circ z)} = L_{(z\circ y)}L_x + L_{(x\circ y)}L_z + L_{(x\circ z)}L_y$$

as desired. □

Equation (7.2) is special because the right-hand side, when applied to some $w \in V$, becomes a symmetric expression in x,y,z,w. We can thus permute those variables to derive even more polarization identities. For example,

Proposition 29. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, then for all $y,z,u \in V$ we have*

Baes, Section 2.3.3

$$L_uL_{(z\circ y)} + L_zL_{(u\circ y)} + L_yL_{(u\circ z)} = L_{(u\circ(y\circ z))} + L_yL_uL_z + L_zL_uL_y. \tag{7.3}$$

Proof. Let $x = u$ on both sides of Equation (7.2) and apply them to w:

$$\forall u,z,y,w \in V : \begin{cases} u\circ((z\circ y)\circ w) + z\circ((u\circ y)\circ w) + y\circ((u\circ z)\circ w) \\ = \\ (z\circ y)\circ(u\circ w) + (u\circ y)\circ(z\circ w) + (u\circ z)\circ(y\circ w)\end{cases}$$

Now let $x = w$ on both sides of Equation (7.2) and apply them to u:

$$\forall u,z,y,w \in V : \begin{cases} w\circ((z\circ y)\circ u) + z\circ((w\circ y)\circ u) + y\circ((w\circ z)\circ u) \\ = \\ (z\circ y)\circ(w\circ u) + (w\circ y)\circ(z\circ u) + (w\circ z)\circ(y\circ u).\end{cases}$$

The right-hand sides of these expressions are equal, so the left-hand sides are too!

$$\forall u,z,y,w \in V : \begin{cases} \left[L_uL_{(z\circ y)} + L_zL_{(u\circ y)} + L_yL_{(u\circ z)}\right](w) \\ = \\ w\circ((z\circ y)\circ u) + z\circ((w\circ y)\circ u) + y\circ((w\circ z)\circ u).\end{cases}$$

Now we use commutativity to rearrange the latter expression until it looks like something acting on w,

$$\forall u,z,y,w \in V : \begin{cases} w\circ((z\circ y)\circ u) + z\circ((w\circ y)\circ u) + y\circ((w\circ z)\circ u) \\ = \\ \left[L_{((z\circ y)\circ u)} + L_zL_uL_y + L_yL_uL_z\right](w).\end{cases}$$

Since the two square-bracketed operators are equal on all $w \in V$, they are equal as operators, and that's what we set out to prove. □

That was a lot of work for apparently little gain. But the result is more important than it looks. Using the first polarization identity, we can immediately prove the following:

Koecher, Lemma III.1

Lemma 3. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, then x and $x \circ y$ operator-commute if and only if x^2 and y operator-commute.*

Proof. Suppose that x and $x \circ y$ operator-commute. Then $L_x L_{(x\circ y)} = L_{(x\circ y)} L_x$, and we can cancel those terms on both sides of Equation (7.1) to obtain

$$L_y L_{x^2} = L_{x^2} L_y,$$

which means exactly that x^2 and y commute. On the other hand, if we start by assuming that x^2 and y operator-commute, we can cancel *those* terms from the polarization identity to conclude that $L_x L_{(x\circ y)} = L_{(x\circ y)} L_x$. □

7.2 Proving power-associativity

Our goal is eventually to show that Jordan algebras are power-associative, as in Definition 29. Recall that the problem was that x^3 could have two meanings, either $x \circ (x \circ x)$ or $(x \circ x) \circ x$. To honor the promise we made in Convention 12, we will temporarily we will work around this difficulty by defining a *left-exponentiation* operation.

Definition 56. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, we (temporarily) define

$$x \circ^m \coloneqq \underbrace{x \circ (x \circ (x \circ \cdots (x \circ x)))}_{x \text{ appears } m \text{ times}}$$

By convention we let $x \circ^0 = 1_V$ and $x \circ^1 = x$. Note that $x \circ^2 = x \circ x = x^2$, and in particular that $x \circ^m = x \circ \left(x \circ^{(m-1)}\right)$ for $m \geq 2$.

Proposition 30. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, if $x \in V$, and if there exist $I, J \in \mathbb{N}$ and $\alpha_{ij} \in \mathbb{R}$ such that $P = \sum_{i=0}^{I} \sum_{j=0}^{J} \alpha_{ij} L_x^i L_{x^2}^j$, then P and L_x commute.*

Proof. Do the multiplication, use the fact that the individual terms commute,

and then undo the multiplication:

$$\begin{aligned}
L_x P &= L_x \left(\sum_{i=0}^{I} \sum_{j=0}^{J} \alpha_{ij} L_x^i L_{x^2}^j \right) \\
&= \sum_{i=0}^{I} \sum_{j=0}^{J} \alpha_{ij} L_x^{i+1} L_{x^2}^j \\
&= \sum_{i=0}^{I} \sum_{j=0}^{J} \alpha_{ij} L_{x^2}^j L_x^{i+1} \\
&= \left(\sum_{i=0}^{I} \sum_{j=0}^{J} \alpha_{ij} L_{x^2}^j L_x^i \right) L_x \\
&= \left(\sum_{i=0}^{I} \sum_{j=0}^{J} \alpha_{ij} L_x^i L_{x^2}^j \right) L_x \\
&= P L_x.
\end{aligned}$$

□

Koecher Theorem III.1

Theorem 25. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then for all $m \in \mathbb{N}$, there exist $I, J \in \mathbb{N}$ and $\alpha_{ij} \in \mathbb{R}$ such that $L_{(x \circ^m)} = \sum_{i=0}^{I} \sum_{j=0}^{J} \alpha_{ij} L_x^i L_{x^2}^j$.*

Proof. For $m = 1$ and $m = 2$, we have $L_{(x \circ^1)} = L_x$ and $L_{(x \circ^2)} = L_{x^2}$, so the base cases are handled. Next assume that the result holds for all $m < k$; we will show that it holds for $m = k \geq 3$ as well.

Our induction hypothesis combined with Proposition 30 says that L_x and $L_{(x \circ^m)}$ commute for all $m < k$. Set $u = x, y = x$, and $z = x \circ^{k-2}$ in Equation (7.3) to obtain,

$$\begin{aligned}
&L_x L_{((x \circ^{k-2}) \circ x)} + L_{(x \circ^{k-2})} L_{(x \circ x)} + L_x L_{(x \circ (x \circ^{k-2}))} \\
&= \\
&L_{(x \circ (x \circ (x \circ^{k-2})))} + L_x L_x L_{(x \circ^{k-2})} + L_{(x \circ^{k-2})} L_x L_x.
\end{aligned}$$

Using commutativity, we can write $\left(x \circ^{k-2}\right) \circ x = x \circ \left(x \circ^{k-2}\right) = x \circ^{k-1}$, and by simplifying and rearranging the rest we can solve for the "biggest" power in terms of the "smaller" powers,

$$\begin{aligned}
L_{x \circ^k} = {} & L_x L_{(x \circ^{k-1})} + L_{(x \circ^{k-2})} L_{x^2} + L_x L_{(x \circ^{k-1})} \\
& - L_x L_x L_{(x \circ^{k-2})} - L_{(x \circ^{k-2})} L_x L_x.
\end{aligned} \tag{7.4}$$

Now we simply note that the sum/difference/product of two expressions of the form in Proposition 30 again has the same form. As a result, our induction hypothesis applied to Equation (7.4) shows that $L_{(x \circ^k)}$ has that form. □

Corollary 10. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, if $x \in V$, and if $m, n \in \mathbb{N}$, then $x \circ^m$ and $x \circ^n$ operator-commute.* *Koecher Corollary III.1*

Proof. By Definition 55, $x \circ^m$ and $x \circ^n$ operator-commute if $L_{(x \circ^m)}$ and $L_{(x \circ^n)}$ commute. And Theorem 25 says that both $L_{(x \circ^m)}$ and $L_{(x \circ^n)}$ have the form

$$L_{(x \circ^m)} = \sum_{i=0}^{I} \sum_{j=0}^{J} \alpha_{ij} L_x^i L_{x^2}^j$$

$$L_{(x \circ^n)} = \sum_{k=0}^{K} \sum_{\ell=0}^{L} \beta_{k\ell} L_x^k L_{x^2}^\ell$$

for $I, J, K, L \in \mathbb{N}$ and $\alpha_{ij}, \beta_{k\ell} \in \mathbb{R}$. By expanding the product, we get

$$L_{(x \circ^m)} L_{(x \circ^n)} = \sum_{i=0}^{I} \sum_{j=0}^{J} \sum_{k=0}^{K} \sum_{\ell=0}^{L} \alpha_{ij} \beta_{k\ell} L_x^i L_{x^2}^j L_x^k L_{x^2}^\ell.$$

But now, L_x and L_{x^2} commute! So we can move all of the terms that came from $L_{(x \circ^n)}$ to the left of those that came from $L_{(x \circ^m)}$:

$$\begin{aligned} \cdots = L_{(x \circ^m)} L_{(x \circ^n)} &= \sum_{k=0}^{K} \sum_{\ell=0}^{L} \sum_{i=0}^{I} \sum_{j=0}^{J} \beta_{k\ell} \alpha_{ij} L_x^k L_{x^2}^\ell L_x^i L_{x^2}^j \\ &= L_{(x \circ^n)} L_{(x \circ^m)}. \end{aligned}$$

□

Finally, the big result that we've been doing all this algebra for.

Theorem 26. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then*

$$\forall m, n \in \mathbb{N} : (x \circ^m) \circ (x \circ^n) = x \circ^{(m+n)} = (x \circ^n) \circ (x \circ^m).$$

Proof. For $m = 1$ or $n = 1$, the result is trivial. Without loss of generality, $\left(x \circ^1\right) \circ (x \circ^n) = x \circ (x \circ^n) = x \circ^{(n+1)}$ by Definition 56. It is similarly easy to check the case where one (or both) of m, n is zero.

Let $\ell := m + n$, and suppose that the result holds for $\ell < k$, where we can take $k \geq 3$ since we've manually checked the cases where $m + n \in \{0, 1, 2\}$. We aim to show that the result holds for $\ell = k$ as well. Now, having checked the case where one of the exponents is one, we can assume that either $m > 1$ or $n > 1$. Without loss of generality (since we could always switch the order of the m, n terms below), suppose that $n > 1$. Then

$$(x \circ^m) \circ (x \circ^n) = (x \circ^m) \circ \left(x \circ \left(x \circ^{(n-1)}\right)\right) = L_{(x \circ^m)} L_x \left(x \circ^{(n-1)}\right),$$

and Corollary 10 lets us rearrange this to

$$L_x L_{(x \circ^m)} \left(x \circ^{(n-1)}\right) = L_x \left[(x \circ^m) \circ \left(x \circ^{(n-1)}\right)\right],$$

which, by the induction hypothesis, is simply

$$L_x \left[x \circ^{(m+n-1)}\right] = x \circ^{(m+n)}.$$

□

Let's summarize these results in terms of our new definition.

Theorem 27. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, if $x \in V$, and if $m, n \in \mathbb{N}$, then*

Koecher, Theorem III.2; Faraut and Korányi, Proposition II.1.2

- $x^m \circ x^n = x^n \circ x^m = x^{(m+n)}$*; by Theorem 26, and*
- $L_{x^m} L_{x^n} = L_{x^n} L_{x^m}$*, by Corollary 10.*
- *The algebra $(V, \circ, \langle\cdot,\cdot\rangle)$ is power-associative per Definition 29.*

Convention 13: Power notation in an EJA

Since Theorem 27 shows that every Euclidean Jordan algebra is power-associative, we will from now on write x^k instead of $x \circ^k$ to indicate the product of x with itself, k times, in any order. This is in agreement with Definition 29 and Convention 12.

Chapter 8

The unique spectral decomposition

Recall that the main reason we care about power-associativity is that it allows us to work in the associative subalgebra generated by a single element. Proposition 12 gives us an explicit representation of that associative subalgebra, and associative algebras are just plain easier to work with.

Since we now know that Euclidean Jordan algebras are power-associative, if $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then $\operatorname{alg}(\{x\})$ forms an associative Euclidean Jordan algebra after restricting the Jordan and inner products. While $\operatorname{alg}(\{x\})$ may not be very large, we know that things are at least well-behaved there. We will see an application of this in a moment.

From one perspective, the reason that Euclidean Jordan algebras are so useful in optimization is because they're one of the most general structures whose elements have eigenvalues and a spectral decomposition. We have hopefully convinced you in Section 4.2 that having a spectral decomposition is rather convenient. In this chapter, we'll present one version of a spectral decomposition (akin to the unique decomposition into projectors in linear algebra) that works in a Euclidean Jordan algebra. We'll then spend a good amount of time trying to push that result through to a "full" decomposition like we get from diagonalizing a symmetric matrix.

8.1 Idempotents

Definition 57. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $c \in V$ satisfies $c^2 = c$, then c is *idempotent*. The letter c is used by many authors to denote an idempotent—don't ask me why.

Warning 9: Zero is an idempotent

Koecher defines idempotents to be non-zero but we don't. Be wary of the definitions when switching between references.

Proposition 31. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $c, d \in V$ are idempotent with $c \circ d = 0$, then $\langle c, d\rangle = 0$.*

Faraut and Korányi, Chapter III Section 1

Proof. Suppose $c \circ d = 0$. Then

$$0 = \langle c, 0\rangle = \langle c, c \circ d\rangle = \left\langle c^2, d\right\rangle = \langle c, d\rangle . \qquad \square$$

Definition 58. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, then a subset $\{c_1, c_2, \ldots, c_k\} \subseteq V$ is a *complete system of orthogonal idempotents* if

Faraut and Korányi, Chapter III Section 1

- Each c_i is idempotent.
- $c_i \circ c_j = 0$ whenever $i \neq j$.
- $c_1 + c_2 + \cdots + c_k = 1_V$.

When talking about idempotents, the term *orthogonal* a priori means that, for example, $c \circ d = 0$ rather than $\langle c, d\rangle = 0$. As we saw a moment ago in Proposition 31, this sort of orthogonality implies the usual kind. The two are actually equivalent, but it's not easy to prove. We will eventually learn that any inner-product on a simple Euclidean Jordan algebra must be a positive scalar multiple of the so-called *canonical trace inner-product*, and the canonical trace inner product of c and d is zero only when $c \circ d = 0$. One nice thing to know about orthogonal idempotents (in this sense) is that they operator-commute.

Proposition 32. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $c, d \in V$ are idempotent with $c \circ d = 0$, then $L_c L_d = L_d L_c$.*

Proof. Let $x \coloneqq c$ and $y \coloneqq d$ in Equation (7.1). $\square$

Corollary 11. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, if $\mathbf{c}$ is a set of orthogonal idempotents in V, and if $x, y \in V$ are both finite linear combinations of the elements of $\mathbf{c}$, then x and y operator-commute.*

Proof. Suppose that $x = \sum_{i=1}^{k} \alpha_i c_i$ and $y = \sum_{j=1}^{k} \beta_j c_j$, where possibly some of the $\alpha_i \in \mathbb{R}$ and $\beta_j \in \mathbb{R}$ are zero, and each $c_i, c_j \in \mathbf{c}$. Expand using linearity as in Proposition 25 to find

$$L_x L_y = \sum_{i=1}^{k}\sum_{j=1}^{k} \alpha_i \beta_j L_{c_i} L_{c_j} = \sum_{i=1}^{k}\sum_{j=1}^{k} \alpha_i \beta_j L_{c_j} L_{c_i} = L_y L_x,$$

where we were able to replace $L_{c_i} L_{c_j}$ with $L_{c_j} L_{c_i}$ thanks to Proposition 32. □

The definition of a complete system of orthogonal idempotents should remind the reader of the spectral theorem for linear algebra. One version of the spectral theorem decomposes a self-adjoint operator into a linear combination of orthogonal projections P_i onto the eigenspaces of L. Those projections all sum to the identity operator, and satisfy $P_i^2 = P_i$ and $P_i P_j = 0$ when $i \neq j$. Thus it is safe to say that a complete system of orthogonal idempotents is a generalization of those projections. Unsurprisingly, they play a huge part in the spectral theorem for Euclidean Jordan algebras.

Lemma 4. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra, if $\{c_1, c_2, \ldots, c_k\}$ is a complete system of orthogonal idempotents, and if $p \in \mathbb{R}[X]$ with the two associated functions,*

$$p\restriction_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}, \text{and}$$
$$p\restriction_{V} : V \to V,$$

then for all $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{R}$, we have

$$p\restriction_{V} \left(\sum_{i=1}^{k} \lambda_i c_i \right) = \sum_{i=1}^{k} p\restriction_{\mathbb{R}} (\lambda_i)\, c_i.$$

Proof. If $p = a_0 X^0 + a_1 X^1 + \cdots + a_m X^m$, then from the orthogonality and idempotence of the c_i, we have

$$\left(\sum_{i=1}^{k} \lambda_i c_i \right)^2 = \sum_{i=1}^{k} \lambda_i^2 c_i,$$

and likewise for higher powers. It follows that

$$p\restriction_{V} \left(\sum_{i=1}^{k} \lambda_i c_i \right) = a_0 1_V + a_1 \left(\sum_{i=1}^{k} \lambda_i c_i \right) + a_2 \left(\sum_{i=1}^{k} \lambda_i^2 c_i \right) + \cdots + a_m \left(\sum_{i=1}^{k} \lambda_i^m c_i \right).$$

By re-grouping this expression, we arrive at

$$p\restriction_{V} \left(\sum_{i=1}^{k} \lambda_i c_i \right) = a_0 1_V + \sum_{i=1}^{k} \left(a_1 \lambda_i + a_2 \lambda_i^2 + \cdots + a_m \lambda_i^m \right) c_i.$$

Now since $1_V = c_1 + c_2 + \cdots + c_m$, we can subtitute that into the first term and then move the resulting $a_0 c_i$ into the corresponding terms of the sum,

$$\begin{aligned} p\restriction_{V} \left(\sum_{i=1}^{k} \lambda_i c_i \right) &= a_0 \left(c_1 + c_2 + \cdots + c_m \right) + \sum_{i=1}^{k} \left(a_1 \lambda_i + a_2 \lambda_i^2 + \cdots + a_m \lambda_i^m \right) c_i \\ &= \sum_{i=1}^{k} \left(a_0 + a_1 \lambda_i + a_2 \lambda_i^2 + \cdots + a_m \lambda_i^m \right) c_i \\ &= \sum_{i=1}^{k} p\restriction_{\mathbb{R}} (\lambda_i)\, c_i. \end{aligned}$$

□

8.2 The spectral theorem

Faraut and Korányi Theorem III.1.1

Theorem 28 (unique EJA spectral theorem)**.** *Suppose that* $(V, \circ, \langle \cdot, \cdot \rangle)$ *is a Euclidean Jordan algebra. If* $x \in V$*, then there exists a unique set of pairs* $\{(\lambda_1, c_1), (\lambda_2, c_2), \ldots, (\lambda_k, c_k)\} \subseteq \mathbb{R} \times \operatorname{alg}(\{x\})$ *such that*

- *The set* $\{c_1, c_2, \ldots, c_k\}$ *forms a complete system of non-zero orthogonal idempotents,*
- *The real numbers* λ_1 *through* λ_k *are non-zero and distinct,*
- $x = \lambda_1 c_1 + \lambda_2 c_2 + \cdots + \lambda_k c_k$.

Proof. Let $\widetilde{L_x}$ be the restriction of L_x to the d-dimensional subalgebra $\mathcal{A} \coloneqq \operatorname{alg}(\{x\})$. Since L_x is self-adjoint on V by Proposition 25, it is also self-adjoint on $\mathcal{A}$; this follows trivially from Definition 37. It therefore has a spectral decomposition with distinct real eigenvalues λ_i and spectral projectors P_i,

$$\widetilde{L_x} = \lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_k P_k.$$

Now let W be the space of self-adjoint linear operators on $\mathcal{A}$, and note that W forms a Euclidean Jordan algebra because it is basically the Real Symmetric EJA. The first thing we want to claim is that, for each projection operator P_j, there exists a polynomial $p_j \in \mathbb{R}[X]$ such that $P_j = p_j\restriction_W \left(\widetilde{L_x}\right)$. Let's just construct some polynomials that will do what we want. Let

$$q_j = \prod \{(X - \lambda_i) \mid i \in \{1, 2, \ldots, k\}, i \neq j\} \in \mathbb{R}[X].$$

Since the λ_j are distinct, q_j is now a polynomial that is zero on all λ_i except when $i = j$. Compute using Lemma 4,

$$\begin{aligned} q_j\restriction_W \left(\widetilde{L_x}\right) &= q_j\restriction_{\mathbb{R}}(\lambda_1) P_1 + q_j\restriction_{\mathbb{R}}(\lambda_2) P_2 + \cdots + q_j\restriction_{\mathbb{R}}(\lambda_k) P_k \\ &= 0 + 0 + \cdots + q_j\restriction_{\mathbb{R}}(\lambda_j) P_j + 0 + 0 \cdots + 0 \\ &= q_j\restriction_{\mathbb{R}}(\lambda_j) P_j. \end{aligned}$$

Now since the coefficients of our polynomials are allowed to be in $\mathbb{R}$, we can simply divide:

$$p_j \coloneqq \frac{q_j}{q_j\restriction_{\mathbb{R}}(\lambda_j)}.$$

This will do the job. The reason we went to all of that trouble is so that we can make the following definition. Define

$$c_j \coloneqq p_j\restriction_V (x) \in \mathcal{A},$$

Since c_j is a sum of multiples of products of x, we know that it lives in $\mathcal{A}$. We can thus legally write L_{c_j} for its left-multiplication-by operator in $\mathcal{A}$, and it is easy to see using the associativity in $\mathcal{A}$ that

$$L_{c_j} = L_{p_j\restriction_V (x)} = p_j\restriction_W \left(\widetilde{L_x}\right) = P_j.$$

To verify the inner equality, simply apply both operators to an arbitrary $y \in \mathcal{A}$ and use associativity. Also using associativity we can deduce that

$$\forall y \in \mathcal{A} : L_{(c_i \circ c_j)}(y) = (c_i \circ c_j)(y) = c_i \circ (c_j(y)) = L_{c_i}\left(L_{c_j}(y)\right),$$

which in turn implies,

$$L_{(c_i \circ c_j)} = L_{c_i} L_{c_j} = P_i P_j = \begin{cases} P_i = L_{c_i} & \text{if } i = j, \\ 0 = L_0 & \text{otherwise.} \end{cases}$$

Finally, by linearity, we have

$$L_{\left(\sum_{j=1}^{k} c_j\right)} = \sum_{j=1}^{k} L_{c_j} = \sum_{j=1}^{k} P_j = L_{1_{\mathcal{A}}} = L_{1_V}$$

and

$$L_{\left(\sum_{j=1}^{k} \lambda_j c_j\right)} = \sum_{j=1}^{k} \lambda_j L_{c_j} = \sum_{j=1}^{k} \lambda_j P_j = \widetilde{L_x}.$$

If $L_z = 0$ for any z in a Euclidean Jordan algebra, then we have $z = 0$. Why? Because (by the contrapositive), if $z \neq 0$, then $L_z(1_V) = z \neq 0$. It follows from Axler's Proposition 3.2 that the linear map $z \mapsto L_z$ is injective. In our case, we can apply this to the previous three equations, one at a time, to conclude that

$$c_i \circ c_j = \begin{cases} c_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

$$\sum_{i=1}^{k} c_j = 1_V$$

$$\sum_{i=1}^{k} \lambda_j c_j = x.$$

This decomposition is unique by construction. We just showed that the decomposition

$$\widetilde{L_x} = \sum_{j=1}^{k} \lambda_j L_{c_j}$$

is a decomposition of $\widetilde{L_x}$ into orthogonal spectral projectors. If there were some other complete orthogonal system $\{d_1, d_2, \ldots, d_m\}$ and associated real numbers $\delta_1, \delta_2, \ldots, \delta_m$, then we would also deduce (in exactly the same way) that

$$\widetilde{L_x} = \sum_{j=1}^{m} \delta_j L_{d_j}$$

However, the linear-algebra spectral decomposition, eigenspaces, and eigenvalues are themselves all unique, so we would then conclude that $m = k$. If we additionally choose an ordering for the real numbers λ_i, then we must have $\delta_j = \lambda_j$ and therefore $L_{d_j} = L_{c_j}$ implying $d_j = c_j$. Without the ordering, the uniqueness is only "up to a permutation." □

Typically we order the λ_i by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$ to assuage the uniqueness concerns. You need to order them anyway if you want to think of, say, λ_1 as being a function of x. The "first real number λ_i" is meaningless, but the "largest real number λ_i" is actually well-defined. Identifying the λ_i with functions is useful if you want to show that they're continuous. The λ_i will turn out to be the "eigenvalues" of x, but we don't know what that means yet.

But in any case, modulo some boring details, this first version of the spectral decomposition is unique.

Warning 10: Zeros invalidate uniqueness

Refer back to Warning 5 about the operator spectral decomposition. There, we had to restrict ourselves to non-zero eigenvalues and projections, and we have to do the same thing in the unique EJA spectral theorem. Since the zero element in a Euclidean Jordan algebra is an idempotent (see Warning 9), the version of the spectral theorem in Faraut and Korányi (which allows the idempotents to be zero) has a bug in it. You could easily add in as many multiples of zero as you want to your decomposition to make it non-unique.

Exercise 19 (equivalence of spectral decompositions for matrices). Let L be any element of the Real Symmetric EJA, and show that its matrix spectral decomposition into projections (via the spectral theorem for linear algebra) and its Euclidean Jordan Algebra spectral decomposition (via the unique EJA spectral theorem) are the same thing.

Recall that a matrix has two sorts spectral decompositions. Take, for example, the identity matrix $I \in \mathcal{S}^n$. The sole eigenspace (corresponding to $\lambda = 1$) for I is $\mathbb{R}^n$, and I itself projects onto that space. Thus $I = 1I$ is the unique spectral decomposition of I into spectral projections. But we can also diagonalize I by choosing any orthonormal basis $\{u_1, u_2, \ldots, u_n\}$ for $\mathbb{R}^n$. Then the matrix U that has those vectors as its columns trivially diagonalizes the identity matrix,

$$I = UIU^T = 1u_1u_1^T + 1u_2u_2^T + \cdots + 1u_nu_n^T.$$

But this choice is not unique, since any orthonormal basis of $\mathbb{R}^n$ will work the same way. Uniqueness was obtained only by grouping all of the one-dimensional projections $u_i u_i^T$ having the same corresponding eigenvalue—or all of them in this case. Obtaining a full, non-unique decomposition into as many idempotents as possible in a Euclidean Jordan algebra is much harder. But that's our goal moving forward.

8.3 Solutions to exercises

Solution to Exercise 19 (equivalence of spectral decompositions for matrices). We have to show that the projections in the spectral theorem for linear algebra satisfy Definition 58 of a complete system of orthogonal non-zero idempotents in a Euclidean Jordan algebra. First of all, projections are self-adjoint, so if we start with a symmetric matrix $L \in \mathcal{S}^n$, then each P_i in its spectral decomposition will also belong to $\mathcal{S}^n$. Projections are idempotent by definition, so $P_i \circ P_i = P_i P_i = P_i$ for all i. And the projections in the spectral decomposition are onto orthogonal subspaces, which means that $P_i P_j = 0$ whenever $i \neq j$. This implies that

$$P_i \circ P_j = \frac{P_i P_j + P_j P_i}{2} = (0 + 0)/2 = 0.$$

Finally, the fact that $I = \sum_{i=1}^k P_i$ is part of the matrix spectral theorem, and we already know that I is the unit element of $\mathcal{S}^n$ considered as a Euclidean Jordan algebra. The matrix spectral theorem also says they're non-zero; therefore, $\{P_i\}_{i=1}^k$ is a complete system of non-zero orthogonal idempotents in the Euclidean Jordan algebra $\mathcal{S}^n$. Now, given an $L \in \mathcal{S}^n$, the classical spectral decomposition is

$$L = \sum_{i=1}^k \lambda_i P_i$$

where the $\lambda_i \in \mathbb{R}$ are distinct and non-zero. However if we let $c_i = P_i$, then $\{c_i\}_{i=1}^k$ is a complete system of non-zero orthogonal idempotents, and

$$L = \sum_{i=1}^k \lambda_i c_i$$

is a valid EJA spectral decomposition according to the unique EJA spectral theorem. Since the EJA spectral decomposition is unique, and since the matrix spectral decomposition always agrees with it, they're identical.

Chapter 9

Minimal and characteristic polynomials

Through the eigenspaces and their dimensions, the full spectral decomposition for a linear operator is closely tied to its characteristic polynomial. And the characteristic polynomial is, in turn, related to the minimal polynomial. To achieve a full spectral decomposition in a Euclidean Jordan algebra, we will have to study these concepts in a more general setting.

9.1 The minimal polynomial

One might wonder how big the associative subalgebra $\operatorname{alg}((x))$ is for a particular x in the V. It turns our that some elements are better than others at generating independent powers. The next definition captures this idea.

Definition 59. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then the *degree* of x is

$$\deg(x) \coloneqq \dim(\operatorname{alg}(\{x\})).$$

Clearly, $\deg(x) \leq \dim(V)$ for all x.

For example, the degree of the unit element is 1 in any nontrivial algebra, since all powers of 1_V are the same (equal to 1_V itself), and thus $\operatorname{alg}(\{1_V\}) = \{\alpha 1_V \mid \alpha \in \mathbb{R}\} = \operatorname{span}(\{1_V\})$, which clearly has dimension one.

Warning 11: Many authors define degree incorrectly

Many authors define the degree of an element x to be

$$\deg(x) \coloneqq \min\left(\left\{d \in \mathbb{N} \;\middle|\; \left\{x^0, \ldots, x^d\right\} \text{ is linearly-dependent}\right\}\right),$$

but this definition is subtly incorrect. To see why, take the example $x \coloneqq 1_V$ that we have already given. Its degree is supposed to be one, but $x^0 = x^1 = x^2 = x^3 = \cdots = x^d$ for any $d \in \mathbb{N}$. As a result,

$$\left\{d \in \mathbb{N} \;\middle|\; \left\{x^0, x^1, \ldots, x^d\right\} \text{ is linearly-dependent}\right\} = \left\{d \in \mathbb{N} \mid \{x\} \text{ is linearly-dependent}\right\}.$$

The set $\{x\}$ is always linearly-independent (when $x \neq 0$), so the set of natural numbers above is actually empty; no choice of $d \in \mathbb{N}$ will make $\{x\}$ linearly-dependent. And since we can't take the minimum of an empty set, the given definition of $\deg(x)$ is invalid.

Why are we going to all this trouble? Recall from Warning 2 that an algebra (with vector addition and algebra multiplication) might *not* form a ring if the algebra multiplication isn't associative. However, in a Euclidean Jordan algebra, the subalgebra $\operatorname{alg}(\{x\})$ is always associative because the big algebra is power-associative. Thus $\operatorname{alg}(\{x\})$ *does* form a ring, and we an use ring-theoretic tools to chip away at it. Specifically, all of the polynomial tools that we developed for and used in classical linear algebra.

Proposition 33. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, if $x \in V$, and if we define*

$$I_x \coloneqq \{p \in \mathbb{R}[\Lambda] \mid p\restriction_V(x) = 0\},$$

where $p\restriction_V : V \to V$ is as in Definition 30, then I_x is a ring ideal in $\mathbb{R}[\Lambda]$.

Proof. Corollary 6 shows that $p \mapsto p\restriction_V$ is an isomorphism, so ring ideals in one ring are ring ideals the other.

The fact that I_x is a ring ideal is fairly easy to see. The zero polynomial/function is clearly zero on x. And if we evaluate $[p+q]\restriction_V(x)$ as $p\restriction_V(x) + q\restriction_V(x)$, then I_x is obviously closed under addition. Finally, if we multiply $p \in I_x$ by any $q \in \mathbb{R}[\Lambda]$, then $[pq]\restriction_V(x) = q\restriction_V(x) \circ p\restriction_V(x) = q\restriction_V(x) \circ 0 = 0$, so I_x is a ring ideal. □

We won't need this fact, but $\text{alg}(\{x\})$ and $\mathbb{R}[\Lambda]/I_x$ are isomorphic as rings (Faraut and Korányi, II.2). The ring $\mathbb{R}[\Lambda]$ is a priori much larger than $\text{alg}(\{x\})$, since the former contains all of the powers Λ^n for $n \in \mathbb{N}$, while $\text{alg}(\{x\})$ contains only a finite number of powers of x. However, modding out by I_x addresses that. We can easily take $f \in \text{alg}(\{x\})$ to $[f] \in \mathbb{R}[\Lambda]/I_x$. To get back, let $g \in [f]$ and note that $g(x) = f(x)$ by the definition of I_x and the factor ring. Suppose $\deg(x) = d$. In the expression $g(x) = f(x) = \sum_{i=0}^{\infty} \alpha_i x^i$, we now simply rewrite every $x^d, x^{d+1}, \ldots$ power in terms of the lower ones $x^0, x^1, \ldots, x^{d-1}$. This gets us back to an (unique) element of $\text{alg}(\{x\})$. These operations should be inverse ring homomorphisms, or isomorphisms. The idea is similar to how we proved Proposition 12.

Corollary 12. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then the ring ideal*

$$I_x \coloneqq \{p \in \mathbb{R}[\Lambda] \mid p\restriction_V(x) = 0\}$$

where $p\restriction_V : V \to V$ is as in Definition 30 is generated by a single, unique, monic polynomial that divides every other element of I_x.

Proof. Theorem 8 says that I_x is generated by a single polynomial μ. Definition 22 pretty much says that μ divides everything else.

Typically we would have $\text{ideal}(\{\mu\}) = \text{ideal}(\{\alpha\mu\})$ for any nonzero scalar $\alpha \in \mathbb{R}$, making it non-unique. However, scaling to make μ monic makes it unique in this case. For if μ_1 and μ_2 are both monic and generate I_x, then they have the same degree because they divide each other (see Example 14). We can thus obtain a polynomial of lesser degree that is also zero on x, namely $\mu_1 - \mu_2$ (see Example 13). That's a contradiction unless $\mu_1 - \mu_2 = 0$, or $\mu_1 = \mu_2$. □

Definition 60. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then the *minimal polynomial* of x is the unique monic generator of the ring ideal I_x in Corollary 12, and is written μ_x.

The name *minimal polynomial* derives from the fact that the "divides" ordering of Example 40 forms a partial order on the set of real monic nonzero polynomials, and that with respect to that ordering, the chosen polynomial is minimal in the sense of Definition 50.

Example 49. In the trivial Euclidean Jordan algebra of Example 45, the element $0 \in V$ acts as the unit element. Thus the polynomial $1_{\mathbb{R}[\Lambda]}$ is isomorphic to the map $\xi \mapsto 1_V$ by Corollary 6. And since $1_V = 0$ in this case, the polynomial $1_{\mathbb{R}[\Lambda]}$ is clearly the monic polynomial of minimal degree that evaluates to zero on $0 \in V$. Therefore $\mu_0 = 1_{\mathbb{R}[\Lambda]}$ is the minimal polynomial of the sole element of the trivial Euclidean Jordan algebra.

In fact, we already have a way to compute the minimal polynomial of a given element x in a Euclidean Jordan algebra. Let $d = \deg(x)$. Then by Corollary 5, the set $\left\{x^0, x^1, \ldots, x^{d-1}\right\}$ is a basis for $\text{alg}(\{x\})$. And since $x^d \in \text{alg}(\{x\})$, we can write x^d as a linear combination,

$$x^d = \alpha_0 x^0 + \alpha_1 x^1 + \cdots + \alpha_{(d-1)} x^{d-1}.$$

Rearranging, we obtain,

$$x^d - \alpha_0 x^0 + \alpha_1 x^1 + \cdots + \alpha_{(d-1)} x^{d-1} = 0. \tag{9.1}$$

Proposition 34. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra and if $x \in V$ with $d \coloneqq \deg(x)$, then the minimal polynomial of x is*

$$\mu_x = \Lambda^d - a_0 \Lambda^0 - a_1 \Lambda^1 - \cdots - a_{(d-1)} \Lambda^{d-1} \in \mathbb{R}[\Lambda],$$

where the coefficients $a_0, a_1, \ldots, a_{d-1}$ are the coordinates of x^d with respect to the basis $\{x^0, x^1, \ldots, x^{d-1}\}$ in $\operatorname{alg}(\{x\})$.

Proof. We'll show that μ_x is a monic minimal element of the ring ideal I_x defined in Corollary 12. The claim then follows from its uniqueness.

Clearly, μ_x is monic, and Equation (9.1) shows that $\mu_x \in I_x$. To see that it is minimal, suppose that some other monic polynomial $p \in I_x$ divides it, so that $\mu_x = pq$ for some q. A priori, the degree of p is less than or equal to the degree of μ_x (see Example 14), which gives us two cases.

Case 1: the degree of p is strictly less than that of μ_x.

Since $p \in I_x$, we should have $p\restriction_V(x) = 0$. However, that would be a contradiction: the set of powers $\{x^0, x^1, \ldots, x^{d-1}\}$ appearing in $p\restriction_V(x) = 0$ is linearly-independent by Corollary 5, but $p\restriction_V(x) = 0$ expresses $0 \in V$ as a nontrivial linear combination of its elements.

Case 2: the degree of p is the same as μ_x.

In this case, $\mu_x - p$ has degree at most $d-1$, because their Λ^d terms cancel (see Example 13). But then notice that the difference $\mu_x - p$ belongs to the set I_x, because I_x is an ideal. This would contradict the fact that p is a minimal element of that ideal. We can thus evaluate $\mu_x - p\restriction_V(x) = 0$ to reach the same contradiction that we did in the first case; evaluating the polynomial writes $0 \in V$ as a nontrivial linear combination of linearly-independent vectors.

Since both cases lead to a contradiction, p cannot exist, and μ_x is minimal. □

Corollary 13. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then $\deg(x) = \deg(\mu_x)$.*

Example 50. The minimal polynomial of the unit element 1_V in a nontrivial algebra is $\mu_{1_V} = \Lambda - 1_{\mathbb{R}[\Lambda]} \in \mathbb{R}[\Lambda]$, since $\mu_{1_V}\restriction_V(1_V) = 1_V - 1_V = 0$ and no monic polynomial of smaller degree satisfies the same property (there's only one monic degree-zero polynomial).

Exercise 20 (minimal polynomial of zero). Suppose that $(V, \circ, \langle \cdot, \cdot \rangle)$ is any Euclidean Jordan algebra of dimension n with $n \geq 1$. Find the minimal polynomial of $0 \in V$.

Example 51. Suppose $x = (1,0,2)^T$ in the Hadamard EJA. In this algebra, the unit element is $x^0 = (1,1,1)^T$ and $x^2 = (1,0,4)^T$. Using basic linear algebra, it is not hard to see that $\left\{x^0, x^1, x^2\right\}$ is linearly-independent. But the dimension of $\mathbb{R}^3$ is three, so it's clear that $x^3 = (1,0,8)^T$ must be a linear combination of the lower powers. Indeed, $x^3 = 3x^2 - 2x$, which means that

$$\mu_x = \Lambda^3 - 3\Lambda^2 + 2\Lambda \in \mathbb{R}[\Lambda]$$

is the minimal polynomial of x by Proposition 34.

Exercise 21 (spin algebra minimal polynomial). Find the minimal polynomial of $x = (1,2,3)^T$ in the Jordan Spin EJA on $\mathbb{R}^3$.

Proposition 35. *Suppose that $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra. If $x \in V$ with $d \coloneqq \deg(x)$, and if $\widetilde{L_x}$ denotes the restriction of L_x to $\operatorname{alg}(\{x\})$, then the minimal polynomial of x is the minimal polynomial of the matrix of $\widetilde{L_x}$ with respect to any basis.* *Baes, Proposition 2.3.16*

Proof. We know that $\operatorname{alg}(\{x\}) = \operatorname{span}\left(\left\{x^0, x^1, \ldots, x^{(d-1)}\right\}\right)$ is a d-dimensional vector space from the definition of $\deg(x)$. Let $\mathcal{A} \coloneqq \operatorname{alg}(\{x\})$ for notational convenience. Now $x \in \mathcal{A}$ of course, so $\widetilde{L_x}$ is the left-multiplication-by-x operator on $\mathcal{A}$. The range of $\widetilde{L_x}$ is also contained in $\mathcal{A}$, as is easily seen by applying it to the powers of x that form a basis for $\mathcal{A}$. Thus we are justified in writing $\widetilde{L_x} \in \mathcal{B}(\mathcal{A})$.

Since $\widetilde{L_x}$ is a linear operator on a d-dimensional space, we know from the Cayley-Hamilton theorem that the minimal polynomial of $\widetilde{L_x}$ can have degree at most d. Thus we can suppose that

$$p = \sum_{i=0}^{d} \alpha_i \Lambda^i \in \mathbb{R}[\Lambda]$$

is the minimal polynomial of $\widetilde{L_x}$ with two associated functions

$$p\restriction_{\mathcal{B}(\mathcal{A})} : \mathcal{B}(\mathcal{A}) \to \mathcal{B}(\mathcal{A}),$$
$$p\restriction_V : V \to V.$$

Then since $p\restriction_{\mathcal{B}(\mathcal{A})}\left(\widetilde{L_x}\right) = 0$ from the definition of a minimal polynomial, we can write

$$\left(p\restriction_{\mathcal{B}(\mathcal{A})}\left(\widetilde{L_x}\right)\right)(1_{\mathcal{A}}) = 0,$$

But now we notice that

$$\left(p\restriction_{\mathcal{B}(\mathcal{A})}\left(\widetilde{L_x}\right)\right)(1_{\mathcal{A}}) = \sum_{i=0}^{d} \alpha_i \left(x^i \circ 1_{\mathcal{A}}\right) = \sum_{i=0}^{d} \alpha_i x^i = p\restriction_V(x),$$

and by combining the two equations above, we see that $p\restriction_{\mathcal{B}(\mathcal{A})}(x) = 0$. Thus, from the Definition 60 of a minimal polynomial in a Euclidean Jordan algebra, we know that μ_x divides p. However, μ_x is of degree d by Proposition 34. And $\deg(p) \leq d$ a priori, so we conclude that $\deg(\mu_x) = \deg(p) = d$. Finally, since both are monic by definition, we have $\mu_x = p$.

We haven't involved a matrix up to this point, but we can choose any basis for $\mathcal{A}$, after which p is by definition the minimal polynomial of the matrix of $\widetilde{L_x}$ with respect to that basis. □

Example 52. Suppose $x = (1,0,2)^T$ in the Hadamard EJA. Since we saw in Example 51 that $\operatorname{alg}(\{x\}) = \operatorname{span}\left(x^0, x^1, x^2\right) = \mathbb{R}^3$, we know that the restriction of L_x to $\operatorname{alg}(\{x\})$ is simply L_x itself. If $\mathbf{b} = \{e_1, e_2, e_3\}$ is the standard basis for $\mathbb{R}^3$, then we can compute the matrix $\mathbf{b}(L_x)$ of L with respect to it by computing

$$\mathbf{b}(L_x(e_1)) = \mathbf{b}\left(\begin{bmatrix}1\\0\\2\end{bmatrix} \circ \begin{bmatrix}1\\0\\0\end{bmatrix}\right) = \mathbf{b}\left(\begin{bmatrix}1\\0\\0\end{bmatrix}\right) = \begin{bmatrix}1\\0\\0\end{bmatrix},$$
$$\mathbf{b}(L_x(e_2)) = \mathbf{b}\left(\begin{bmatrix}1\\0\\2\end{bmatrix} \circ \begin{bmatrix}0\\1\\0\end{bmatrix}\right) = \mathbf{b}\left(\begin{bmatrix}0\\0\\0\end{bmatrix}\right) = \begin{bmatrix}0\\0\\0\end{bmatrix},$$
$$\mathbf{b}(L_x(e_3)) = \mathbf{b}\left(\begin{bmatrix}1\\0\\2\end{bmatrix} \circ \begin{bmatrix}0\\0\\1\end{bmatrix}\right) = \mathbf{b}\left(\begin{bmatrix}0\\0\\2\end{bmatrix}\right) = \begin{bmatrix}0\\0\\2\end{bmatrix}.$$

These are the three columns of $\mathbf{b}(L_x)$, so

$$\mathbf{b}(L_x) = \begin{bmatrix}1 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 2\end{bmatrix}.$$

Now Proposition 35 tells us that the minimal polynomial of this matrix is the minimal polynomial of $x \in V$, so we can ask SageMath to compute it for us.

```
sage: A = matrix(QQ, [ [ 1, 0, 0 ],
....:                  [ 0, 0, 0 ],
....:                  [ 0, 0, 2 ]])
sage: A.minimal_polynomial('t')
t^3 - 3*t^2 + 2*t
```

As expected, this agrees with the minimal polynomial we found in Example 51 up to a renaming of the variable (which doesn't matter if you recall Section 3.1).

Example 53. Suppose you want to apply Proposition 35 to compute the minimal polynomial of some element x in a Euclidean Jordan algebra. When $\operatorname{alg}(\{x\})$ is equal to the entire algebra, we don't need to do much because the restriction of L_x to $\operatorname{alg}(\{x\})$ is just L_x itself. But what if $\operatorname{alg}(\{x\})$ is strictly smaller than the ambient algebra?

Fortunately, what you need to restrict a linear operator to some subspace is a basis for that space, and we already know a basis for $\operatorname{alg}(\{x\})$ by Corollary 5. For example, consider the Jordan Spin EJA on $\mathbb{R}^4$. Let $x = (1,2,0,-1)^T \in \mathbb{R}^4$, and we'll find the minimal polynomial of x using Proposition 35.

First, we need to find a basis for $\operatorname{alg}(\{x\})$. To do that, we take successive powers of x, until one of them can be written as a linear combination of the earlier powers. If we start computing, we find that

$$x^0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad x^1 = \begin{bmatrix} 1 \\ 2 \\ 0 \\ -1 \end{bmatrix}, \quad x^2 = \begin{bmatrix} 6 \\ 4 \\ 0 \\ -2 \end{bmatrix}.$$

The set $\left\{x^0, x^1\right\}$ is linearly-independent by inspection, and it turns out that x^2 can be written as a linear combination of those two, namely $x^2 = 4x^0 + 2x^1$. Thus, $\left\{x^0, x^1\right\}$ forms a basis for $\operatorname{alg}(\{x\})$. Now, it's not obvious, but on $\mathbb{R}^4$, the matrix of L_x with respect to the standard basis $\mathbf{e}$ is

$$\mathbf{e}(L_x) = \begin{bmatrix} 1 & 2 & 0 & -1 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}.$$

You can simply check this on an arbitrary $y = (y_1, y_2, y_3, y_4)^T$. To restrict this operator to $\operatorname{alg}(\{x\})$, we recall that all it takes to uniquely define a linear operator on some space is to define its action on a basis for that space. Thus to define an operator $\widetilde{L_x}$ on $\operatorname{alg}(\{x\})$, we will specify its action on the basis $\mathbf{b} \coloneqq \left\{x^0, x^1\right\}$. And since all we're doing is restricring L_x, we already know how $\widetilde{L_x}$ should act on those two vectors:

$$\begin{aligned} \widetilde{L_x}\left(x^0\right) &= x \circ x^0 = x = 0 \cdot x^0 + 1 \cdot x^1, \\ \widetilde{L_x}\left(x^1\right) &= x \circ x = x^2 = 4 \cdot x^0 + 2 \cdot x^1. \end{aligned}$$

Here we have taken the liberty of expressing x^2 in terms of the basis $\mathbf{b}$. Now we already know the matrix representation of $\widetilde{L_x}$ with respect to $\mathbf{b}$,

$$\mathbf{b}\left(\widetilde{L_x}\right) = \left[\mathbf{b}\left(\widetilde{L_x}\left(x^0\right)\right) \quad \mathbf{b}\left(\widetilde{L_x}\left(x^1\right)\right)\right] = \left[\begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 4 \\ 2 \end{bmatrix}\right] \cong \begin{bmatrix} 0 & 4 \\ 1 & 2 \end{bmatrix}.$$

We can now use SageMath to find the minimal polynomial of this matrix, as well as the minimal polynomial of $\mathbf{e}(L_x)$ so that we may contrast the two answers.

```
sage: L_x = matrix(QQ, [[ 1, 2, 0, -1],
....:                   [ 2, 1, 0,  0],
....:                   [ 0, 0, 0,  0],
....:                   [-1, 0, 0,  1]])
sage: L_x_tilde = matrix(QQ, [[ 0, 4 ],
....:                         [ 1, 2 ]])
sage: L_x.minimal_polynomial()
x^4 - 3*x^3 - 2*x^2 + 4*x
sage: L_x_tilde.minimal_polynomial()
x^2 - 2*x - 4
```

The fact that we're using a different basis in the subalgebra than in the superalgebra is immaterial here. The minimal polynomial is invariant under changes of basis. The attentive reader will notice that our invocation of Proposition 35 here was overkill, since in the process of restricting L_x we had to compute $x^2 = 4 \cdot x^0 + 2 \cdot x^1$ from which the minimal polynomial can be directly read off. Nevertheless, it's nice to have a backup plan.

Exercise 22 (Hadamard EJA minimal polynomial). Suppose that $x \coloneqq (1, 0, -1, 0)^T$ in the Hadamard EJA. First, find a basis for $\operatorname{alg}(\{x\})$. Then use your basis to find the matrix (with respect to that basis) of the linear operator

$$\begin{aligned} \widetilde{L_x} &: \operatorname{alg}(\{x\}) \to \operatorname{alg}(\{x\}) \\ \widetilde{L_x} &= y \mapsto x \circ y. \end{aligned}$$

Finally, find the EJA minimal polynomial of x from the matrix minimal polynomial of the operator $\widetilde{L_x}$.

Example 54. Let $(V, \circ, \langle \cdot, \cdot \rangle)$ be the Real Symmetric EJA. In this algebra, the "square" of a matrix is the same as its matrix-multiplication square:

$$X \circ X \coloneqq \frac{XX + XX}{2} = XX.$$

Moreover, the unit element of this algebra is the identity matrix I. As a result, the symbols X^0, X^1, and X^2 mean the same thing no matter which algebra multiplication (matrix or Jordan) we choose. The same is true for higher powers, thanks to power-associativity:

$$X \circ (X \circ X) = X \circ (XX) = \frac{X(XX) + (XX)X}{2} = XXX,$$

and so on. Let $p \in R[\Lambda]$ be any polynomial, and define the two polynomial

functions associated to p,

$$p\restriction_{\mathcal{S}^n} : \mathcal{S}^n \to \mathcal{S}^n$$
$$p\restriction_V : V \to V.$$

Recall Definitions 40 and 60. Since evaluating $p\restriction_{\mathcal{S}^n}$ and $p\restriction_V$ on a symmetric matrix X results in two identical expressions, the minimal polynomial of X in one algebra must be its minimal polynomial in the other. In other words, the minimal polynomial of $X \in V$ is simply its minimal polynomial when considered as a matrix in $\mathcal{S}^n$.

For another approach, one could compare Propositions 23 and 34. The coordinates—and thus the polynomials—will be the same in both cases because the two subalgebras generated by X are isomorphic.

Exercise 23 (real symmetric minimal polynomial). Let $(\mathcal{S}^n, \circ, \langle\cdot,\cdot\rangle)$ be the Real Symmetric EJA, and let

$$X \coloneqq \begin{bmatrix} 3 & -1 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

be an element of the algebra. Find the eigenvalues of X, and use them to find its EJA minimal polynomial.

Finally, we connect the minimal polynomual of an element to its decomposition from the unique EJA spectral theorem.

Proposition 36. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, if $x \in V$, and if $x = \sum_{i=1}^{k} \lambda_i c_k$ for a complete system of nonzero orthogonal idempotents $\{c_1, c_2, \ldots, c_k\}$ in V and distinct real numbers $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{R}$, then*

$$(\Lambda - \lambda_1)(\Lambda - \lambda_2)\cdots(\Lambda - \lambda_k) \in \mathbb{R}[\Lambda]$$

is the minimal polynomial of x.

Proof. If $p \in \mathbb{R}[\Lambda]$ is any polynomial, then Lemma 4 says that

$$p\restriction_V \left(\sum_{i=1}^{k} \lambda_i c_i\right) = \sum_{i=1}^{k} p\restriction_{\mathbb{R}}(\lambda_i)\, c_i.$$

However, the set $\{c_1, c_2, \ldots, c_k\}$ is pairwise-orthogonal and its elements are nonzero, so in particular it is linearly-independent. Thus,

$$\sum_{i=1}^{k} p\restriction_{\mathbb{R}}(\lambda_i)\, c_i = 0 \iff \forall i \in 1, 2, \ldots, k : p\restriction_{\mathbb{R}}(\lambda_i) = 0.$$

Combining these two equations, we see that

$$p\restriction_V(x) = 0 \iff \forall i \in 1, 2, \ldots, k : p\restriction_{\mathbb{R}}(\lambda_i) = 0.$$

But, the minimal nonzero monic polynomial that evaluates to zero on k distinct real numbers λ_1 through λ_k is clearly the product

$$(\Lambda - \lambda_1)(\Lambda - \lambda_2) \cdots (\Lambda - \lambda_k) \in \mathbb{R}[\Lambda].$$

Thus, this must be the minimal polynomial of x in V as well. □

The minimal polynomial is important in classical linear algebra because the roots of its corresponding real function are the eigenvalues of its associated matrix. In a Euclidean Jordan algebra, we will more or less use this as our definition of the eigenvalues of an element; however, we need to go a bit further: we don't want *just* the eigenvalues—we also want to know their multiplicities! This motivates us to go further, in search of an *EJA characteristic polynomial*.

9.2 Regular elements

Recall that a real symmetric n-by-n matrix $A \in \mathcal{S}^n$ can have between zero and n distinct eigenvalues, each of which is a multiplicity-one root of the real function that corresponds to the matrix's minimal polynomial. This follows from the Cayley-Hamilton Theorem 20, which says that the minimal polynomial defined in Definition 40 must divide the characteristic polynomial of Proposition 22. Let $\sigma(A)$ denote the set of all eigenvalues of a matrix A, called the *spectrum* of A. Then the minimal polynomial μ_A of A is

$$\mu_A = \left(\prod_{\lambda \in \sigma(A)} (\Lambda - \lambda) \right) \in \mathbb{R}[\Lambda],$$

and it therefore has degree $\operatorname{card}(\sigma(A))$. But, each real symmetric matrix *also* has an associated *characteristic polynomial*, which is always of degree n—the maximum degree for any minimal polynomial of an n-by-n matrix. If $m(\lambda)$ denotes the dimension of the eigenspace corresponding to the eigenvalue $\lambda \in \sigma(A)$, then the characteristic polynomial γ_A is

$$\gamma_A = \left(\prod_{\lambda \in \sigma(A)} (\Lambda - \lambda)^{m(\lambda)} \right) \in \mathbb{R}[\Lambda].$$

The extra powers ensure that the characteristic polynomial always has degree n. And in the matrix setting, we used Corollary 8 and the characteristic polynomial to read off the sum (trace), product (determinant), and multiplicities of the eigenvalues. These are all things that we'll want to do in a Euclidean Jordan algebra as well.

So where to start? In the n-by-n matrix setting, the maximum degree of any minimal polynomial is n, which is far smaller than the n^2 that we expect a priori. There must be some maximum degree in a Euclidean Jordan algebra, too; although we can say little about it at the moment.

Definition 61. If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra, then its *rank* is

$$\operatorname{rank}(V) \coloneqq \max(\{\deg(x) \mid x \in V\}).$$

Even though the set V is usually infinite, the set of degrees is bounded between 1 and $\dim(V)$. Thus the maximum is taken over a finite set and is well-defined. And since each $\deg(x) \leq \dim(V)$, we naturally have $\operatorname{rank}(V) \leq \dim(V)$.

Example 55. The rank of the Real Symmetric EJA in $\mathcal{S}^n$ is n. This is fairly easy to see, because by Corollary 13, Example 54 and the Cayley-Hamilton Theorem 20, we know that the maximum degree of any element $X \in \mathcal{S}^n$ is n. Moreover the degree n is achieved by any X that has n distinct eigenvalues.

Example 56. The rank of the Hadamard EJA in n dimensions is n. The largest possible dimension that $\deg(x) \coloneqq \dim(\operatorname{alg}(\{x\}))$ could have in Definition 61 is clearly n. So if we can find an x with $\dim(\operatorname{alg}(\{x\})) = n$, then we will have shown that the rank of the algebra is n.

Let $x = (1, 2, \ldots, n)^T$, and consider the powers $x^0, x^1, \ldots, x^{n-1}$. If we create a matrix X whose columns are these powers of x, then

$$X = \begin{bmatrix} x^0 & x^1 & x^2 & \cdots & x^{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1^2 & \cdots & 1^{n-1} \\ 1 & 2 & 2^2 & \cdots & 2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & n & n^2 & \cdots & n^{n-1} \end{bmatrix}.$$

This is a famous matrix called the *Vandermonde matrix*, named after Alexandre-Théophile Vandermonde. It is known that the determinant of this matrix is non-zero if the numbers $1, 2, \ldots, n$ are all distinct—which of course they are. Thus the columns of the matrix form a linearly-independent set, meaning that

$$\dim\left(\operatorname{span}\left(\{x^0, x^1, \ldots, x^{n-1}\}\right)\right) = n,$$

and showing that $\operatorname{alg}(\{x\}) \subseteq \mathbb{R}^n$ must actually be equal to $\mathbb{R}^n$. Since the degree of this particular x is as large as it can be (that is, n), the rank of of algebra must also be n.

Exercise 24 (spin algebra rank). Let $(V = \mathbb{R}^n, \circ, \langle \cdot, \cdot \rangle)$ be a Jordan Spin EJA for some $n \geq 2$. Find the minimal polynomial of an arbitrary element $x = (x_1, \bar{x})^T \in V$, and thereby show that the degree of any element in the Jordan spin algebra is less than or equal to two. Having done that, find an element having degree equal to two. Combine these facts to find the rank of any spin algebra with $n \geq 2$.

Definition 62. If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra and if $x \in V$ has $\deg(x) = \operatorname{rank}(V)$, then x is a *regular element* of the algebra.

The main goal in this section is to prove that the regular elements are dense in a Euclidean Jordan algebra. This will let us make continuity arguments for

the entire algebra based on knowledge of the regular elements. But to prove this innocent-looking claim, we unfortunately need some heavy machinery from algebraic geometry. And before can can apply that, we need to know that everything is made up of polynomials. Hearken back to Convention 10 for the matrix-of-polynomials notation we're about to use.

Lemma 5. *If* $(V, \circ, \langle\cdot,\cdot\rangle)$ *is a Euclidean Jordan algebra of dimension* n *with basis* $\mathbf{b}$*, then there exists a matrix* $M_{\mathbf{b}} \in \left[\mathbb{P}^n\left(\mathbb{R}\right)\right]^{n\times n}$ *such that*

$$\forall x \in V : M_{\mathbf{b}}\restriction_{\mathbb{R}^n}\left(\mathbf{b}\left(x\right)\right) = \mathbf{b}\left(L_x\right).$$

Proof. Recall from Proposition 25 that the map $x \mapsto L_x$ is linear, and let $x = x_1 b_1 + x_2 b_2 + \cdots + x_n b_n$ be the representation of an arbitrary $x \in V$ with respect to the basis $\mathbf{b}$. Then using linearity, we have

$$L_x = L_{(x_1 b_1 + x_2 b_2 + \cdots + x_n b_n)} = x_1 L_{b_1} + x_2 L_{b_2} + \cdots + x_n L_{b_n}$$

and thus

$$\begin{aligned}\mathbf{b}\left(L_x\right)_{ij} &= \mathbf{b}\left(x_1 L_{b_1} + x_2 L_{b_2} + \cdots + x_n L_{b_n}\right)_{ij} \\ &= x_1 \mathbf{b}\left(L_{b_1}\right)_{ij} + x_2 \mathbf{b}\left(L_{b_2}\right)_{ij} + \cdots + x_n \mathbf{b}\left(L_{b_n}\right)_{ij}.\end{aligned}$$

Each $\mathbf{b}\left(L_{b_k}\right)_{ij}$ above is a constant, because the left-multiplication-by-b_k matrix is fixed. Thus we see that not only is the i,jth entry of $\mathbf{b}\left(L_x\right)$ the result of evaluating a polynomial at $\left(x_1, x_2, \ldots, x_n\right)^T$, but that said polynomial is linear. It follows that if we define

$$M_{ij} \coloneqq \mathbf{b}\left(L_{b_1}\right)_{ij} X_1 + \mathbf{b}\left(L_{b_2}\right)_{ij} X_2 + \cdots + \mathbf{b}\left(L_{b_n}\right)_{ij} X_n,$$

then the matrix

$$M_{\mathbf{b}} \coloneqq \left[M_{ij}\right]$$

does the job: evaluating $\left(M_{\mathbf{b}}\right)_{ij} = M_{ij}$ at $\left(x_1, x_2, \ldots, x_n\right)^T$ gives us the i,jth entry of $\mathbf{b}\left(L_x\right)$. □

It is important that one polynomial matrix works for every element x of the algebra in the preceding lemma. As a result, we need only compute its polynomial entries once, delaying their evaluation until we are given a specific x for which we want to know $\mathbf{b}\left(L_x\right)$.

Example 57. Take the Hadamard EJA on $\mathbb{R}^4$ and the standard basis $\mathbf{b}$. If $\mathbf{b}\left(x\right) = \left(x_1, x_2, x_3, x_4\right)^T$, then the left-multiplication-by-x operation is represented by the matrix

$$\mathbf{b}\left(L_x\right) = \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix},$$

since if $\mathbf{b}(y) = (y_1, y_2, y_3, y_4)^T$, then

$$\begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} x_1 y_1 \\ x_2 y_2 \\ x_3 y_3 \\ x_4 y_4 \end{bmatrix} = x \circ y.$$

In this case, the $4^2 = 16$ polynomials

$$M_{ij} := \begin{cases} X_i & \text{if } i = j, \\ 0 & \text{otherwise} \end{cases} \in \mathbb{R}[X_1, X_2, X_3, X_4]$$

give us the entries of $\mathbf{b}(L_x)$ when we evaluate the corresponding functions at the coordinates $\mathbf{b}(x)_1 = x_1$, $\mathbf{b}(x)_2 = x_2$, et cetera, of x. For example, if $\mathbf{b}(x) = (1, 2, 3, 4)^T$, then

$$\begin{aligned} M_{22}\restriction_{\mathbb{R}^4} &: \mathbb{R}^4 \to \mathbb{R} \\ M_{22}\restriction_{\mathbb{R}^4} &= (x_1, x_2, x_3, x_4)^T \mapsto x_2 \\ M_{22}\restriction_{\mathbb{R}^4}(1, 2, 3, 4) &= M_{22}\restriction_{\mathbb{R}^4}(\mathbf{b}(x)_1, \mathbf{b}(x)_2, \mathbf{b}(x)_3, \mathbf{b}(x)_4) = 2, \end{aligned}$$

which tells us the $2, 2$ entry of

$$\mathbf{b}(L_x) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}.$$

Example 58. In the Jordan Spin EJA on $\mathbb{R}^3$, if we let $\mathbf{b}(x) = (x_1, x_2, x_3)^T$, then with respect to the standard basis $\mathbf{b}$, we have

$$\mathbf{b}(L_x) = \begin{bmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & 0 \\ x_3 & 0 & x_1 \end{bmatrix},$$

since if $\mathbf{b}(y) = (y_1, y_2, y_3)^T$, then

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & 0 \\ x_3 & 0 & x_1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 y_1 + x_2 y_2 + x_3 y_3 \\ x_2 y_1 + x_1 y_2 \\ x_3 y_1 + x_1 y_3 \end{bmatrix} = \begin{bmatrix} \langle x, y \rangle \\ y_1 \begin{bmatrix} x_2 \\ x_3 \end{bmatrix} + x_1 \begin{bmatrix} y_2 \\ y_3 \end{bmatrix} \end{bmatrix}$$

which is nothing other than $\mathbf{b}(x \circ y)$. And clearly, the entries of $\mathbf{b}(L_x)$ are given by (linear) polynomials in the $\mathbf{b}$-coordinates of x.

Exercise 25 (general left multiplication in the Real Symmetric EJA). In the Real Symmetric EJA, first find a basis $\mathbf{b}$ for $\mathcal{S}^2$. Then let $\mathbf{b}(x) = (x_1, x_2, \ldots)^T$ be the coordinates of an arbitrary $x \in \mathcal{S}^2$ with respect to that

basis, and find the matrix $\mathbf{b}(L_x)$ of L_x with respect to $\mathbf{b}$. Your matrix $\mathbf{b}(L_x)$ should be filled with polynomial expressions in x_1, x_2, and so on. Conclude that there exist $\left(\dim\left(\mathcal{S}^2\right)\right)^2$ polynomials M_{ij} that, when evaluated at the $\mathbf{b}$-coordinates of x, give you the matrix $\mathbf{b}(L_x)$. To check your answer, let

$$x \coloneqq \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \quad \text{and} \quad y \coloneqq \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

Your matrix $\mathbf{b}(L_x)$ should satisfy

$$\mathbf{b}(L_x)\,\mathbf{b}(y) = \mathbf{b}(L_x(y)) = \mathbf{b}(x \circ y).$$

Corollary 14. *In the context of Lemma 5, define p_0 to be the embedding of $\mathbf{b}(1_V)$ into $[\mathbb{P}^n(\mathbb{R})]^{n\times 1}$. Then for all $k \in \mathbb{N}$, the polynomial column-matrices $p_k \coloneqq (M_{\mathbf{b}})^k p_0$ satisfy,*

$$\forall x \in V : p_k\restriction_{\mathbb{R}^n}(\mathbf{b}(x)) = \mathbf{b}\left(x^k\right).$$

Proof. The statement holds by definition for p_0. And for $k \geq 1$, we have by Proposition 10 that,

$$\begin{aligned}\left[(M_{\mathbf{b}})^k p_0\right]\restriction_{\mathbb{R}^n}(\mathbf{b}(x)) &= \left[M_{\mathbf{b}}\restriction_{\mathbb{R}^n}(\mathbf{b}(x))\right]^k(\mathbf{b}(1_V)) \\ &= \mathbf{b}(L_x)^k\,\mathbf{b}(1_V) \\ &= \mathbf{b}\left(x^k\right).\end{aligned}$$

□

Example 59. Sticking with Jordan Spin EJA on $\mathbb{R}^3$, let $\mathbf{b}(x) = (x_1, x_2, x_3)^T$. Then

$$x^2 = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \circ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1^2 + x_2^2 + x_3^3 \\ 2x_1x_2 \\ 2x_1x_3 \end{bmatrix}$$

and

$$x^3 = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \circ \begin{bmatrix} x_1^2 + x_2^2 + x_3^2 \\ 2x_1x_2 \\ 2x_1x_3 \end{bmatrix} = \begin{bmatrix} x_1^3 + 3x_1x_3^2 + 3x_1x_2^2 \\ 3x_1^2x_2 + x_2^3 + x_2x_3^2 \\ 3x_1^2x_3 + x_2^2x_3 + x_3^3 \end{bmatrix}$$

The entries of x^3 are obviously polynomials in the $\mathbf{b}$-coordinates x_1, x_2, x_3 of x; and moreover, this same expression can be obtained by exponentiating the matrix of polynomials that give us the entries of $\mathbf{b}(L_x)$.

Suppose $M_{\mathbf{b}}$ is the matrix from Lemma 5 whose entries $M_{ij} \in \mathbb{R}[X_1, X_2, X_3]$ give us the (i,j)th entry of $\mathbf{b}(L_x)$. Then from our previous examples,

$$M_{\mathbf{b}} = \begin{bmatrix} X_1 & X_2 & X_3 \\ X_2 & X_1 & 0 \\ X_3 & 0 & X_1 \end{bmatrix}, \quad 1_V = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix},$$

and

$$(M_{\mathbf{b}})^3(1_V) = (M_{\mathbf{b}})^2 \begin{bmatrix} X_1 \\ X_2 \\ X_3 \end{bmatrix} = \begin{bmatrix} X_1^2+X_2^2+X_3^2 & 2X_1X_2 & 2X_1X_3 \\ 2X_1X_2 & X_1^2+X_2^2 & X_2X_3 \\ 2X_1X_3 & X_2X_3 & X_1^2+X_3^2 \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \\ X_3 \end{bmatrix}$$
$$= \begin{bmatrix} X_1^3+3X_1X_3^2+3X_1X_2^2 \\ 3X_1^2X_2+X_2^3+X_2X_3^2 \\ 3X_1^2X_3+X_2^2X_3+X_3^3 \end{bmatrix}.$$

Evaluating this at $X_1 = 1, X_2 = 2, X_3 = 3$ should tell us that x^3 is when $x = (1,2,3)^T$:

$$x^3 = \begin{bmatrix} 1+3\cdot 9+3\cdot 4 \\ 3\cdot 2+8+2\cdot 9 \\ 3\cdot 3+4\cdot 3+27 \end{bmatrix} = \begin{bmatrix} 40 \\ 32 \\ 48 \end{bmatrix}.$$

We can use matrices with polynomial entries in SageMath to let us easily compute all Jordan-algebraic powers of any element:

```
sage: R = PolynomialRing(QQ,["X1","X2","X3"])
sage: X1,X2,X3 = R.gens()
sage: L_x = matrix(R, [ [X1,X2,X3],
....:                   [X2,X1, 0],
....:                   [X3, 0,X1] ])
sage: idV = vector(R, [1,0,0])
sage: cube_of_x = (L_x^3)*idV
sage: cube_of_x.column()
[X1^3 + 3*X1*X2^2 + 3*X1*X3^2]
[  3*X1^2*X2 + X2^3 + X2*X3^2]
[  3*X1^2*X3 + X2^2*X3 + X3^3]
sage: cube_of_x(X1=1, X2=2, X3=3)
(40, 32, 48)
```

Definition 63. If $S \subseteq \mathbb{P}^n(\mathbb{F})$ is a collection of polynomials and if $\mathbb{F}$ is a field, then

Sottile [15], Definition 1.1.1

$$\mathcal{V}(S) \coloneqq \{z \in \mathbb{F}^n \mid \forall f \in S : f\restriction_{\mathbb{F}^n}(z) = 0\}$$

is an *affine variety*.

An affine variety is simply the set of common solutions to a system of polynomial equations, much like a vector subspace is the set of common solutions to a system of linear equations. In fact, vector subspaces are affine varieties when the polynomial equations in the system all happen to be linear.

Definition 64. If $\mathbb{F}$ is a field, then the *Zariski topology* on $\mathbb{F}^n$ is the topology whose closed sets are are the affine varieties in $\mathbb{F}^n$.

Sottile [15], Theorem 1.3.1 and Definition 1.3.2

Exercise 26 (Zariski topology). A *topology* on $\mathbb{R}^n$ is a collection of subsets $\mathcal{T} \subseteq \mathcal{P}(\mathbb{R}^n)$ called "closed sets" that satisfy the following conditions:

1. The empty set is a closed set: $\emptyset \in \mathcal{T}$.
2. The entire space is a closed set: $\mathbb{R}^n \in \mathcal{T}$.
3. If $A \in \mathcal{T}$ and $B \in \mathcal{T}$ are both closed sets, then $(A \cup B) \in \mathcal{T}$ is a closed set as well.
4. If $\{A_i \mid i \in I\} \subseteq \mathcal{T}$ is any collection of closed sets, then their intersection $\left(\bigcap_{i \in \mathcal{I}} A_i\right) \in \mathcal{T}$ is a closed set as well.

Each affine variety in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$. The goal of this exercise is to verify that the set of all affine varieties on $\mathbb{R}^n$,

$$\mathcal{T} \coloneqq \{\mathcal{V}(S) \mid S \subseteq \mathbb{P}^n(\mathbb{R})\}, \tag{9.2}$$

forms a topology on $\mathbb{R}^n$. You should do this in four steps:

1. Find an $S \subseteq \mathbb{P}^n(\mathbb{R})$ such that $\mathcal{V}(S) = \emptyset$. This shows that $\emptyset$ belongs to the set $\mathcal{T}$ defined by Equation (9.2).
2. Find an $S \subseteq \mathbb{P}^n(\mathbb{R})$ such that $\mathcal{V}(S) = \mathbb{R}^n$. This shows that $\mathbb{R}^n$ belongs to the set $\mathcal{T}$ defined by Equation (9.2).
3. Suppose that $S, T \subseteq \mathbb{P}^n(\mathbb{R})$ and show that

   $$\mathcal{V}(S) \cup \mathcal{V}(T) = \mathcal{V}(Q),$$

   where

   $$\begin{aligned} Q &\coloneqq \{pq \mid p \in S, q \in T\}, \\ \mathcal{V}(Q) &= \{z \in \mathbb{R}^n \mid [pq]\restriction_{\mathbb{R}^n}(z) = p\restriction_{\mathbb{R}^n}(z)\, q\restriction_{\mathbb{R}^n}(z) = 0\}. \end{aligned}$$

   Since each p and q here belongs to $\mathbb{P}^n(\mathbb{R})$, their product does too. Thus $Q \subseteq \mathbb{P}^n(\mathbb{R})$, showing that $(\mathcal{V}(S) \cup \mathcal{V}(T)) = \mathcal{V}(Q) \in \mathcal{T}$.
4. Suppose $\{S_i \mid i \in I\}$ is some collection of sets $S_i \subseteq \mathbb{P}^n(\mathbb{R})$, and show that

   $$\bigcap_{i \in \mathcal{I}} \mathcal{V}(S_i) = \mathcal{V}\left(\bigcup_{i \in \mathcal{I}} S_i\right).$$

   Then since each S_i is a subset of $\mathbb{P}^n(\mathbb{R})$, their union is a subset of $\mathbb{P}^n(\mathbb{R})$ as well, showing that $\bigcap_{i \in \mathcal{I}} \mathcal{V}(S_i) \in \mathcal{T}$.

Theorem 29. *A nonempty open subset of $\mathbb{R}^n$ in the Zariski topology is open and dense in the Euclidean topology on $\mathbb{R}^n$.*

Sottile [15], Theorem 1.3.5

Lemma 6. *Suppose* $(V, \circ, \langle\cdot,\cdot\rangle)$ *is a Euclidean Jordan algebra of dimension* n *and rank* r*, and let* $R \coloneqq \mathbb{P}^n(\mathbb{R})$*. Then there exists a regular element* $\xi \in V$*, a basis* $\mathbf{b}_\xi$ *of* V*, and an* n*-by-*n *matrix* $A_\xi \in R^{n\times n}$ *such that* $\det(A_\xi) \in R$ *and*

$$\forall x \in V : \det(A_\xi)\restriction_{\mathbb{R}^n}(\mathbf{b}_\xi(x)) \neq 0 \iff x \text{ is regular}.$$

Proof. Definition 61 of the rank of an EJA says that the rank is the maximum degree achieved by any element, so we know that *some* element has its degree equal to the rank of the algebra. Let $\xi \in V$ be that element; then ξ is regular by definition, and $\left\{\xi^0, \xi^1, \ldots, \xi^{r-1}\right\}$ is linearly-independent because it forms a basis of $\operatorname{alg}(\{\xi\})$. Now let $\{e_{r+1}, \ldots, e_n\}$ be a basis for the orthogonal complement of $\operatorname{alg}(\{\xi\})$ in V. It follows that $\mathbf{b}_\xi \coloneqq \left\{\xi^0, \xi^1, \ldots, \xi^{r-1}, e_{r+1}, \ldots, e_n\right\}$ is a basis for V, and so we've found ξ and $\mathbf{b}_\xi$ already.

Corollary 14 says that there exist polynomials matrices $p_j \in R^{n\times 1}$ such that

$$\forall x \in V : p_j\restriction_{\mathbb{R}^n}(\mathbf{b}_\xi(x)) = \mathbf{b}_\xi\left(x^j\right).$$

Define a matrix $A_\xi \in R^{n\times n}$ whose jth column is p_j for $j < r$, and whose remaining columns are the standard basis vectors $\mathbf{b}_\xi(e_{r+1}), \ldots, \mathbf{b}_\xi(e_n)$, interpreted as having entries in R. For example, $\mathbf{b}_\xi(e_n)$ is the vector in $R^{n\times 1}$ with a $1_R \in R$ in the nth position and 0_R elsewhere. These additional columns serve mainly to ensure that A_ξ is square so that its determinant will exist.

Now each entry of A_ξ is a polynomial in R, and so A_ξ itself belongs to the module whose elements are n-by-n matrices with entries in R and whose "scalars" are again polynomials in R. This module was discussed in Example 15. Since R is a commutative ring and since $A_\xi \in R^{n\times n}$, Definition 35 shows that $\det(A_\xi)$ is a well-defined element of R itself. And as a result, $\det(A_\xi)\restriction_{\mathbb{R}^n}$ is a function from $\mathbb{R}^n$ to $\mathbb{R}$. Since $p \mapsto p\restriction_{\mathbb{R}^n}$ is a ring homomorphism (Proposition 10), the explicit formula in Definition 35 further implies that

$$\det(A_\xi)\restriction_{\mathbb{R}^n} = z \mapsto \det\left([A_{ij}\restriction_{\mathbb{R}^n}(z)]\right).$$

Thus $\det(A_\xi)\restriction_{\mathbb{R}^n}$ is the *same* function that we'd get from evaluating each $A_{ij}\restriction_{\mathbb{R}^n}$ on the argument, and *then* taking the determinant of the resulting real n-by-n matrix.

At this point, we note that x is regular if and only if the set $\left\{x^0, x^1, \ldots, x^{r-1}\right\}$ is linearly-independent if and only if the set $\left\{\mathbf{b}_\xi\left(x^0\right), \mathbf{b}_\xi\left(x^1\right), \ldots, \mathbf{b}_\xi\left(x^{r-1}\right)\right\}$ is linearly-independent. Since those are the first r columns of $[A_{ij}\restriction_{\mathbb{R}^n}(\mathbf{b}_\xi(x))]$, and a matrix's determinant is nonzero if and only if its columns are linearly-independent, it follows that $\det(A_\xi)\restriction_{\mathbb{R}^n}(\mathbf{b}_\xi(x)) \neq 0$ if and only if x is regular. □

Theorem 30. *If* $(V, \circ, \langle\cdot,\cdot\rangle)$ *is a Euclidean Jordan algebra of dimension* n*, then the set of its regular elements is open and dense in* V*.*

Baes, Proposition 2.7.24; Faraut and Korányi, Proposition II.2.1

Proof. We will show that the set of regular elements of V contains a nonempty, open subset of V in the Zariski topology. From Theorem 29 it then follows that the set of regular elements is open and dense in the Euclidean topology, which

is the "usual" topology induced by a norm on a finite-dimensional vector space. All norms on a finite-dimensional vector space are equivalent (Proposition 1) in the sense they all result in the same topology, so we don't have to worry about what inner product V carries.

Recall the regular element $\xi \in V$, the basis $\mathbf{b}_\xi$, and the polynomial $\det(A_\xi) \in \mathbb{P}^n(\mathbb{R})$ from Lemma 6. Consider the Zariski-closed affine variety,

$$\mathcal{V}(\{\det(A_\xi)\}) = \{z \in \mathbb{R}^n \mid \det(A_\xi)\restriction_{\mathbb{R}^n}(z) = 0\}.$$

The complement of this variety is nonempty, since the regular element ξ satisfies

$$\det(A_\xi)\restriction_{\mathbb{R}^n}(\mathbf{b}_\xi(\xi)) = 1 \neq 0$$

by the construction of A_ξ. Lemma 6 itself shows that

$$\{\mathbf{b}_\xi(x) \mid x \text{ is irregular}\} \subseteq \mathcal{V}(\{\det(A_\xi)\}),$$

and if we now take complements on both sides, we obtain

$$(\mathbb{R}^n \setminus \mathcal{V}(\{\det(A_\xi)\})) \subseteq \{\mathbf{b}(x) \mid x \text{ is regular}\}$$

The set on the left is nonempty and Zariski-open, and therefore dense in $\mathbb{R}^n$ in both topologies. The right-hand side, being its superset, is also dense in both topologies. Now we apply the (continuous, since it's linear) inverse $\mathbf{b}^{-1}(\cdot)$ of the basis representation to the set on the right to finally conclude that

$$\mathbf{b}_\xi^{-1}(\{\mathbf{b}_\xi(x) \mid x \text{ is regular}\}) = \{x \mid x \text{ is regular}\}$$

is dense in the norm topology on V. □

Remark 4. The previous result means that regular elements are in fact pretty regular, as far as elements of the algebra are concerned. Conversely, irregular elements are not. This likens linguistically to the fact that "singular" matrices are rather more rare to come across than those that are not.

9.3 The characteristic polynomial

We'll use the rank of a Euclidean Jordan algebra to try to formulate a definition of a characteristic polynomial. We'll start with the goal that, if x is a regular element in V, then its minimal polynomial should be its characteristic polynomial, because that's how it works for matrices. Keeping that in mind, here's an outline of the next few steps:

1. Let $x \in V$ be a regular element.
2. Assume that the characteristic polynomial of x is the minimal polynomial μ_x of x, which we can compute.

3. Show that μ_x can be obtained from some more-complicated polynomial function Γ that takes the coordinates of x with respect to the basis $\mathbf{b}$ and returns μ_x.

4. Prove that coefficients of Γ live in $\mathbb{P}^n(\mathbb{R})$.

5. Conclude that $\Gamma\restriction_{\mathbb{R}^{\bar{n}}}(\mathbf{b}(x))$ is both the characteristic and minimal polynomial of every regular $x \in V$.

6. Define the characteristic polynomial γ_y of an arbitrary $y \in V$ to be $\Gamma\restriction_{\mathbb{R}^{\bar{n}}}(\mathbf{b}(y))$, essentially extending the definition for regular elements by continuity to the non-regular elements.

In other words, we're going to find a formula for the characteristic polynomial that makes sense for regular elements, and then use it for *every* element. This works for two reasons. First, regular elements all have the same rank. This lets us construct a system of a known size, namely $\operatorname{rank}(V)$, and solve it using "standard" linear algebra to find coefficients for the polynomial Γ that work for any regular element. Second, the regular elements are dense, as we saw in Theorem 30. This allows us to extend the definition of Γ to irregular elements using the continuity of polynomials.

Proposition 37. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of dimension n with basis $\mathbf{b}$ and if $\bar{n} \coloneqq \{1, 2, \ldots, n\}$, then there exists a $\Psi \in \mathbb{P}^n(\mathbb{R})[\Lambda]$ such that for all $x \in V$, the associated function $\Psi\restriction_{\mathbb{R}^{\bar{n}}}$ defined in Theorem 12 satisfies*

$$\begin{aligned}\Psi\restriction_{\mathbb{R}^{\bar{n}}} &: \mathbb{R}^n \to \mathbb{R}[\Lambda] \\ \Psi\restriction_{\mathbb{R}^{\bar{n}}} &= \mathbf{b}(x) \mapsto \gamma_{L_x}.\end{aligned}$$

Proof. Keeping in mind Section 3.3, Theorem 19 says that for a given x,

$$\gamma_{L_x} \coloneqq \gamma_{\mathbf{b}(L_x)} = \det(\Lambda I - \mathbf{b}(L_x)) \in \mathbb{R}[\Lambda].$$

However, Lemma 5 says that the matrix $\mathbf{b}(L_x)$ is obtained as $M_{\mathbf{b}}\restriction_{\mathbb{R}^n}(\mathbf{b}(x))$ using the polynomial matrix $M_{\mathbf{b}} \in [\mathbb{P}^n(\mathbb{R})]^{n\times n}$. Define A to be the embedding of $M_{\mathbf{b}}$ into $[\mathbb{P}^n(\mathbb{R})[\Lambda]]^{n\times n}$, and recall from Theorem 12 that the map $M \mapsto M\restriction_{\mathbb{R}^{\bar{n}}}$ acts like a homomorphism. Then

$$\Psi \coloneqq \det(\Lambda I - A) \in \mathbb{P}^n(\mathbb{R})[\Lambda]$$

satisfies

$$\begin{aligned}\Psi\restriction_{\mathbb{R}^{\bar{n}}}(\mathbf{b}(x)) &= \det((\Lambda I)\restriction_{\mathbb{R}^{\bar{n}}}(\mathbf{b}(x)) - A\restriction_{\mathbb{R}^{\bar{n}}}(\mathbf{b}(x))) \\ &= \det(\Lambda I - \mathbf{b}(L_x)) \in \mathbb{R}[\Lambda],\end{aligned}$$

showing that Ψ is indeed what we want. □

Example 60. Recall Example 58, where we showed that, with respect to the standard basis $\mathbf{b}$,

$$\mathbf{b}\left(L_x\right) = \begin{bmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & 0 \\ x_3 & 0 & x_1 \end{bmatrix} \text{ for all } \mathbf{b}\left(x\right) \in \mathbb{R}^3.$$

The nine polynomials $p_{ij} \in \mathbb{R}\left[X_1, X_2, X_3\right]$ associated with this matrix are

$$\begin{aligned} p_{11} = X_1,\, p_{12} = X_2,\, p_{13} = X_3, \\ p_{21} = X_2,\, p_{22} = X_1,\, p_{23} = 0, \\ p_{31} = X_3,\, p_{32} = 0, \quad p_{33} = X_1. \end{aligned}$$

Thus,

$$\Psi = \det\left(\Lambda I - \left[p_{ij}\right]\right) = \det\left(\begin{bmatrix} \Lambda - X_1 & -X_2 & -X_3 \\ -X_2 & \Lambda - X_1 & 0 \\ -X_3 & 0 & \Lambda - X_1 \end{bmatrix}\right).$$

Expanding this according to the determinant formula gives us

$$\Psi = \Lambda^3 - 3\Lambda^2 X_1 + 3\Lambda X_1^2 - X_1^3 - \Lambda X_2^2 + X_1 X_2^2 - \Lambda X_3^2 + X_1 X_3^2.$$

Suppose $\mathbf{b}\left(x\right) = \left(1,2,3\right)^T$. Then if we evaluate $\Psi\restriction_{\mathbb{R}^3}$ at the coordinates of x, we obtain

$$\begin{aligned} \Psi\restriction_{\mathbb{R}^3}\left(\left(1,2,3\right)^T\right) &= \Lambda^3 - 3\Lambda^2 + 3\Lambda - 1 - 4\Lambda + 4 - 9\Lambda + 9 \\ &= \Lambda^3 - 3\Lambda^2 - 10\Lambda + 12. \end{aligned}$$

On the other hand, the matrix of L_x with respect to $\mathbf{b}$ is,

$$\mathbf{b}\left(L_x\right) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix},$$

and SageMath tells is that its characteristic polynomial is

```
sage: A = matrix(QQ, [ [1,2,3],
....:                  [2,1,0],
....:                  [3,0,1] ])
sage: A.characteristic_polynomial('t')
t^3 - 3*t^2 - 10*t + 12
```

The next theorem is Faraut and Korányi's version of the big characteristic polynomial result. We state it only for contrast with our own. Faraut and Korányi prove the existence of a "minimal polynomial of" function for regular elements in the algebra, which they then extend (by continuity) to the irregular elements, calling the result a *characteristic* polynomial. But there is an annoying practical detail: the basis coordinates in their result are with respect to a regular element, and we have no idea how to find a regular element!

Faraut and Korányi, Proposition II.2.1

Theorem 31. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r and dimension n, then there exists a regular element $\xi \in V$, a basis $\mathbf{b}_\xi$, and polynomials a_0 through a_{r-1} in $\mathbb{P}^n(\mathbb{R})$ such that the minimal polynomial of any regular element $x \in V$ is*

$$\Lambda^r + \sum_{i=0}^{r-1} a_i\restriction_{\mathbb{R}^n}(\mathbf{b}_\xi(x))\,\Lambda^i \in \mathbb{R}[\Lambda].$$

That said, we're going to do pretty much the same thing, but with an arbitrary basis. The ability to bring our own basis will be incredibly useful, because most of our examples have had nice basis elements with integer entries. Our "characteristic polynomial of" function will also stem from polynomial in $(\mathbb{P}^n(\mathbb{R}))[\Lambda]$ whose "coefficients" a_0 through a_{r-1} live in $\mathbb{P}^n(\mathbb{R})$. The trick will be finding those coefficients, and that's what the next result does. While proving it, we'll deviate from our usual approach (Section 3.3) of omitting the embedding of a polynomial into its fraction field. The bookkeeping is itself the hard part of the proof.

Theorem 32. *Let $(V, \circ, \langle\cdot,\cdot\rangle)$ be a Euclidean Jordan algebra of dimension $n \geq 1$ and rank r with basis $\mathbf{b}$. Define $R \coloneqq \mathbb{P}^n(\mathbb{R})$ with its embedding ι into $\mathbb{F} \coloneqq \operatorname{Frac}(R)$, and let p_0 through $p_n \in R^n$ be as in Corollary 14. Then if $s \in \mathbb{N}$ with $s \leq r$, the system*

$$\begin{bmatrix}\iota(p_0) & \iota(p_1) & \cdots & \iota(p_{s-1})\end{bmatrix} a = \iota(p_s) \tag{9.3}$$

has a solution $a \in \mathbb{F}^{n\times 1}$ if and only if $s = r$.

Proof. First we show that $\{\iota(p_0), \iota(p_1), \ldots, \iota(p_{r-1})\}$ is linearly-independent over $\mathbb{F}$. Suppose that

$$\sum_{k=0}^{r-1} \left(\frac{c_k}{d_k}\right) \iota(p_k) = 0_{\mathbb{F}^{n\times 1}}. \tag{9.4}$$

If all of the c_k are zero, then we are done, so suppose that $\rho \in \mathbb{N}$ is the largest index such that $c_\rho \neq 0_R$. If $\rho = 0$, we contradict ourselves with

$$\left(\frac{c_0}{d_0}\right)\iota(p_0) = 0_{\mathbb{F}^{n\times 1}} \iff c_0 p_0 = 0_{R^{n\times 1}} \iff c_0 = 0_R,$$

since $p_0\restriction_{\mathbb{R}^n}(z) = \mathbf{b}(1_V) \neq 0_{\mathbb{R}^n}$ for all $z \in \mathbb{R}^n$. Thus we may suppose that $\rho \geq 1$ to avoid empty sums and products in what follows. Cancelling the denominators

in Equation (9.4) and rearranging, we arrive at

$$\left(\prod_{j=0}^{\rho-1}\frac{d_j}{1_R}\right)\left(\frac{c_\rho}{1_R}\right)\iota\left(p_\rho\right)+\sum_{k=0}^{\rho-1}\left(\prod_{\substack{j=0\\j\neq k}}^{\rho}\frac{d_j}{1_R}\right)\left(\frac{c_k}{1_R}\right)\iota\left(p_k\right)=0_{\mathbb{F}^{n\times 1}}.$$

Or, in terms of the fraction-field embedding,

$$\left(\prod_{j=0}^{\rho-1}\iota\left(d_j\right)\right)\iota\left(c_\rho\right)\iota\left(p_\rho\right)+\sum_{k=0}^{\rho-1}\left(\prod_{\substack{j=0\\j\neq k}}^{\rho}\iota\left(d_j\right)\right)\iota\left(c_k\right)\iota\left(p_k\right)=\iota\left(0_{R^{n\times 1}}\right),$$

which by injectivity reduces to

$$\left(\prod_{j=0}^{\rho-1}d_j\right)c_\rho p_\rho+\sum_{k=0}^{\rho-1}\left(\prod_{\substack{j=0\\j\neq k}}^{\rho}d_j\right)c_k p_k=0_{R^{n\times 1}}. \tag{9.5}$$

We have assumed that $c_\rho\neq 0_R$, and the d_j are all non-zero because they started out as denominators in $\mathbb{F}$. The set of regular elements in V is open and dense (Theorem 30), as are the sets where the $d_j{\restriction}_{\mathbb{R}^n}$ and $c_\rho{\restriction}_{\mathbb{R}^n}$ are nonzero—so we can find a regular element $x\in V$ such that

$$\alpha\coloneqq\left(\prod_{j=0}^{\rho-1}d_j\right){\restriction}_{\mathbb{R}^n}\left(\mathbf{b}\left(x\right)\right)c_\rho{\restriction}_{\mathbb{R}^n}\left(\mathbf{b}\left(x\right)\right)\neq 0_{\mathbb{R}}.$$

If we evaluate Equation (9.5) at $\mathbf{b}\left(x\right)$ and divide by this $\alpha\neq 0_{\mathbb{R}}$, then we arrive at an expression of the form

$$\mathbf{b}\left(x^\rho\right)+\alpha^{-1}\sum_{k=0}^{\rho-1}\beta_k\mathbf{b}\left(x^k\right)=0_{\mathbb{R}^{n\times 1}}$$

for some collection of $\beta_k\in\mathbb{R}$. Inverting the basis-representation map now gives

$$x^\rho+\sum_{k=0}^{\rho-1}\left(\alpha^{-1}\beta_k\right)x^k=0_V.$$

But this is the result of evaluating a monic univariate polynomial of degree $\rho<r$ at x. Since x is regular, it has degree r, and Corollary 13 and Definition 62 say that the result cannot be zero for $\rho<r$. We conclude that indeed all of the c_k are zero, and our claim that $\left\{\iota\left(p_0\right),\iota\left(p_1\right),\ldots,\iota\left(p_{r-1}\right)\right\}$ is linearly-independent follows. This shows that Equation (9.3) has no solution for $s<r$.

Now if, on the other hand, we have $s=r$, then Equation (9.3) has a solution. To see this, extend the linearly-independent set $\left\{\iota\left(p_0\right),\iota\left(p_1\right),\ldots,\iota\left(p_{r-1}\right)\right\}$ to

a basis for $\mathbb{F}^n$ by appending elements $\tilde{q}_1, \tilde{q}_2, \ldots, \tilde{q}_{n-r}$. Without loss of generality we assume that each entry of each $\tilde{q}_k$ has denominator one. This can be accomplished without destroying the linear-independence of the set by scaling each $\tilde{q}_k$ by the least common multiple of their denominators, and thus we may presume that these new basis elements satisfy $\tilde{q}_k = \iota(q_k)$ for some $q_k \in R^n$, and that therefore there exists a nonsingular matrix $Q \in R^{n \times n}$ with

$$\iota(Q) \coloneqq \begin{bmatrix} \iota(p_0) & \iota(p_1) & \cdots & \iota(p_{r-1}) & \iota(q_1) & \iota(q_2) & \cdots & \iota(q_{n-r}) \end{bmatrix} \in \mathbb{F}^{n \times n}.$$

Every entry of $\iota(Q)$ has denominator 1_R, and the determinant of $\iota(Q)$ is nonzero because its columns are linearly-independent. As a result, we can apply Cramer's rule to find the unique solution $\tilde{a} = (a_0, a_1, \ldots, a_{n-1})^T$ to the system $\iota(Q)\,\tilde{a} = \iota(p_r)$:

$$a_i \coloneqq \frac{\det\left(\iota(Q)_{i \to \iota(p_r)}\right)}{\det(\iota(Q))} \in \mathbb{F}. \tag{9.6}$$

It remains to be seen that $a_i = 0_{\mathbb{F}}$ when $i \geq r$, so that no $\iota(q_k)$ are present in the solution and that therefore $a \coloneqq (a_0, a_1, \ldots, a_{r-1})^T$ solves Equation (9.3). However, this follows relatively easily from the properties of the determinant. First notice that by definition we have $a_i = 0_{\mathbb{F}}$ if and only if $\det\left(\iota(Q)_{i \to \iota(p_r)}\right) = 0_{\mathbb{F}}$. This determinant is a sum/product of elements of $\mathbb{F}$, so we can apply ι^{-1} to conclude that $a_i = 0_{\mathbb{F}}$ if and only if $\det(Q_{i \to p_r}) = 0_R$. But $\det(Q_{i \to p_r})$ must be zero for $i \geq r$, since the corresponding function from $\mathbb{R}^n \to \mathbb{R}$ is zero on the **b**-coordinates of any regular element x, the power x^r being a real linear combination of the lower powers in that case. More explicitly, using Proposition 10 and Definition 35,

$$\det(Q_{i \to p_r})\restriction_{\mathbb{R}^n}(\mathbf{b}(x)) = \det(Q_{i \to p_r}\restriction_{\mathbb{R}^n}(\mathbf{b}(x)))$$

and the latter is zero on the dense subset (Theorem 30) of regular $x \in V$ by the linear-dependence of $\{x^0, x^1, \ldots, x^r\}$ in that case. By continuity we conclude that $\det(Q_{i \to p_r})\restriction_{\mathbb{R}^n}$ and hence $\det(Q_{i \to p_r})$ are zero when $i \geq r$. □

Note that the solutions we obtain in the previous result still belong to the fraction field of $\mathbb{P}^n(\mathbb{R})$. Ultimately we'd like them to live in $\mathbb{P}^n(\mathbb{R})$ itself; for that we'll use an old Lemma of Gauss. The proof is omitted, because I don't know where to find it.

Lemma 7 (Gauss's lemma)**.** *Let* $\mathrm{Frac}(R)$ *denote the fraction field of a given ring* R*. If* R *is a unique factorization domain, if* $p \in R[\Lambda]$ *is monic, and if* $q \in \mathrm{Frac}(R)[\Lambda]$ *divides* p*, then* $q \in R[\Lambda]$*.* *Baes, Lemma 2.3.26*

Finally we can state our characteristic polynomial theorem. Beware that our coefficients a_i differ in sign from those of (say) Faraut and Korányi. I prefer to write the polynomial as a simple sum; other authors choose to play with the coefficients so that the expressions for trace and determinant become simpler.

Theorem 33. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r and dimension n with basis $\mathbf{b}$, then there exist polynomials a_0 through a_{r-1} in $R \coloneqq \mathbb{P}^n(\mathbb{R})$ such that the minimal polynomial of any regular $x \in V$ is*

$$\mu_x = \Lambda^r + \sum_{i=0}^{r-1} a_i\restriction_{\mathbb{R}^n}(\mathbf{b}(x))\,\Lambda^i \in \mathbb{R}[\Lambda].$$

As a result, there exists a polynomial

$$\Gamma = \Lambda^r + \sum_{i=0}^{r-1} a_i\Lambda^i \in R[\Lambda]$$

such that its associated function $\Gamma\restriction_{\mathbb{R}^{\bar{n}}}$ is the "minimal polynomial of" function for (basis coordinates of) regular elements.

Proof. Theorem 32 gives us a solution $\tilde{a} = (\tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{r-1})^T \in \operatorname{Frac}(R)^n$ to Equation (9.3), so that

$$p_r = \tilde{a}_0 p_0 + \tilde{a}_1 p_1 + \cdots + \tilde{a}_{r-1} p_{r-1},$$

or equvalently:

$$p_r - \sum_{i=0}^{r-1} \tilde{a}_i p_i = 0.$$

Suppose for the moment that these $\tilde{a}_i$ belonged to R instead of $\operatorname{Frac}(R)$. Then by letting $a_i \coloneqq -\tilde{a}_i$, we would have for all regular $x \in V$,

$$p_r\restriction_{\mathbb{R}^n}(\mathbf{b}(x)) + \sum_{i=0}^{r-1} a_i\restriction_{\mathbb{R}^n}(\mathbf{b}(x))\, p_i\restriction_{\mathbb{R}^n}(\mathbf{b}(x)) = 0.$$

Considering the definition of p_k from Corollary 14, this would be equivalent to,

$$\mathbf{b}(x^r) + \sum_{i=0}^{r-1} a_i\restriction_{\mathbb{R}^n}(\mathbf{b}(x))\,\mathbf{b}\left(x^i\right) = 0.$$

This equation is in $\mathbb{R}^n$, but if we apply $\mathbf{b}^{-1}$ to both sides, we obtain

$$x^r + \sum_{i=0}^{r-1} a_i\restriction_{\mathbb{R}^n}(\mathbf{b}(x))\, x^i = 0_V$$

in the Euclidean Jordan algebra. Thus it would follow that Γ is the minimal polynomial for any regular $x \in V$. With that in mind, our job is to prove that these a_i actually live in R, and not $\operatorname{Frac}(R)$. Or at least, that their denominator is 1_R in $\operatorname{Frac}(R)$. This will require a bit of a digression. You are encouraged to read Chapter B before proceeding.

For the moment, we can still define $\Gamma \coloneqq \Lambda^r + \sum_{i=0}^{r-1} a_i\Lambda^i$ using the coefficients a_i that we found, but under the assumption that $\Gamma \in \operatorname{Frac}(R)[\Lambda]$. Recall the

polynomial $\Psi \in R[\Lambda]$ from Proposition 37 that generates the characteristic polynomial of every L_x for $x \in V$ via the relationship $\Psi\restriction_{\mathbb{R}^n}(\mathbf{b}(x)) = \gamma_{L_x} \in \mathbb{R}[\Lambda]$. We'd like to show that Γ divides Ψ, allowing us to apply Gauss's lemma. Basically the plan is that if Γ doesn't divide Ψ, then there is no $q \in \operatorname{Frac}(R)[\Lambda]$ such that $\Psi = q\Gamma$, and we want to prove that by applying both sides (as functions) to regular elements x. But doing that requires us to know how to treat rational functions as actual functions. This is a very subtle business, and requires a careful application of the tools developed in Chapter B.

First things first: let's embed the coefficients of Ψ into $\operatorname{Frac}(R)$, so that $\Psi \in \operatorname{Frac}(R)[\Lambda]$ and each of its coefficients has a denominator of one. We do this only so that Ψ and Γ live in the same space.

Next, note that the set of regular elements of V is open and dense in V by Theorem 30. The coefficients of Ψ all have representatives with a one in the denominator, and $1\restriction_{\mathbb{R}^n}$ is obviously non-zero on the set of regular elements. Moreover each a_i has a representative with a denominator that is nonzero; the one given in in Equation (9.6) must be nonzero on the dense set of regular elements to avoid contradicting their degree. Let D_{-1} denote the set of $\mathbf{b}$-coordinates of the regular elements in V. It follows that both Ψ and Γ have associated functions $\Psi\restriction_{D_{-1}}$ and $\Gamma\restriction_{D_{-1}}$ by the discussion in Chapter B.

Now, suppose that Γ does not divide Ψ in $\operatorname{Frac}(R)\restriction_{\Lambda}$. Then

$$\forall q \in \operatorname{Frac}(R)[\Lambda] : \Psi \neq q\Gamma.$$

Each q here has a finite number—call it J—of non-zero coefficients e_j/f_j and Theorem 29 shows that each f_j is nonzero on some open dense subset of $\mathbb{R}^n$. Call those sets D_j, and let $D_q \coloneqq \bigcap_{j=-1}^{J} D_j$. This set is again open and dense, and now all each of $\Psi\restriction_{D_q}$, $q\restriction_{D_q}$, and $\Gamma\restriction_{D_q}$ exist. Using the injectivity of $f \mapsto f\restriction_{D_q}$,

$$\forall q \in \operatorname{Frac}(R)[\Lambda] : \Psi\restriction_{D_q} \neq q\restriction_{D_q}\Gamma\restriction_{D_q}$$

which simply means that

$$\forall q \in \operatorname{Frac}(R)[\Lambda], \exists z \in D_q : \Psi\restriction_{D_q}(z) \neq q\restriction_{D_q}(z)\,\Gamma\restriction_{D_q}(z).$$

But for any q and any regular x we have $\Psi\restriction_{D_q}(\mathbf{b}(x)) = \gamma_{L_x}$ and $\Gamma\restriction_{D_q}(\mathbf{b}(x)) = \mu_x$, so

$$\forall q \in \operatorname{Frac}(R)[\Lambda], \exists x \in \mathbf{b}^{-1}(D_q) : \gamma_{L_x} \neq q\restriction_{D_q}(\mathbf{b}(x))\,\mu_x. \tag{9.7}$$

Now notice that

$$\gamma_{L_x}\restriction_V(x) = 0 \iff \left[\gamma_{L_x}\restriction_{\mathcal{B}(V)}(L_x)\right](1_V) = 0,$$

since the Cayley-Hamilton theorem for matrices, Theorem 20, tells us that $\gamma_{L_x}\restriction_{\mathcal{B}(V)}(L_x)$ is the zero operator. Thus $\gamma_{L_x}\restriction_V(x) = 0$, and γ_{L_x} must live in a ring ideal that is generated by its minimal element μ_x as in Definition 60 and Proposition 34. In other words, μ_x divides γ_{L_x} for any x. This contradicts Equation (9.7), so we were wrong when we supposed that Γ does not divide Ψ.

As a result, there does exist some $q \in \text{Frac}(R)[\Lambda]$ such that $\Psi = q\Gamma$. Here's why we introduced that strange lemma of Gauss. The polynomial Ψ is monic, and has coefficients that are essentially in R, since all we did was embed them into $\text{Frac}(R)$. Thus we can apply Lemma 7 to show that, in fact, both q and Γ have coefficients with ones in the denominator. Reversing the $R \hookrightarrow \text{Frac}(R)$ embedding, we can think of q and Γ as living in $R[\Lambda]$, which is what we wanted all along. □

Somewhat trivially, this gives us a "characteristic polynomial of" function for regular elements, since morally the "minimal polynomial of" and "characteristic polynomial of" functions should be the same for regular elements.

Corollary 15. *In the context of Theorem 33, $\Gamma\restriction_{\mathbb{R}^{\bar{n}}} \circ \mathbf{b}$ is the "minimal polynomial of" function on the set of regular elements in V.*

All that remains to upgrade this "minimal polynomial of" to "the characteristic polynomial of" is to notice that $\Gamma\restriction_{\mathbb{R}^{\bar{n}}} \circ \mathbf{b}$ can be applied to *any* element of the underlying Euclidean Jordan algebra, and not just to regular elements. This leads us to define the characteristic polynomial of an arbitrary element in a way that makes "the characteristic polynomial of" a tautology. Later we will collect more evidence that this is a good choice.

Definition 65. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if Γ and $\mathbf{b}$ are as in Theorem 33, then the *characteristic polynomial* of $x \in V$ is $\gamma_x := \Gamma\restriction_{\mathbb{R}^{\bar{n}}}(\mathbf{b}(x))$.

Exercise 27 (spin algebra inverse via minimal polynomial). Let $x := (1,2,3)^T$ be an element of the Jordan Spin EJA on $\mathbb{R}^3$. In Exercise 21, we found the minimal polynomial of x to be

$$\mu_x = -12X^0 - 2X^1 + X^2 \in \mathbb{R}[X].$$

Taking your inspiration from Exercise 10 where the matrix characteristic polynomial was used, find an element y in the spin algebra such that $x \circ y = 1_V$. (Note: this alone does not show that y is the inverse of x. We define the inverse in a Euclidean Jordan algebra in a moment, in Definition 66.)

Note that the function $x \mapsto \Gamma\restriction_{\mathbb{R}^n}(\mathbf{b}(x))$ in Definition 65 is continuous: it's the composition of a polynomial function on $\mathbb{R}^n$, which is continuous by Proposition 14, with a linear operator. This is going to help us prove things about the *irregular* elements, of which there are fortunately not too many. For example, the next result we're going to prove is an analogue of the Theorem 20 in a Euclidean Jordan algebra. The result is obvious for regular elements, but we'll need the continuity of the "characteristic polynomial of" function to extend the result to irregular elements. A quick exercise shows why such a result might be nice to have.

Corollary 16 (EJA Cayley-Hamilton)**.** *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then $\gamma_x\restriction_V(x) = 0$.* *Alizadeh, Theorem, 14*

Proof. The characteristic polynomial of a regular element is its minimal polynomial and is therefore zero when evaluated at that regular element by definition. Using Theorem 29, we can suppose that x_n is a sequence of regular elements converging to x, and define $\delta_n := x_n - x$ so that $x_n = x + \delta_n$. Note that as $x_n \to x$, we have $\delta_n \to 0$. Now,

$$\begin{aligned}
0 &= \lim_{n\to\infty} \gamma_{x_n}\restriction_V (x_n) \\
&= \lim_{n\to\infty} [\Gamma\restriction_{\mathbb{R}^n} (\mathbf{b}(x_n))]\restriction_V (x_n) \\
&= \lim_{n\to\infty} \left[\Lambda^r + \sum_{i=0}^{r-1} a_i\restriction_{\mathbb{R}^n} (\mathbf{b}(x+\delta_n))\,\Lambda^i\right]\restriction_V (x+\delta_n) \\
&= \lim_{n\to\infty} (x+\delta_n)^r + \sum_{i=0}^{r-1} a_i\restriction_{\mathbb{R}^n} (\mathbf{b}(x+\delta_n))\,(x+\delta_n)^i .
\end{aligned}$$

Since the expression under the limit is a composition of continuous functions by Proposition 14, we can move the limit inside its argument $x + \delta_n$, and use the fact that $\delta_n \to 0$ to arrive at

$$0 = x^r + \sum_{i=0}^{r-1} a_i\restriction_{\mathbb{R}^n} (\mathbf{b}(x))\, x^i = [\Gamma\restriction_{\mathbb{R}^n} (\mathbf{b}(x))]\restriction_V (x) = \gamma_x\restriction_V (x) . \qquad \square$$

Corollary 17. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then the minimal polynomial of x divides the characteristic polynomial of x.*

Proof. By Definition 60, the minimal polynomial of x is the unique monic generator of an ideal that contains γ_x by Corollary 16. $\square$

Corollary 18. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then the characteristic polynomial γ_x of the element x divides the characteristic polynomial γ_{L_x} of the operator L_x.*

Proof. We already showed in Theorem 33 that $\Psi = q\Gamma$ for some $q \in \mathbb{P}^n(\mathbb{R})$, where Ψ is the polynomial such that $\Psi\restriction_{\mathbb{R}^{\bar{n}}} (\mathbf{b}(x)) = \gamma_{L_x}$. So, stick the $\mathbf{b}$-coordinates of x into $\Psi\restriction_{\mathbb{R}^{\bar{n}}} = q\restriction_{\mathbb{R}^{\bar{n}}} \Gamma\restriction_{\mathbb{R}^{\bar{n}}}$. $\square$

Definition 66. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, if $x \in V$, and if there exists a $y \in \operatorname{alg}(\{x\})$ such that $x \circ y = y \circ x = 1_V$, then x is *invertible* and y is the *inverse* of x. In that case, we write x^{-1} to denote the inverse of x, and use x^{-k} as an abbreviation for $\left(x^{-1}\right)^k$.

We require the inverse of x to belong to not only the big algebra, but specifically the subalgebra of V generated by x. This is done intentionally so that the inverse of any element will be unique, thereby justifying our use of the phrase "the inverse" in Definition 66. It also serves another purpose: since $\operatorname{alg}(\{x\})$ is associative, requiring x^{-1} to belong to $\operatorname{alg}(\{x\})$ allows us to cancel positive powers with negative ones. For example, we can simplify $x^{-2}x^3$ to x, since we

can use associativity to pair up the two x^{-1} with an x and then replace them with the unit element.

Proposition 38. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$ is invertible, then the inverse of x is unique.*

Proof. Suppose $y_1, y_2 \in \operatorname{alg}(\{x\})$ are both inverses of x, so that they satisfy $y_1 \circ x = 1_V$ and $y_2 \circ x = 1_V$. Then multiplying the first equation on the left by y_2 gives $y_2 \circ (y_1 \circ x) = y_2$. Now $\operatorname{alg}(\{x\})$ is associative, so we can re-parenthesize $(y_2 \circ y_1) \circ x = y_2$, and then use commutativity to switch the order of y_1, y_2:

$$(y_1 \circ y_2) \circ x = y_2.$$

Use associativity again to conclude that

$$y_2 = y_1 \circ (y_2 \circ x) = y_1 \circ 1_V = y_1. \qquad \square$$

The associativity of $\operatorname{alg}(\{x\})$ is key to showing that the inverse of x is unique, when it exists, as the following example shows.

Example 61. Take $(V, \circ, \langle\cdot,\cdot\rangle)$ to be the Real Symmetric EJA on $\mathcal{S}^2$, and let

$$X \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \; Y_1 \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \; Y_2 \coloneqq \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \in V = \mathcal{S}^2.$$

Then

$$X \circ Y_1 = X^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_V,$$

and

$$\begin{aligned} X \circ Y_2 &= \left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right) /2 \\ &= \left(\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \right) /2 \\ &= \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 1_V. \end{aligned}$$

Thus both Y_1 and Y_2 act like the inverse of $X \in \mathcal{S}^2$.

We now define a determinant and trace for Euclidean Jordan algebras by analogy with Theorem 21 and Corollary 8. The determinant will then influence the invertibility of an element, just like it does for matrices.

Definition 67. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r and if

$$\gamma_x = a_0 z^0 + a_1 z^1 + a_2 z^2 + \cdots + a_{r-1} z^{r-1} + z^r \in \mathbb{R}[z]$$

is the characteristic polynomial of $x \in V$, then by analogy with Corollary 8, we define the *determinant of x* to be

$$\det(x) \coloneqq (-1)^r a_0 = (-1)^r \gamma_x(0)$$

and define the *trace of* x to be

$$\operatorname{trace}(x) \coloneqq -a_{r-1}.$$

Proposition 39. *If* $(V, \circ, \langle\cdot,\cdot\rangle)$ *is a Euclidean Jordan algebra of rank* r*, if* $x \in V$ *with* $\det(x) \neq 0$*, and if the characteristic polynomial of* x *is*

Faraut and Korányi, Proposition II.2.4

$$\gamma_x = a_0 z^0 + a_1 z + a_2 z^2 + \cdots + z^r \in \mathbb{R}[z],$$

then x *is invertible and*

$$x^{-1} = (-1)^{r+1} \left(a_1 1_V + a_2 x^1 + \cdots + x^{r-1}\right) / \det(x).$$

Proof. We check that the claimed inverse is indeed an inverse. Since the algebra multiplication is commutative, we need only check it on the left, using the definition of $\det(x)$ from Definition 67. Apply Corollary 16 to obtain

$$\begin{gathered}
\gamma_x(x) = a_0 1_V + a_1 x + a_2 x^2 + \cdots + x^r = 0 \\
\iff \\
a_1 x + a_2 x^2 + \cdots + x^r = -a_0 1_V \\
\iff \\
x \circ \frac{-\left(a_1 1_V + a_2 x^1 + \cdots + x^{r-1}\right)}{a_0} = 1_V \\
\iff \\
x \circ \frac{(-1)^{r+1}\left(a_1 1_V + a_2 x^1 + \cdots + x^{r-1}\right)}{(-1)^r a_0} = 1_V \\
\iff \\
x \circ \frac{(-1)^{r+1}\left(a_1 1_V + a_2 x^1 + \cdots + x^{r-1}\right)}{\det(x)} = 1_V.
\end{gathered}$$

This shows that the thing we claimed to be an inverse actually acts like an inverse. Note also that

$$(-1)^{r+1}\left(a_1 1_V + a_2 x^1 + \cdots x^{r-1}\right) / \det(x) \in \operatorname{alg}(\{x\}),$$

since it's a linear combination of powers of x. As a result, it satisfies Definition 66 and is the unique inverse of x. □

9.4 Solutions to exercises

Solution to Exercise 20 (minimal polynomial of zero). The zero polynomial is not monic, so it's out. And no non-zero constant polynomial $p = a_0 \in \mathbb{R}[X]$ will work, since if $p\restriction_V = x \mapsto a_0 1_V$ with $a_0 \neq 0$ is the associated function, then $p\restriction_V(0) = a_0 1_V \neq 0$.

Thus, the smallest possible degree that the minimal polynomial of 0 could have is one. Let $p = X \in \mathbb{R}[X]$. Then p is clearly monic, and of the smallest possible degree. Moreover, $p\restriction_V(0) = 0$. Thus, $\mu_0 = X \in \mathbb{R}[X]$ is the minimal polynomial of 0.

Solution to Exercise 21 (spin algebra minimal polynomial). From Exercise 14, we know that $x^0 = (1,0,0)^T$ and of course we were told that $x^1 = (1,2,3)^T$. Obviously no scalar multiple of x^0 will give us x^1, so we try degree two. An easy computation shows that $x^2 = x \circ x = (14,4,6)^T$. Can we solve

$$\begin{gathered} a_0 + a_1 x = x^2 \\ \iff \\ a_0 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 14 \\ 4 \\ 6 \end{bmatrix} \end{gathered}$$

for $a_0, a_1 \in \mathbb{R}$? Sure. Using either linear algebra or just by staring hard enough at the problem, it's clear that $a_1 = 2$ and then we must have $a_0 = 12$. From Proposition 34, we know that the minimal polynomial is found from the first power that is a linear combination of the lower powers, and thus

$$\mu_x = -a_0 X^0 - a_1 X + X^2 = -12X^0 - 2X + X^2 \in \mathbb{R}[X]$$

is the minimal polynomial of x.

Solution to Exercise 22 (Hadamard EJA minimal polynomial). The unit element in this algebra is $(1,1,1,1)^T$, and cubing x gives you back x. Therefore the set

$$\mathbf{b} \coloneqq \left\{ x^0 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \; x^1 = \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}, \; x^2 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\}$$

must span $\operatorname{alg}(\{x\})$. The set $\mathbf{b}$ is also obviously linearly-independent, so it's a basis for $\operatorname{alg}(\{x\})$. Now we can find the matrix of of the linear operator

$$\begin{aligned} \widetilde{L_x} &: \operatorname{alg}(\{x\}) \to \operatorname{alg}(\{x\}) \\ \widetilde{L_x} &= y \mapsto x \circ y. \end{aligned}$$

with respect to the basis $\mathbf{b}$:

$$\begin{aligned} \widetilde{L_x}\left(x^0\right) &= x^1 = 0x^0 + 1x^1 + 0x^2, \\ \widetilde{L_x}\left(x^1\right) &= x^2 = 0x^0 + 0x^1 + 1x^2, \\ \widetilde{L_x}\left(x^2\right) &= x^3 = 0x^0 + 1x^1 + 0x^2. \end{aligned}$$

If we put those coefficients into the columns of a matrix, we get the representation of $\widetilde{L_x}$ with respect to $\mathbf{b}$,

$$\mathbf{b}\left(\widetilde{L_x}\right) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Proposition 35 says that the minimal polynomial of this matrix is the minimal polynomial of x, so we can simply ask SageMath to find it:

```
sage: A = matrix(QQ, [ [0,0,0],
....:                  [1,0,1],
....:                  [0,1,0] ])
sage: A.minimal_polynomial('t')
t^3 - t
```

Solution to Exercise 23 (real symmetric minimal polynomial). Since the matrix

$$X := \begin{bmatrix} 3 & -1 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

is symmetric, $\mathbb{R}^3$ has an orthonormal basis consisting of eigenvectors of X by the spectral theorem for linear algebra. A simple computation (or a computer) shows that the eigenvectors of X are $u_1 = (1,-1,0)^T, u_2 = (0,0,1)^T, u_3 = (1,1,0)^T$. After normalizing them, we can construct a matrix whose columns are those eigenvectors,

$$U := \begin{bmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ -1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 1 & 0 \end{bmatrix},$$

and then use it to diagonalize X:

$$\begin{aligned} U^T X U &= \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} & 0 \\ 0 & 0 & 1 \\ 1/\sqrt{2} & 1/\sqrt{2} & 0 \end{bmatrix} \begin{bmatrix} 3 & -1 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ -1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{bmatrix}. \end{aligned}$$

This diagonal matrix has three distinct eigenvalues, so its matrix minimal polynomial can be read off,

$$\mu_X = (\Lambda - 4)(\Lambda - 3)(\Lambda - 2) \in \mathbb{R}[\Lambda].$$

Since matrix-multiplication exponentiation is identical to Jordan-product exponentiation in $\mathcal{S}^n$, this must also be the minimal polynomial of X in the Euclidean Jordan algebra, just as we saw in Example 54.

Solution to Exercise 24 (spin algebra rank). If we write an arbitrary element $x \in V$ in block form, then

$$x^0 = \begin{bmatrix} 1 \\ \bar{0} \end{bmatrix}, \quad x^1 = \begin{bmatrix} x_1 \\ \bar{x} \end{bmatrix}, \quad x^2 = \begin{bmatrix} \|x\|^2 \\ 2x_1\bar{x} \end{bmatrix}.$$

If we stare at this for a second, it becomes clear that x^2 is a linear combination of x^0 and x^1:

$$\begin{bmatrix} \|x\|^2 \\ 2x_1\bar{x} \end{bmatrix} = \left(\|x\|^2 - 2x_1^2\right)\begin{bmatrix} 1 \\ \bar{0} \end{bmatrix} + 2x_1\begin{bmatrix} x_1 \\ \bar{x} \end{bmatrix}$$

As a result, the minimal polynomial of x (which was completely arbitrary) has degree two at most. We may need fewer, but we cannot need *more* powers of x.

Let $e = (1, 1, \ldots, 1)^T$ now be the vector of n ones. For this element,

$$e^0 = \begin{bmatrix} 1 \\ \bar{0} \end{bmatrix} \text{ and } e^1 = \begin{bmatrix} 1 \\ \bar{e} \end{bmatrix}.$$

Clearly, e^1 cannot be written as a linear combination (that is, a scalar multiple) of e^0, and vice-versa. Thus $\deg(e) > 1$. We showed that the maximum degree of any element in this algebra is two, and then we found an element of degree two or more. It follows that the rank of the algebra, which was the largest degree attained by an element in the algebra, must be two.

Solution to Exercise 25 (general left multiplication in the Real Symmetric EJA). The simplest (but not normalized!) basis for $\mathcal{S}^2$ is

$$\mathbf{b} = \left\{ b_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \; b_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; b_3 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

Thus $\mathcal{S}^2$ is three-dimensional, and

$$x = \begin{bmatrix} x_1 & x_2 \\ x_2 & x_3 \end{bmatrix} \implies \mathbf{b}(x) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$

To find the matrix of L_x, we only need to compute $\mathbf{b}$-coordinates:

$$\begin{aligned}
\mathbf{b}\left(L_x\left(b_1\right)\right) &= \mathbf{b}\left(\left(\begin{bmatrix} x_1 & x_2 \\ x_2 & x_3 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x_1 & x_2 \\ x_2 & x_3 \end{bmatrix}\right)/2\right) \\
&= \frac{1}{2}\mathbf{b}\left(\begin{bmatrix} 2x_1 & x_2 \\ x_2 & 0 \end{bmatrix}\right) \\
&= \left(x_1, \frac{x_2}{2}, 0\right)^T, \\
\mathbf{b}\left(L_x\left(b_2\right)\right) &= \mathbf{b}\left(\left(\begin{bmatrix} x_1 & x_2 \\ x_2 & x_3 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} x_1 & x_2 \\ x_2 & x_3 \end{bmatrix}\right)/2\right) \\
&= \frac{1}{2}\mathbf{b}\left(\begin{bmatrix} 2x_2 & x_1+x_3 \\ x_1+x_3 & 2x_2 \end{bmatrix}\right) \\
&= \left(x_2, \frac{x_1+x_3}{2}, x_2\right)^T, \\
\mathbf{b}\left(L_x\left(b_3\right)\right) &= \mathbf{b}\left(\left(\begin{bmatrix} x_1 & x_2 \\ x_2 & x_3 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x_1 & x_2 \\ x_2 & x_3 \end{bmatrix}\right)/2\right) \\
&= \frac{1}{2}\mathbf{b}\left(\begin{bmatrix} 0 & x_2 \\ x_2 & 2x_3 \end{bmatrix}\right) \\
&= \left(0, \frac{x_2}{2}, x_3\right)^T.
\end{aligned}$$

Putting these into a matrix as its columns, we obtain

$$\mathbf{b}\left(L_x\right) = \begin{bmatrix} x_1 & x_2 & 0 \\ \frac{x_2}{2} & \frac{x_1+x_3}{2} & \frac{x_2}{2} \\ 0 & x_2 & x_3 \end{bmatrix}.$$

Clearly, the entries of this matrix correspond to elements of $\mathbb{R}\left[X_1, X_2, X_3\right]$. For example if $M_{22} = \left(X_1 + X_3\right)/2$, then $M_{22}\restriction_{\mathbb{R}^3}\left(\left(x_1, x_2, x_3\right)^T\right) = \left(x_1 + x_3\right)/2$ gives us the entry $\mathbf{b}\left(L_x\right)_{22}$.

To check, we substitute $x_1 = 1$, $x_2 = 2$, and $x_3 = 3$, and then apply the resulting matrix to $\mathbf{b}\left(y\right) = \left(1, -1, 1\right)^T$

$$\mathbf{b}\left(L_x\right)\mathbf{b}\left(y\right) = \begin{bmatrix} 1 & 2 & 0 \\ 1 & 2 & 1 \\ 0 & 2 & 3 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}.$$

Does this check out? Indeed,

$$\begin{aligned}
\mathbf{b}\left(x \circ y\right) &= \mathbf{b}\left(\left(\begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}\right)/2\right) \\
&= \mathbf{b}\left(\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\right) \\
&= \left(-1, 0, 1\right)^T.
\end{aligned}$$

Solution to Exercise 26 (Zariski topology).

1. Let $f \coloneqq X_1^0 \in \mathbb{P}^n(\mathbb{R})$, and $S \coloneqq \{f\}$. Then

$$\mathcal{V}(S) = \{z \in \mathbb{R}^n \mid f\restriction_{\mathbb{R}^n}(z) = 0\} = \left\{z \in \mathbb{R}^n \;\middle|\; z_1^0 = 1 = 0\right\} = \emptyset,$$

   showing that $\emptyset \in \mathcal{T}$.

2. Let $f = 0 \in \mathbb{P}^n(\mathbb{R})$, and $S \coloneqq \{f\}$. Then

$$\mathcal{V}(S) = \{z \in \mathbb{R}^n \mid f\restriction_{\mathbb{R}^n}(z) = 0\} = \{z \in \mathbb{R}^n \mid 0 = 0\} = \mathbb{R}^n,$$

   showing that $\mathbb{R}^n \in \mathcal{T}$.

3. First suppose that $z \in \mathcal{V}(S) \cup \mathcal{V}(T)$ so either $z \in \mathcal{V}(S)$ or $z \in \mathcal{V}(T)$. In the first case, we have $p\restriction_{\mathbb{R}^n}(z) = 0$ for all $p \in S$. Thus,

$$p\restriction_{\mathbb{R}^n}(z)\, q\restriction_{\mathbb{R}^n}(z) = 0 \cdot q\restriction_{\mathbb{R}^n}(z) = 0$$

   for all $p \in S$ and $q \in T$, showing that $z \in \mathcal{V}(Q)$. On the other hand, if $z \in \mathcal{V}(T)$, the situation is almost identical;

$$p\restriction_{\mathbb{R}^n}(z)\, q\restriction_{\mathbb{R}^n}(z) = p\restriction_{\mathbb{R}^n}(z) \cdot 0 = 0$$

   for all $p \in S$ and $q \in T$, showing that $z \in \mathcal{V}(Q)$. Combining the two, we have $\mathcal{V}(S) \cup \mathcal{V}(T) \subseteq \mathcal{V}(Q)$.

   For the other inclusion, suppose that $z \in \mathcal{V}(Q)$. Checking a truth table, we see that $z \in \mathcal{V}(S) \cup \mathcal{V}(T)$ is logically equivalent to $z \notin \mathcal{V}(S) \implies z \in \mathcal{V}(T)$ and $z \notin \mathcal{V}(T) \implies z \in \mathcal{V}(S)$. Thus, without loss of generality, we can suppose that $z \notin \mathcal{V}(S)$, and try to show that $z \in \mathcal{V}(T)$. Since $z \notin \mathcal{V}(S)$, there exists some $p_0 \in S$ such that $p_0\restriction_{\mathbb{R}^n}(z) \neq 0$. However, $z \in \mathcal{V}(Q)$, so in particular we have

$$\forall q \in T : p_0\restriction_{\mathbb{R}^n}(z)\, q\restriction_{\mathbb{R}^n}(z) = 0.$$

   Since we're in the real numbers, we can just multiply both sides by $\left[p_0\restriction_{\mathbb{R}^n}(z)\right]^{-1}$ to conclude that $q\restriction_{\mathbb{R}^n}(z) = 0$ for all $q \in T$, or that $z \in \mathcal{V}(T)$.

4. This one is just a rearrangement of equivalent logical sentences,

$$\begin{array}{c} z \in \displaystyle\bigcap_{i\in\mathcal{I}} \mathcal{V}(S_i) \iff \forall i \in \mathcal{I}\ \forall f \in S_i : f\restriction_{\mathbb{R}^n}(z) = 0 \\ \Updownarrow \\ \forall f \in \displaystyle\bigcup_{i\in\mathcal{I}} S_i : f\restriction_{\mathbb{R}^n}(z) = 0 \iff z \in \mathcal{V}\left(\displaystyle\bigcup_{i\in\mathcal{I}} S_i\right). \end{array}$$

Solution to Exercise 27 (spin algebra inverse via minimal polynomial). Since the polynomial function associated with μ_x evaluates to zero on x, we have

$$-121_V - 2x + x^2 = 0.$$

Rearranging,

$$-121_V = 2x - x^2 \iff x\frac{1}{12}(x - 21_V) = 1_V.$$

Thus, $\frac{1}{12}(x - 21_V) = \frac{1}{12}(-1, 2, 3)^T$ acts like an inverse of x. We can check,

$$\begin{bmatrix}1\\2\\3\end{bmatrix} \circ \left(\frac{1}{12}\begin{bmatrix}-1\\2\\3\end{bmatrix}\right) = \frac{1}{12}\begin{bmatrix}-1+4+9\\1\begin{bmatrix}2\\3\end{bmatrix} + (-1)\begin{bmatrix}2\\3\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\\0\end{bmatrix} = 1_V.$$

Chapter 10

A full spectral decomposition

10.1 Eigenvalues

There is a reason we went to all of that trouble to define the characteristic polynomial in a Euclidean Jordan algebra. In the matrix case, we showed that some interesting matrix functions—the determinant and trace—can be computed using the characteristic polynomial. We also showed that these two functions were the product and sum of an operator's eigenvalues, respectively. What should "eigenvalues" be in a Euclidean Jordan algebra? Now that we have a characteristic polynomial at our disposal in a Euclidean Jordan algebra, we can finally make sense of this question.

Definition 68. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then the *eigenvalues of* x are the roots of $\gamma_x\restriction_{\mathbb{R}}$.

Theorem 34. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then all of the eigenvalues of x are real.*

Koecher, Chaper VI Theorem 11

Proof. Recall that L_x is self-adjoint by Proposition 25. It therefore has real eigenvalues by Theorem 17, and its characteristic polynomial factors over $\mathbb{R}$. Now factor γ_x into a product of monic irreducible terms, and note that γ_x divides γ_{L_x} by Corollary 18. We can thus apply Corollary 3 to conclude that the roots of $\gamma_x\restriction_{\mathbb{R}}$ must be real as well. □

Since every element x in a Euclidean Jordan algebra has only real eigenvalues, its characteristic polynomial γ_x factors into a product of degree-one terms. Completely by analogy with the matrix case, this means that the determinant of x in the EJA is the product of its eigenvalues and its trace in the EJA is the sum of its eigenvalues.

Corollary 19. *If* $(V, \circ, \langle\cdot,\cdot\rangle)$ *is a Euclidean Jordan algebra and if* $x \in V$*, then* $\det(x)$ *is the product of the eigenvalues of* x*, and* $\operatorname{trace}(x)$ *is the sum of the eigenvalues of* x*.*

Proof. First use Theorem 34 to factor $\gamma_x \in \mathbb{R}[\Lambda]$,

$$\gamma_x = (\Lambda - \lambda_1)(\Lambda - \lambda_2)\cdots(\Lambda - \lambda_r),$$

and then follow the exact same steps as in Corollary 8 to find

$$\begin{aligned} \det(x) &:= (-1)^r a_0 = \lambda_1\lambda_2\cdots\lambda_r, \text{ and} \\ \operatorname{trace}(x) &:= -a_{r-1} = \lambda_1 + \lambda_2 + \cdots + \lambda_r. \end{aligned}$$

□

Example 62. Suppose that $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r. We saw in Example 50 that the minimal polynomial of the unit element is $\Lambda - 1 \in \mathbb{R}[\Lambda]$. Since the minimal polynomial divides the characteristic polynomial by Corollary 17, and since the characteristic polynomial of every element has degree r, we conclude that $\gamma_{1_V} = (\Lambda - 1)^r$. It follows that $\det(1_V) = 1$ and $\operatorname{trace}(1_V) = r$, since there are r roots of $\gamma_{1_V}\restriction_{\mathbb{R}}$ and they're all 1.

Exercise 28 (eigenvalues of idempotents). If c is idempotent in some Euclidean Jordan algebra V, use Proposition 36 and the fact that $c = 1c + 0(1_V - c)$ to find the possible minimal polynomials, eigenvalues, and characteristic polynomials of c.

10.2 Jordan frames

The way we get from the unique spectral decomposition in the spectral theorem for linear algebra to the matrix diagonalization one is by taking an eigenspace E and its corresponding projector P_E, and then decomposing P_E into (for example) $P_E = P_1 + P_2 + P_3$ where P_1, P_2, P_3 are projections onto one-dimensional subspaces of E. If $E = \operatorname{span}(\{e_1, e_2, e_3\})$, then P_1 would be the projection onto the span of e_1, and so on. This decomposition is not unique because it depends on the basis that you choose for the eigenspace. In the matrix case, you can choose any orthonormal basis $\{u_1, u_2, \ldots\}$ of the eigenspace, and then the one-dimensional projectors look like $u_1 u_1^T$. This too has an analogy in a Euclidean Jordan algebra.

Definition 69. Let $(V, \circ, \langle\cdot,\cdot\rangle)$ be a Euclidean Jordan algebra and $c \in V$ be a non-zero idempotent. If there do not exist two non-zero idempotents $c_1, c_2 \in V$ such that $c = c_1 + c_2$, then c is a *primitive idempotent*. A complete system of orthogonal primitive idempotents is called a *Jordan frame*.

Finding Jordan frames can be tricky. Even if you are able to "guess" a complete system of orthogonal idempotents, it usually won't be easy to show that those idempotents are primitive. What follows is the simplest possible case.

Example 63. In the Hadamard EJA on $\mathbb{R}^n$, the standard basis $\{e_1, e_2, \ldots, e_n\}$ is a Jordan frame. It's not hard to see that each e_i is idempotent; and naturally the e_i are mutually orthogonal. To show that each e_i is primitive, we shall suppose that $e_i = c + d$ for two idempotents c and d, and then show that one of c or d must necessarily be zero.

Since e_i has a 1 in its ith position and zeroes elsewhere, the equation $e_i = c+d$ implies that $d_i = c_i - 1$, and that $d_j = -c_j$ for all other $j \neq i$. But of course, $c_j = c_j^2$ for *all* j if c is idempotent. A priori, that means that $c_j \in \{0, 1\}$ for all j. But if $c_j = 1$ for any $j \neq i$, then the corresponding entry of d is $d_j = -c_j = -1$, which would contradict the idempotence of d. Thus $c_j = 0$ and $d_j = -c_j = 0$ for all $j \neq i$. Now consider the ith entry of c. Either $c_i = 0$, which means that $c = 0$, or $c_i = 1$, whence we deduce that $d_i = c_i - 1 = 0$. In either case, one of c or d is zero.

Since decomposing e_i into the sum of two other idempotents cannot be done unless one of those idempotents is zero, each e_i is primitive. It follows from the definition now that $\{e_1, e_2, \ldots, e_n\}$ is a Jordan frame.

Lemma 8. *if $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $c, c_1, c_2 \in V$ are non-zero idempotents such that $c = c_1 + c_2$, then $\langle c_1, c_2\rangle = 0$.*

Proof. The fact that c is idempotent means that

$$c_1 + c_2 = c = c^2 = (c_1 + c_2)^2 = c_1^2 + 2c_1 \circ c_2 + c_2^2 = c_1 + 2c_1 \circ c_2 + c_2.$$

Subtracting $c_1 + c_2$ from both sides gives $2c_1 \circ c_2 = 0$, implying that $c_1 \circ c_2 = 0$. Now Proposition 31 shows that $\langle c_1, c_2\rangle = 0$. □

Lemma 9. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r and if $x = \sum_{i=1}^k \lambda_i c_i$ is the spectral decomposition of $x \in V$ from the unique EJA spectral theorem, then $k \leq r$ and x is regular if and only if $k = r$.*

Proof. Combining Corollary 13 and Proposition 36 we have

$$k = \deg(\mu_x) = \deg(x) \leq \operatorname{rank}(V) = r.$$ □

Proposition 40. *Let $(V, \circ, \langle\cdot,\cdot\rangle)$ be a Euclidean Jordan algebra and let $x = \sum_{i=1}^k \lambda_i c_i$ be the spectral decomposition of $x \in V$ from the unique EJA spectral theorem. If x is regular, then each idempotent c_i is primitive.*

Proof. For the contrapositive, suppose not. If, say, c_1 is *not* primitive, then we can write it as $c_1 = c_1^a + c_1^b$ where $\langle c_1^a, c_1^b\rangle = 0$ by Lemma 8. The resulting set $\{c_1^a, c_1^b, c_2, c_3, \ldots, c_k\}$ is thus still a complete system of orthogonal idempotents, and this process can be repeated until we obtain a Jordan frame. The procedure must terminate eventually because each time we decompose c_i into $c_i^a + c_i^b$, we gain an element that is pairwise orthogonal to everything else. Since we are in a finite dimensional space, we can't keep doing that. When we can't any more, the idempotents that we have are primitive.

In any case, suppose that we've done this until we have a Jordan frame $\{d_1, d_2, \ldots, d_\ell\}$, where $\ell > k$ by the assumption that some c_i was not primitive. Now

$$x \coloneqq 1d_1 + 2d_2 + \cdots + \ell d_\ell$$

is an element of V, but Proposition 36 tells us that

$$(X-1)(X-2)\cdots(X-\ell) \in \mathbb{R}[X]$$

is the minimal polynomial of x. This is a contradiction, since the minimal polynomial has degree $\ell > k$, and $k = r$ is the rank of V by Lemma 9. □

We'll need one more stepping stone before proving the full spectral decomposition. Neither Faraut and Korányi nor Baes mention why the idempotents in the following spectral decomposition should be non-zero, which is a fairly important detail. By analogy with the symmetric matrices, we would like to show that the idempotents all have norms greater than (or equal to) some fixed number—one, it turns out. The map $(x, y) \mapsto \operatorname{trace}(x \circ y)$ in a Euclidean Jordan algebra turns out to be an associative, symmetric, and positive-definite bilinear form—that is, an inner-product. It thus induces a norm, and then with respect to that norm, the idempotents have norm one. However, the proof that $(x, y) \mapsto \operatorname{trace}(x \circ y)$ is an associative bilinear form is rather difficult, so we'd like to defer it until Section 10.4.

Lemma 10. *If $(V, \circ, \langle\cdot,\cdot\rangle_V)$ is a Euclidean Jordan algebra, then the function*

$$\begin{aligned} \|\cdot\|_L &: V \to \mathbb{R} \\ \|x\|_L &\coloneqq \max\left(\{\|L_x(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \end{aligned}$$

is a norm on V.

Proof. The domain and codomain of $\|\cdot\|_L$ are satisfactory, so we need only prove the three properties, all of which follow from the fact that $\|\cdot\|_V$ is itself a norm. First, the triangle inequality:

$$\begin{aligned} \|x+z\|_L &\coloneqq \max\left(\left\{\left\|L_{(x+z)}(y)\right\|_V \mid y \in V, \|y\|_V = 1\right\}\right) \\ &= \max\left(\{\|L_x(y) + L_z(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \\ &\leq \max\left(\{\|L_x(y)\|_V + \|L_z(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \\ &\leq \|x\|_L + \|z\|_L . \end{aligned}$$

Then absolute homogeneity:

$$\begin{aligned} \|\alpha x\|_L &\coloneqq \max\left(\{\|L_{\alpha x}(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \\ &= \max\left(\{\|\alpha L_x(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \\ &= \max\left(\{|\alpha| \, \|L_x(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \\ &= |\alpha| \max\left(\{\|L_x(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \\ &= |\alpha| \, \|x\|_L . \end{aligned}$$

And finally, positive-definiteness:

$$\begin{aligned} x \neq 0 \implies \|x\|_L &:= \max\left(\{\|L_x(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \\ &\geq \left\| L_x\left(\frac{1_V}{\|1_V\|_V}\right)\right\|_V \\ &= \frac{\|x\|_V}{\|1_V\|_V} \\ &> 0. \end{aligned}$$

□

10.3 The spectral theorem (again)

Faraut and Korányi Theorem III.1.2

Theorem 35 (full EJA spectral theorem)**.** *Suppose that $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r. If $x \in V$, then there exists a Jordan frame $\{c_1, c_2, \ldots, c_r\}$ and real numbers $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$ such that*

$$x = \lambda_1 c_1 + \lambda_2 c_2 + \cdots + \lambda_r c_r.$$

The numbers λ_i are the eigenvalues of x, and this decomposition is unique in the following sense: if $\{d_1, d_2, \ldots, d_r\}$ is a Jordan frame in V and if there exist real numbers $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_r$ such that

$$x = \mu_1 d_1 + \mu_2 d_2 + \cdots + \mu_r d_r,$$

then $\mu_i = \lambda_i$ for all i, and

$$\sum_{\{i \mid \lambda_i = t\}} c_i = \sum_{\{i \mid \mu_i = t\}} d_i$$

for any real number t.

Proof. If x is regular, then we can apply the unique EJA spectral theorem, to find

$$x = \lambda_1 c_1 + \lambda_2 c_2 + \cdots + \lambda_k c_k$$

where $\lambda_i \in \mathbb{R}$ and $\{c_1, c_2, \ldots, c_k\}$ is a complete system of orthogonal system of idempotents. From Lemma 9 we see that $k = r$, and then Proposition 40 shows that each c_i is primitive. Thus

$$x = \lambda_1 c_1 + \lambda_2 c_2 + \cdots + \lambda_r c_r$$

is a spectral decomposition of x in terms of a Jordan frame. Now Proposition 36 tells us that the minimal polynomial (which is the same as the characteristic polynomial, for regular elements) of x is

$$\mu_x = (\Lambda - \lambda_1)(\Lambda - \lambda_2)\cdots(\Lambda - \lambda_r) \in \mathbb{R}[\Lambda].$$

Definition 68 says that the roots of $\mu_x\restriction_{\mathbb{R}}$ are the eigenvalues of x, and those are clearly $\lambda_1, \lambda_2, \ldots, \lambda_r$. For regular elements, the theorem is proved.

The next thing we need to do is justify the claim that the numbers λ_i are continuous functions of x when x is irregular. Since x is regular, it has r distinct eigenvalues, so the fact that we have used strict inequality is not a problem. In this setting, the characteristic polynomial of x is monic and all of the roots of $\gamma_x\restriction_{\mathbb{R}}$ are of multiplicity one, so Theorem 9 can be applied to conclude that each number λ_i is in fact obtained from a continuous function $\lambda_i : V \to \mathbb{R}$ applied to x. The roots of $\gamma_x\restriction_{\mathbb{R}}$ are continuous in the coefficients of γ_x, but those coefficients are continuous in (the coordinates of) x by Theorem 33. Likewise, we can think of the elements c_i of the Jordan frame as being functions of x. Without saying anything about their continuity, we can suppose $c_i : V \to V$ is a function that takes a regular element x and returns the idempotent paired with $\lambda_i(x)$ in the unique spectral decomposition of x.

With that out of the way, we're ready to tackle irregular elements. If x is *not* regular, then Theorem 30 lets us suppose that $x^{(n)}$ is a sequence of regular elements whose limit is x. Each $x^{(n)}$ has its own spectral decomposition,

$$x^{(n)} = \left[\sum_{i=1}^{r} \lambda_i\left(x^{(n)}\right) c_i\left(x^{(n)}\right)\right] \to x.$$

Since this sequence is convergent, it is contained in some compact—and therefore bounded—subset of V by Theorems 3 and 6. Yet each individual Jordan frame $\left\{c_i\left(x^{(n)}\right) \mid i = 1, 2, \ldots, r\right\}$ is complete. So,

$$c_1\left(x^{(n)}\right) + c_2\left(x^{(n)}\right) + c_r\left(x^{(n)}\right) = 1_V.$$

If we take norms on both sides and square using the fact that the $c_i\left(x^{(n)}\right)$ are orthogonal,

$$\left\|c_1\left(x^{(n)}\right)\right\|^2 + \left\|c_2\left(x^{(n)}\right)\right\|^2 + \left\|c_r\left(x^{(n)}\right)\right\|^2 = \|1_V\|^2.$$

This shows that each sequence $c_i\left(x^{(n)}\right)$ is itself bounded, because the number $\|1_V\|^2$ is fixed. In particular, that sequence is contained in the closed (and compact) ball of radius $\|1_V\|$, which is a compact set. It therefore has a subsequence $c_i\left(x^{\left(n_{k(i)}\right)}\right)$ that converges by Theorem 5.

Likewise, each sequence $\lambda_i\left(x^{\left(n_{k(i)}\right)}\right)$ is bounded, because we have already shown that the λ_i are continuous, and thus Proposition 4 says that the image of λ_i on whatever compact set contains the sequence $x^{\left(n_{k(i)}\right)}$ is also compact (and thus bounded). As a result, there exists *another* subsequence $x^{\left(n_{k(i)_{\ell(i)}}\right)}$. Before the notation gets any further out-of-hand, let $\operatorname{lcm}(Z)$ denote the least common multiple of the elements of $Z \subseteq \mathbb{N}$, and then let

$$g(n) \coloneqq \operatorname{lcm}\left(\left\{n_{k(i)_{\ell(i)}} \;\middle|\; i = 1, 2, \ldots, r\right\}\right),$$

so that the subsequences $x^{(g(n))}$, $c_i\left(x^{(g(n))}\right)$, and $\lambda_i\left(x^{(g(n))}\right)$ all converge regardless of i. Now, the limit of a subsequence of a convergent sequence is the

same as the limit of that convergent sequence. So,

$$\lim_{n\to\infty} x^{(g(n))} = \lim_{n\to\infty} \left[\sum_{i=1}^{r} \lambda_i\left(x^{(g(n))}\right) c_i\left(x^{(g(n))}\right)\right] = x.$$

Since we defined the characteristic polynomial of an irregular element x to be the limit of the characteristic polynomials of regular elements, the sequences $\lambda_i\left(x^{(g(n))}\right)$ here must converge to the associated root of $\gamma_x\restriction_{\mathbb{R}}$. We don't know what the subsequence $c_i\left(x^{(g(n))}\right)$ converges to, but we know it converges to something—call it $c_i(x)$. Since real-number multiplication is continuous, the limits can be moved inside the product,

$$\begin{aligned} x = \lim_{n\to\infty} x^{(g(n))} &= \lim_{n\to\infty} \left[\sum_{i=1}^{r} \lambda_i\left(x^{(g(n))}\right) c_i\left(x^{(g(n))}\right)\right] \\ &= \sum_{i=1}^{r} \left[\lim_{n\to\infty} \lambda_i(x)\right]\left[\lim_{n\to\infty} c_i\left(x^{(g(n))}\right)\right] \\ &= \sum_{i=1}^{r} \lambda_i(x)\, c_i(x). \end{aligned}$$

To complete the proof, we need to show that the limits $c_i(x) \in V$ form a Jordan frame. First, we note that they sum to the identity, since they are a limit of Jordan frames:

$$\begin{gathered} \sum_{i=1}^{r} c_i\left(x^{(g(n))}\right) = 1_V \\ \Longrightarrow \\ \lim_{n\to\infty}\left[\sum_{i=1}^{r} c_i\left(x^{(g(n))}\right)\right] = \lim_{n\to\infty} 1_V \\ \Longrightarrow \\ \sum_{i=1}^{r} c_i(x) = 1_V. \end{gathered}$$

They are also idempotent, since the Jordan algebra multiplication is continuous

by Proposition 5:

$$\begin{gathered}
c_i\left(x^{(g(n))}\right) \circ c_i\left(x^{(g(n))}\right) = c_i\left(x^{(g(n))}\right) \\
\Longrightarrow \\
\lim_{n\to\infty}\left[c_i\left(x^{(g(n))}\right) \circ c_i\left(x^{(g(n))}\right)\right] = \lim_{n\to\infty} c_i\left(x^{(g(n))}\right) \\
\Longrightarrow \\
\left[\lim_{n\to\infty} c_i\left(x^{(g(n))}\right)\right] \circ \left[\lim_{n\to\infty} c_i\left(x^{(g(n))}\right)\right] = c_i(x) \\
\Longrightarrow \\
c_i(x) \circ c_i(x) = c_i(x).
\end{gathered}$$

They are orthogonal for the same reason; bilinear operators are continuous on finite-dimensional spaces, and the inner-product on V is bilinear:

$$\begin{gathered}
\forall i \neq j : \left\langle c_i\left(x^{(g(n))}\right), c_j\left(x^{(g(n))}\right)\right\rangle = 0 \\
\Longrightarrow \\
\forall i \neq j : \lim_{n\to\infty}\left[\left\langle c_i\left(x^{(g(n))}\right), c_j\left(x^{(g(n))}\right)\right\rangle\right] = \lim_{n\to\infty} 0 \\
\Longrightarrow \\
\forall i \neq j : \left\langle \left[\lim_{n\to\infty} c_i\left(x^{(g(n))}\right)\right], \left[\lim_{n\to\infty} c_j\left(x^{(g(n))}\right)\right]\right\rangle = 0 \\
\Longrightarrow \\
\forall i \neq j : \langle c_i(x), c_j(x)\rangle = 0.
\end{gathered}$$

If we can show that each $c_i(x)$ is non-zero, it will follow (from their orthogonality) that the elements of $\{c_i(x) \mid i = 1, 2, \ldots, r\}$ are distinct, and that therefore there are indeed r elements in that set. In other words, that it is a Jordan frame. But first, we need to show that no $c_i(x)$ can be zero.

Let $c \in V$ be any idempotent, and consider the norm of c defined in Lemma 10. We can choose c itself inside the maximum to deduce that

$$\begin{aligned}
\|c\|_L &:= \max\left(\{\|L_c(y)\|_V \mid y \in V, \|y\|_V = 1\}\right) \\
&\geq \left\|L_c\left(\frac{c}{\|c\|_V}\right)\right\|_V = \left\|\frac{c}{\|c\|_V}\right\|_V = \frac{\|c\|_V}{\|c\|_V} = 1.
\end{aligned}$$

Thus $\|c\|_L \geq 1$ for any idempotent c, and in particular for each $c_i\left(x^{(g(n))}\right)$ in the sequence that converges to $c_i(x)$. The inequality holds in the limit as well, so $\|c_i(x)\|_L \geq 1$ for all i. Now we apply Proposition 1, and we find that there exists a single $\alpha > 0$ such that $\|c_i(x)\|_V \geq \alpha > 0$ for $i = 1, 2, \ldots, r$. In other words, no $c_i(x)$ is zero. □

Refer back to Examples 24 and 27 where we used the spectral decomposition to easily compute powers of a symmetric matrix. The full EJA spectral theorem can be used in a similar way.

Example 64. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r and if $x \in V$ has full spectral decomposition $x = \lambda_1 c_1 + \lambda_2 c_2 + \cdots + \lambda_r c_r$, then $x^2 = \lambda_1^2 c_1 + \lambda_2^2 c_2 + \cdots + \lambda_r^2 c_r$. This is easy to see using the bilinearity of the Jordan product and the fact that the elements of the Jordan frame $\{c_1, c_2, \ldots, c_r\}$ are orthogonal, and it easily extends to higher powers.

Remark 5. The unique spectral decomposition of an element can be obtained from its full spectral decomposition. If $x = \lambda_1 c_1 + \lambda_2 c_2 + \cdots + \lambda_r c_r$ is the full decomposition of an element x, then the idempotents with common coefficients can be grouped and combined to obtain an expression of the form $x = \mu_1 d_1 + \mu_2 d_2 + \cdots + \mu_k d_k$ where $k \leq r$, the μ_j are distinct, and the d_j form a complete system of orthogonal (but not necessarily primitive) idempotents. This latter expression satisfies the conditions for being the unique decomposition in unique EJA spectral theorem, so it must in fact be that unique decomposition.

Exercise 29 (eigenvalues of primitive idempotents). Let $(V, \circ, \langle\cdot,\cdot\rangle)$ be a nontrivial Euclidean Jordan algebra of rank r, and $c \in V$ be idempotent. Use the full spectral decomposition and the result of Exercise 28 to show that if c is primitive, then $\gamma_c = \Lambda^{r-1}(\Lambda - 1)$.

10.4 The canonical trace inner product

In this section, we prove the existence of a "canonical" inner product that exists on any Euclidean Jordan algebra, namely the map $(x, y) \mapsto \operatorname{trace}(x \circ y)$. This inner product has several nice properties that make the rest of what we want to do a lot easier. Of course, proving that $(x, y) \mapsto \operatorname{trace}(x \circ y)$ is in fact an inner product is not so easy. Recall from Definition 13 the properties that this function needs to have. A few of them are "easy," at this point anyway, so we'll get them out of the way.

Proposition 41. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r, if $\alpha \in \mathbb{R}$ and if $x \in V$, then $\operatorname{trace}(\alpha x) = \alpha \operatorname{trace}(x)$, and $\operatorname{trace}(x^2) \geq 0$ with $\operatorname{trace}(x^2) = 0$ if and only if $x = 0$.*

Proof. If the eigenvalues of x are $\{\lambda_1, \lambda_2, \ldots, \lambda_r\}$ in the full EJA spectral theorem, it is easy to see that the eigenvalues of αx are $\{\alpha\lambda_1, \alpha\lambda_2, \ldots, \alpha\lambda_r\}$, and that the trace of x is therefore $\sum_{i=1}^r \alpha\lambda_i = \alpha\left(\sum_{i=1}^r \lambda_i\right) = \alpha \operatorname{trace}(x)$. Likewise, we saw in Example 64 that the eigenvalues of x^2 are $\left\{\lambda_1^2, \lambda_2^2, \ldots, \lambda_r^2\right\}$, so that $\operatorname{trace}(x) = \sum_{i=1}^r \lambda_i^2 \geq 0$ with equality if and only if each λ_i (and thus x itself) is zero. □

Next we'll show that the trace is linear. This isn't easy to derive directly, so we'll have to go back and look at the form of the coefficients in the "characteristic polynomial of" function, recalling that the trace of x was obtained from a particular coefficient polynomial evaluated on the basis coordinates of x (Corollary 19).

Proposition 42. *In Theorem 33, the coefficients a_i of polynomial Γ are themselves homogeneous polynomials of degree $r-i$. In particular, the trace coefficient a_{r-1} is homogeneous of degree one (a linear form).*

Proof. We show that the functions $a_i\restriction_{\mathbb{R}^n}$ are homogeneous of degree $r-i$, and the result follows from Proposition 11.

If $x \in V$, then the characteristic polynomial of x factors (from its spectral decomposition, for example) as

$$\gamma_x = (\Lambda - \lambda_1(\mathbf{b}(x)))(\Lambda - \lambda_2(\mathbf{b}(x)))\cdots(\Lambda - \lambda_r(\mathbf{b}(x)))\,.$$

where the λ_i are continuous functions that compute the eigenvalues of x from its basis representation as in the full EJA spectral theorem. Suppose we define the convenience function

$$\begin{aligned}\lambda &: V \to \mathbb{R}^n \\ \lambda &\coloneqq x \mapsto (\lambda_1(\mathbf{b}(x)), \lambda_2(\mathbf{b}(x)), \ldots, \lambda_r(\mathbf{b}(x)))^T\,,\end{aligned}$$

and a polynomial

$$\Omega \coloneqq (\Lambda - \Lambda_1)(\Lambda - \Lambda_2)\cdots(\Lambda - \Lambda_r) \in \mathbb{R}[\Lambda_1, \Lambda_2, \ldots, \Lambda_r, \Lambda]\,.$$

Then

$$\forall x \in V : \Omega\restriction_{\mathbb{R}^{\bar{n}}}(\lambda(x)) = \gamma_x = \Gamma(\mathbf{b}(x))\,.$$

Thus the coefficient functions—call them $c_i\restriction_{\mathbb{R}^n}$— of Ω must be equal to the coefficient functions $a_i\restriction_{\mathbb{R}^n}$ of Γ. But it is well-known that (up to a factor of -1) expanding the product Ω produces as the coefficients c_i (and thus the coefficients a_i as well) the *elementary symmetric polynomials* of degree $r-i$ in the variables $\Lambda_1, \Lambda_2, \ldots, \Lambda_r$. In fact, we proved this for c_0 and c_{r-1} back in Corollary 8, and the others are similar. So, for example, we have $-c_{r-1} = \Lambda_1 + \Lambda_2 + \cdots + \Lambda_r$. And in general, each c_i has the form

$$c_i = \sum_{j_1=0}^{d_1}\sum_{j_2=0}^{d_2}\cdots\sum_{j_n=0}^{d_n}\beta_{(j_1,j_2,\ldots,j_n)}\Lambda_1^{j_1}\Lambda_2^{j_2}\cdots\Lambda_n^{j_n}\,,$$

where each nonzero index $(j_1, j_2, \ldots, j_n)$ satisfies $j_1 + j_2 + \cdots + j_n = r - i$.

Note quickly that the full spectral decomposition shows that $\lambda(\alpha x) = \alpha\lambda(x)$ for all $\alpha \in \mathbb{R}$ and $x \in V$. Then evaluate, for an arbitrary $x \in V$,

$$\begin{aligned}&a_i\restriction_{\mathbb{R}^n}(\alpha\mathbf{b}(x)) = a_i\restriction_{\mathbb{R}^n}(\mathbf{b}(\alpha x)) \\ &= c_i\restriction_{\mathbb{R}^n}(\lambda(\alpha x)) = c_i\restriction_{\mathbb{R}^n}(\alpha\lambda(x)) \\ &= \sum_{j_1=0}^{d_1}\sum_{j_2=0}^{d_2}\cdots\sum_{j_n=0}^{d_n} b_{(j_1,j_2,\ldots,j_n)}\alpha^{j_1}\alpha^{j_2}\cdots\alpha^{j_n}\lambda_1(\mathbf{b}(x))^{j_1}\cdots\lambda_n(\mathbf{b}(x))^{j_n} \\ &= \alpha^{r-i}c_i\restriction_{\mathbb{R}^n}(\lambda(x)) = \alpha^{r-i}a_i\restriction_{\mathbb{R}^n}(\mathbf{b}(x))\,.\end{aligned}$$

Proposition 11 now shows that each a_i is itself a homogeneous polynomial of degree $r-i$. □

Corollary 20. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r and dimension n with basis $\mathbf{b}$, then the trace function from V to $\mathbb{R}$ is additive.*

Proof. For any $x \in V$, we have $\operatorname{trace}(x) = a_{r-1}\restriction_{\mathbb{R}^n} \circ \mathbf{b}$ by Corollary 19. We just showed that the polynomial $a_{r-1} \in \mathbb{P}^n(\mathbb{R})$ is homogeneous of degree one. It can therefore be expressed as

$$a_{r-1} = c_1 X_1 + c_2 X_2 + \cdots + c_n X_n,$$

for coefficients $c_i \in \mathbb{R}$. It follows that,

$$\begin{aligned}
&\operatorname{trace}(x+y) \\
&= a_{r-1}\restriction_{\mathbb{R}^n}(\mathbf{b}(x+y)) \\
&= a_{r-1}\restriction_{\mathbb{R}^n}(\mathbf{b}(x) + \mathbf{b}(y)) \\
&= c_1(\mathbf{b}(x)_1 + \mathbf{b}(y)_1) + c_2(\mathbf{b}(x)_2 + \mathbf{b}(y)_2) + \cdots + c_n(\mathbf{b}(x)_n + \mathbf{b}(y)_n) \\
&= a_{r-1}\restriction_{\mathbb{R}^n}(\mathbf{b}(x)) + a_{r-1}\restriction_{\mathbb{R}^n}(\mathbf{b}(y)) \\
&= \operatorname{trace}(x) + \operatorname{trace}(y).
\end{aligned}$$

This same argument could be used to show that the trace is homogeneous if we had not already done that in Proposition 41. □

The following is an immediate consequence of the trace's linearity.

Corollary 21. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, then the map $(x, y) \mapsto \operatorname{trace}(x \circ y)$ from V to $\mathbb{R}$ is bilinear.*

And finally, we can prove the following important fact about Jordan frames.

Proposition 43. *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra of rank r, then $\operatorname{trace}(c) = 1$ for any primitive idempotent $c \in V$, and any Jordan frame in V has exactly r elements.*

Proof. We showed in Exercise 29 that any primitive idempotent has exactly one non-zero eigenvalue $\lambda_1 = 1$ and that therefore $\operatorname{trace}(c) = \lambda_1 + 0 + 0 + \cdots + 0 = 1$. Now, the elements of any Jordan frame must sum to the unit element by definition, and $\operatorname{trace}(1_V) = r$ from Example 62. So if $\{c_1, c_2, \ldots, c_k\} \subseteq V$ is a Jordan frame, then by linearity, $\operatorname{trace}(1_V) = r = \sum_{i=1}^{k} \operatorname{trace}(c_k) = k$. We conclude that $k = r$. □

10.5 Solutions to exercises

Solution to Exercise 28 (eigenvalues of idempotents). First note that if $c = 0$, then the minimal polynomial of c is $\Lambda \in \mathbb{R}[\Lambda]$, as we showed in Exercise 20. Likewise, if $c = 1_V$, then we showed in Example 50 that the minimal polynomial of c is $\Lambda - 1\mathbb{R}[\Lambda]$.

If neither c nor $(1_V - c)$ is zero, then $\{c, 1_V - c\}$ is a complete system of nonzero orthogonal idempotents, and Proposition 36 can be applied to the expression $c = 1c + 0\,(1_V - c)$ to conclude that $\mu_c = \Lambda\,(\Lambda - 1)$. In any case, the eigenvalues of c (the roots of its minimal polynomial) are contained in the set $\{0, 1\}$. Its minimal polynomial is thus of the form $\mu_c = \Lambda^{m_1}\,(\Lambda - 1)^{m_2}$ for $m_1, m_2 \in \{0, 1\}$, and its characteristic polynomial is therefore of the form $\Lambda^k\,(\Lambda - 1)^{r-k}$ for some $k \in \{0, 1, \ldots, r\}$.

Solution to Exercise 29 (eigenvalues of primitive idempotents). Suppose c is primitive and thus non-zero. Exercise 28 showed that γ_c is of the form $\Lambda^k\,(\Lambda - 1)^{r-k}$ for some k, but if $k < r - 1$, then the full spectral decomposition of c looks like $c = 1d_1 + 1d_2 + \cdots + \lambda_r d_r$, contradicting the fact that c was supposed to be primitive. As a result, $k \geq r - 1$, but k cannot be equal to r since that would make c equal to zero.

Chapter 11

Peirce decompositions

The Peirce decomposition (pronounced "purse") is a bigger idea from the theory of algebras. To get started, we'll need one final polarization identity.

Proposition 44. *If* $(V, \circ, \langle \cdot, \cdot \rangle)$ *is a Euclidean Jordan algebra, then*

Faraut and Korányi Proposition II.1.1.iii

$$\forall x, z \in V : 2L_x L_z L_x + L_{(x^2 \circ z)} = 2L_{(x \circ z)} L_x + L_{(x^2)} L_z. \tag{11.1}$$

Proof. Apply both sides of the polarization identity Equation (7.1) to an arbitrary $z \in V$:

$$\forall x, y, z \in V : 2L_x L_{(x \circ y)}(z) + L_y L_{x^2}(z) = 2L_{(x \circ y)} L_x(z) + L_{x^2} L_y(z),$$

Expand what this means,

$$\forall x, y, z \in V : \begin{cases} 2(x \circ ((x \circ y) \circ z)) + y \circ (x^2 \circ z) \\ = \\ 2((x \circ y) \circ (x \circ z)) + x^2 \circ (y \circ z) \end{cases},$$

use the commutativity of the Jordan product to rearrange,

$$\forall x, y, z \in V : \begin{cases} 2(x \circ (z \circ (x \circ y))) + (x^2 \circ z) \circ y \\ = \\ 2((x \circ z) \circ (x \circ y)) + x^2 \circ (z \circ y) \end{cases},$$

and then put things back in terms of left-multiplication-by operators acting on y, now, instead of z:

$$\forall x, y, z \in V : 2L_x L_z L_x(y) + L_{(x^2 \circ z)}(y) = 2L_{(x \circ z)} L_x(y) + L_{(x^2)} L_z(y).$$

Since this holds for all $y \in V$, we conclude that the operators on both sides are equal, which was the desired result. □

11.1 With respect to an idempotent

Exercise 30 (Peirce decomposition). Suppose that $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, and let $c \in V$ be idempotent. Substitute c for both x and z in Proposition 44 to obtain a polynomial expression in L_c that is equal to zero.

Factor your expression, and use standard linear algebra (particularly, what you know about the minimal polynomial of L_c) to find a set of three real numbers that contains all of eigenvalues of L_c. Conclude that V decomposes into an orthogonal direct sum of three eigenspaces. (Use the convention that if λ is not an eigenvalue of L_c, then the eigenspace of L_c corresponding to λ is $\{0\}$.)

If you solved Exercise 30, then you know that for any idempotent c in a Euclidean Jordan algebra V, the operator L_c has at most three eigenvalues, all coming from the set $\left\{0, \frac{1}{2}, 1\right\}$. Since L_c is self-adjoint with respect to the algebra's inner product, the vector space V therefore decomposes into an orthogonal direct sum of the three (possibly-trivial) eigenspaces,

$$V = V(c, 0) \oplus V\left(c, \frac{1}{2}\right) \oplus V(c, 1),$$

where, for example, $V(c, 0)$ denotes the eigenspace of L_c in V corresponding to the eigenvalue $\lambda = 0$. This notation is fairly standard, so let's make it official.

Definition 70 (Peirce subspaces, part 1)**.** If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $c \in V$ is idempotent, then we define

$$V(c, \lambda) \coloneqq \{x \in V \mid L_c(x) = \lambda x\}$$

to be the eigenspace of L_c corresponding to the eigenvalue $\lambda \in \left\{0, \frac{1}{2}, 1\right\}$.

Examples of Peirce subspaces abound. Let's start with something trivial.

Example 65. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is any Euclidean Jordan algebra, then 1_V is idempotent, and $1_V \circ x = x$ for all $x \in V$. As a result, 1_V has only the single eigenvalue $\lambda = 1$ whose corresponding eigenspace is $V(1_V, 1) = V$. Its other two eigenspaces are then necessarily $V(1_V, 0) = V\left(1_V, \frac{1}{2}\right) = \{0\}$. You can of course write $V = V \oplus \{0\} \oplus \{0\}$ if you so desire. An equally-silly decomposition arises from the idempotent $0 \in V$.

Example 66. Let $c = \frac{1}{2}\left(1, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)^T$ in the Jordan Spin EJA on $\mathbb{R}^5$. A quick check shows that $c^2 = c$. With respect to the standard basis $\mathbf{b}$ in $\mathbb{R}^n$, we can "compute" the matrix of L_c by substituing the entries of c into a matrix of the form we found in Example 58:

$$\mathbf{b}(L_c) = \begin{bmatrix} c_1 & c_2 & c_3 & c_4 & c_5 \\ c_2 & c_1 & 0 & 0 & 0 \\ c_3 & 0 & c_1 & 0 & 0 \\ c_4 & 0 & 0 & c_1 & 0 \\ c_5 & 0 & 0 & 0 & c_1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & \frac{1}{2} & 0 & 0 & 0 \\ 1/4 & 0 & \frac{1}{2} & 0 & 0 \\ 1/4 & 0 & 0 & \frac{1}{2} & 0 \\ 1/4 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

If we ask a computer to find the eigenspaces of this matrix, we see that

$$V(c,0) = \operatorname{span}\left(\begin{bmatrix} 1/2 \\ -1/4 \\ -1/4 \\ -1/4 \\ -1/4 \end{bmatrix}\right), \quad V(c,1) = \operatorname{span}\left(\begin{bmatrix} 1/2 \\ 1/4 \\ 1/4 \\ 1/4 \\ 1/4 \end{bmatrix}\right),$$

$$V\left(c, \frac{1}{2}\right) = \operatorname{span}\left(\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ -1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ -1 \end{bmatrix}\right).$$

Two of the Peirce subspaces in Definition 70 are special in that they not only form vector subspaces of V, but in fact form subalgebras.

Proposition 45. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra and if $c \in V$ is idempotent, then $V(c,0)$ and $V(c,1)$ form Euclidean Jordan subalgebras of V. Moreover, the unit element of $V(c,1)$ is c.*

Proof. As is typical of these sorts of proofs, we show only that the two subspaces $V(c,0)$ and $V(c,1)$ are closed under the given Jordan product. All that would then remain, if we are being pedantic (and we are), is to restrict the Jordan and inner-product from the superalgebra onto the subspaces.

To show that $V(c,0)$ is closed, take any $z, w \in V(c,0)$. Set $x \coloneqq c$ and z be itself in Equation (11.1). Using $c^2 = c$ and $c \circ z = 0$, we can cancel two terms immediately,

$$\begin{gathered} 2L_c L_z L_c + L_{(c^2 \circ z)} = 2L_{(c \circ z)} L_c + L_{(c^2)} L_z \\ \iff \\ 2L_c L_z L_c = L_{(c^2)} L_z. \end{gathered}$$

Again we can replace the remaining c^2 by c, and apply both sides of this equation to our $w \in V(c,0)$ to find that

$$2L_c L_z (c \circ w) = L_c (z \circ w).$$

The left-hand side here is zero, because $c \circ w$ is. Thus we conclude that $z \circ w$ is an eigenvector of L_c corresponding to $\lambda = 0$. Since z, w were arbitrary elements of $V(c,0)$, this shows that $V(c,0)$ is closed under the given Jordan product.

The idea for $V(c,1)$ is similar. Take $z, w \in V(c,1)$. Set $x \coloneqq c$ and let z be itself in Equation (11.1). Using $c^2 = c$ and $c \circ z = z$,

$$\begin{gathered} 2L_c L_z L_c + L_{(c^2 \circ z)} = 2L_{(c \circ z)} L_c + L_{(c^2)} L_z \\ \iff \\ 2L_c L_z L_c + L_z = 2L_z L_c + L_c L_z. \end{gathered}$$

If we apply both sides to $w = c \circ w$ and start rearranging things,

$$\begin{gathered} 2L_c L_z (c \circ w) + z \circ w = 2L_z (c \circ w) + L_c (z \circ w) \\ \iff \\ 2L_c (z \circ w) + z \circ w = 2 (z \circ w) + L_c (z \circ w) \\ \iff \\ L_c (z \circ w) = z \circ w. \end{gathered}$$

As before, this completes the proof that $V(c, 1)$ is closed. It goes without saying that c lives in $V(c, 1)$, and that $c \circ bx = x$ for all x in $V(c, 1)$ by definition. It follows that c is the unit element in the algebra $V(c, 1)$. □

11.2 With respect to a Jordan frame

Definition 71 (Peirce subspaces, part 2)**.** If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra of rank r and if $\mathbf{c} \coloneqq \{c_1, c_2, \ldots, c_r\}$ is a Jordan frame in V, then the *diagonal Peirce subalgebras* of V are

$$V_{ii}(\mathbf{c}) \coloneqq V(c_i, 1)$$

and the *off-diagonal Peirce subspaces* of V are

$$V_{ij}(\mathbf{c}) \coloneqq V\left(c_i, \frac{1}{2}\right) \cap V\left(c_j, \frac{1}{2}\right).$$

11.3 Some consequences

Faraut and Korányi Lemma X.2.2

Lemma 11. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra of rank r and if $x, y \in V$ operator-commute, then there exists a Jordan frame $\{c_1, c_2, \ldots, c_r\}$ and sets of real numbers $\{\lambda_1, \lambda_2, \ldots, \lambda_r\}$ and $\{\mu_1, \mu_2, \ldots, \mu_r\}$ such that*

$$x = \lambda_1 c_1 + \lambda_2 c_2 + \cdots + \lambda_r c_r \quad \text{and} \quad y = \mu_1 c_1 + \mu_2 c_2 + \cdots + \mu_r c_r.$$

In other words, x and y have full Euclidean Jordan algebra spectral decompositions with respect to the same Jordan frame. Conversely, if x and y have full spectral decompositions with respect to a common Jordan frame, then x and y operator-commute.

Proof. The converse is easy: the elements of a Jordan frame are orthogonal idempotents, so Corollary 11 applies.

For the other direction. Let x have unique the spectral decomposition $x = \lambda_1 d_1 + \lambda_2 d_2 + \cdots + \lambda_k d_k$ where $k < r$ and where $\mathbf{d} \coloneqq \{d_1, d_2, \ldots, d_k\}$ is a complete system of (not necessarily primitive) orthogonal idempotents. With respect to $\mathbf{d}$, we can consider the Peirce decomposition of y,

$$\begin{aligned} y &= \sum_{i=1}^{k} \sum_{j=1}^{i} y_{ij} = \sum_{i=1}^{k} y_{ii} + \sum_{i=1}^{k} \sum_{j=1}^{i-1} y_{ij}, \\ y_{ij} &\in V_{ij}(\mathbf{d}). \end{aligned}$$

Our goal will be to use the fact that x and y operator-commute to show that the $y_{ij} = 0$ whenever $j \neq i$. We'll do this by applying the operator $L_y L_x - L_x L_y = 0$ to x itself, so there are a few intermediate terms for us to compute. First,

$$y \circ x = \sum_{i=1}^{k} \sum_{m=1}^{k} \lambda_m \left(y_{ii} \circ d_m \right) + \sum_{i=1}^{k} \sum_{j=1}^{i-1} \sum_{m=1}^{k} \lambda_m \left(y_{ij} \circ d_m \right).$$

We know that $d_m \in V(d_m, 1)$, and using Proposition IV.1.1 in Faraut and Korányi, we see that $V_{ii}(\mathbf{d}) \circ V_{mm}(\mathbf{d}) = \{0\}$ when $m \neq i$. Thus the products $y_{ii} \circ d_m$ are nonzero only when $m = i$. Similarly, Theorem IV.2.1 in Faraut and Korányi shows that $V_{mm}(\mathbf{d}) \circ V_{ij}(\mathbf{d})$ is nonzero only when $m = i$ or $m = i$. We therefore need only retain two terms (corresponding to $m = i$ and $m = j$ of the sum $\sum_{m=1}^{k} \lambda_m \left(y_{ij} \circ d_m \right)$). After making both of these simplifications, we're left with

$$y \circ x = \sum_{i=1}^{k} \lambda_i \left(y_{ii} \circ d_i \right) + \sum_{i=1}^{k} \sum_{j=1}^{i-1} \lambda_i \left(y_{ij} \circ d_i \right) + \lambda_j \left(y_{ij} \circ d_j \right).$$

Now we use the fact that y_{ii} is an eigenvectors of L_{d_i} with eigenvalue one, and that y_{ij} is an eigenvector of both L_{d_i} and L_{d_j}, both with eigenvalues one-half:

$$y \circ x = \sum_{i=1}^{k} \lambda_i y_{ii} + \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \lambda_i y_{ij} + \lambda_j y_{ij}$$

That's it for $y \circ x$. We also need to know $y \circ x^2$, but there's a shortcut for that. Simply compute

$$x \circ x = \left(\sum_{i=1}^{k} \lambda_i d_i \right) \circ \left(\sum_{j=1}^{k} \lambda_j d_j \right) = \sum_{i=1}^{k} \sum_{j=1}^{k} \lambda_i \lambda_j \left(d_i \circ d_j \right) = \sum_{i=1}^{k} \lambda_i^2 d_i$$

where the last equality follows since $d_i \circ d_j$ is non-zero only when $j = i$. Thus x^2 has the same spectral decomposition as x itself... except with the eigenvalues squared. So to compute $y \circ x^2$, we can simply replace each λ_i with λ_i^2 in the expression for $y \circ x$:

$$y \circ x^2 = \sum_{i=1}^{k} \lambda_i^2 y_{ii} + \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \lambda_i^2 y_{ij} + \lambda_j^2 y_{ij}$$

Finally, we'll need to know $x \circ (y \circ x)$. There are no new tricks here, just more

tedious computation with $x = \sum_{m=1}^{k} \lambda_m d_m$:

$$\begin{aligned} x \circ (y \circ x) = &\sum_{i=1}^{k} \sum_{m=1}^{k} \lambda_m \lambda_i \left(d_m \circ y_{ii}\right) \\ &+ \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \sum_{m=1}^{k} \lambda_m \lambda_i \left(d_m \circ y_{ij}\right) \\ &+ \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \sum_{m=1}^{k} \lambda_m \lambda_j \left(d_m \circ y_{ij}\right). \end{aligned}$$

By exactly the same reasoning we applied earlier, each of these lines can be expanded and/or simplied to,

$$\begin{aligned} x \circ (y \circ x) = &\sum_{i=1}^{k} \lambda_i^2 y_{ii} \\ &+ \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \lambda_i^2 \frac{1}{2} y_{ij} + \lambda_j \lambda_i \frac{1}{2} y_{ij} \\ &+ \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \lambda_i \lambda_j \frac{1}{2} y_{ij} + \lambda_j^2 \frac{1}{2} y_{ij}, \end{aligned}$$

which leaves us with

$$x \circ (y \circ x) = \sum_{i=1}^{k} \lambda_i^2 y_{ii} + \frac{1}{4} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \left(\lambda_i^2 + 2\lambda_i \lambda_j + \lambda_j^2\right) y_{ij}.$$

Now, we are ready to start the problem! Recall that $L_y L_x - L_x L_y$ is the zero operator, and apply it to $x \in V$ to conclude that $y \circ x^2 - x \circ (y \circ x) = 0$. Substitute in the two big expressions that we just found for those terms, and conclude that

$$\begin{aligned} 0 &= \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \lambda_i^2 y_{ij} + \lambda_j^2 y_{ij} - \frac{1}{4} \sum_{i=1}^{k} \sum_{j=1}^{i-1} \left(\lambda_i^2 + 2\lambda_i \lambda_j + \lambda_j^2\right) y_{ij} \\ &= \sum_{i=1}^{k} \sum_{j=1}^{i-1} \left(\frac{1}{4} \lambda_i^2 - \frac{1}{2} \lambda_i \lambda_j + \frac{1}{4} \lambda_j^2\right) y_{ij} \\ &= \sum_{i=1}^{k} \sum_{j=1}^{i-1} \left(\frac{\lambda_i - \lambda_j}{2}\right)^2 y_{ij}. \end{aligned}$$

Since the y_{ij} live in orthogonal vector spaces, the only way this sum can be zero is if each term is zero. The lambdas were distinct, and j is strictly less than i in each of the terms, so in particular it is not equal to i and $\lambda_i - \lambda_j \neq 0$. We conclude that each y_{ij} is zero above, and that therefore $y = \sum_{i=1}^{k} y_{ii}$.

Recall now that each pair of x_{ii} and y_{ii} in $V_{ii} = V(d_i, 1)$ live in the same sub*algebra* (this was Proposition 45). Within each V_{ii} where d_i is the unit element, we can therefore use the full EJA spectral theorem to decompose

$$y_{ii} = \sum_{\ell=1}^{p_i} \mu_\ell d_{i,\ell},$$

where $d_{i,1}, d_{i,2}, \ldots, d_{i,p_i}$ are orthogonal primitive idempotents that sum up to d_i. Adding everything up, we get

$$y = \sum_{i=1}^{k} y_{ii} = \sum_{i=1}^{k} \sum_{\ell=1}^{p_i} \mu_\ell d_{i,\ell},$$

which must be the full spectral decomposition of y in V itself: in the the full collection of all $d_{i,\ell}$, the idempotents remain orthogonal and primitive since the spaces V_{ii} are orthogonal to one another. But we can also decompose x in terms of this Jordan frame! Since $d_i = \sum_{\ell=1}^{p_i} d_{i,\ell}$, we have

$$x = \sum_{i=1}^{k} \lambda_i d_j = \sum_{i=1}^{k} \sum_{\ell=1}^{p_i} \lambda_i d_{i,\ell}.$$

After relabeling some subscripts, these are two full spectral decompositions of x and y with respect to the same Jordan frame. □

The preceding lemma is a powerful tool. Here is an example application.

Theorem 36. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra of rank r and if $x \in V$, then $\det(x) \neq 0$ if and only if x is invertible.*

Proof. If $\det(x) \neq 0$, then we have already seen in Proposition 39 how to construct the inverse of x.

Conversely, if $\det(x) = 0$, then by Corollary 19, some eigenvalue of x is zero. Use the full EJA spectral theorem to write $x = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_r e_r$, and suppose without loss of generality that $\lambda_1 = 0$. If x were invertible, it would operator-commute with x^{-1}, so we use Lemma 11 to write $x^{-1} = \mu_1 e_1 + \mu_2 e_2 + \cdots + \mu_r e_r$. Now $x \circ x^{-1}$ is supposed to be 1_V; however, multiplying out the spectral decompositions gives an expression involving only $e_2, e_3, \ldots, e_r$. Notably, e_1 is missing. Since $1_V = e_1 + e_2 + \cdots + e_r$, this is a contradiction: e_1 cannot be replaced by a linear combination of the remaining elements of the Jordan frame. □

Corollary 22. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra of rank r and if $x \in V$ is invertible with full spectral decomposition $x = \sum_{i=1}^{r} \lambda_i c_i$, then its inverse is $x^{-1} = \sum_{i=1}^{r} \lambda_i^{-1} c_i$.*

Proof. Since x is invertible, we have $\prod_{i=1}^{r} \lambda_i = \det(x) \neq 0$ by Corollary 19 and Theorem 36, so each eigenvalue λ_i must be nonzero. We can therefore legally define $y \coloneqq \sum_{i=1}^{r} \lambda_i^{-1} c_i$. It is easy to see that $x \circ y = 1_V$.

The tricky part, then, is showing that $y \in \text{alg}(\{x\})$. The fact that we want to exploit here is that in the unique EJA spectral theorem, each of the idempotents already belongs to $\text{alg}(\{x\})$. The idempotents in the *full* decomposition may not belong to $\text{alg}(\{x\})$, but if you group them by eigenvalues and add them up, you recover the (non-primitive) idempotents from the unique decomposition. We mentioned this briefly in Remark 5.

So, group together all of the c_i that have the same coefficient λ_i^{-1} and relabel them d_j and μ_j^{-1} to obtain $y = \sum_{j=1}^{k} \mu_j^{-1} d_j$, where now the μ_j are distinct, and the d_j form a system of orthogonal (but not necessarily primitive) idempotents. Since $\lambda_i = \lambda_j$ if and only if $\lambda_i^{-1} = \lambda_j^{-1}$, the set $\{d_1, d_2, \ldots, d_k\}$ is exactly the same complete system of orthogonal system of idempotents in the unique spectral decomposition of x, because we obtained them in the same way (by grouping according to coefficients) that we would have if we started with the full spectral decomposition of x. The only change is that we grouped by λ_i^{-1} rather than the λ_i themselves; but, this amounts to the same thing. So, each d_j belongs to $\text{alg}(\{x\})$, and as a result, y itself belongs to $\text{alg}(\{x\})$, since subalgebras are closed under additional and scaling. □

Example 67. Example 63 showed that the standard basis $\{e_1, e_2, \ldots, e_n\}$ forms a Jordan frame in the Hadamard EJA on $\mathbb{R}^n$. If $x = (x_1, x_2, \ldots, x_n)^T$, then we can write

$$x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n.$$

By its uniqueness, this must be the full spectral decomposition of x. Its eigenvalues are therefore $x_1, x_2, \ldots, x_n$, and by Theorem 36, x is invertible if and only if $\det(x) = x_1 x_2 \cdots x_n \neq 0$, which is then equivalent to saying that all coordinates x_i are nonzero.

When x is invertible, Corollary 22 thus shows that

$$x^{-1} = \left(\frac{1}{x_1}\right) e_1 + \left(\frac{1}{x_2}\right) e_2 + \cdots + \left(\frac{1}{x_n}\right) e_n.$$

You should compare this with Example 24.

Corollary 23. *If $(V, \circ, \langle \cdot, \cdot \rangle)$ is a Euclidean Jordan algebra of rank r, then the set of invertible elements of V is dense in V.*

Proof. We show that the set $\{x \in V \mid \det(x) \neq 0\}$ is dense in V; then Theorem 36 can be applied. Let $x \in V$ be given. We aim to find a $y \in V$, arbitrarily close to x, such that $\det(y) \neq 0$. Use the full EJA spectral theorem to write $x = c_1\lambda_1 + c_2\lambda_2 + \cdots + c_r\lambda_r$. If all of the λ_i are nonzero, then great; take $y \coloneqq x$ and we are done. If not, define $y \coloneqq \hat{\lambda}_1 c_1 + \hat{\lambda}_2 c_2 + \cdots + \hat{\lambda}_r c_r$ for some real numbers $\hat{\lambda}_i$ that we imagine to be perturbations of the λ_i. It's easy to see that

$$\|x - y\|^2 = \langle x - y, x - y \rangle = \sum_{i=1}^{r} \left(\lambda_i - \hat{\lambda}_i\right)^2 \|c_i\|^2$$

can be made as small as necessary by choosing the $\hat{\lambda}_i$ nonzero and sufficiently close to λ_i. And if all of the $\hat{\lambda}_i$ are chosen to be nonzero, then

$$\det(y) = \prod_{i=1}^{r} \hat{\lambda}_i \neq 0$$

by Corollary 19. □

11.4 Solutions to exercises

Solution to Exercise 30 (Peirce decomposition). Set $x \coloneqq c$ and $z \coloneqq c$ in Equation (11.1) to obtain

$$2L_c L_c L_c + L_{(c^2 \circ c)} = 2L_{(c \circ c)} L_c + L_{(c^2)} L_c.$$

Simplify using the fact that $c^2 = c$,

$$\begin{aligned} 2L_c L_c L_c + L_c &= 2L_c L_c + L_c L_c \\ &\iff \\ 2L_c^3 - 3L_c^2 + L_c &= 0, \end{aligned}$$

and then factor:

$$\begin{aligned} L_c\left(2L_c^2 - 3L_c + L_c^0\right) &= 0 \\ &\iff \\ L_c\left(2L_c - L_c^0\right)\left(L_c - L_c^0\right) &= 0. \end{aligned}$$

The left-hand side corresponds to the polynomial

$$p \coloneqq X\left(2X - X^0\right)\left(X - X^0\right) \in \mathbb{R}[X],$$

and since the corresponding function $p\restriction_{\mathcal{B}(V)}$ evaluates to zero on L_c, p must be a multiple of the minimal polynomial of L_c. But the roots of $\mu_{L_c}\restriction_{\mathbb{R}}$ are the eigenvalues of L_c, and the roots of $p\restriction_{\mathbb{R}}$ are 0, $\frac{1}{2}$, and 1. Thus if λ is an eigenvalue of L_c, then $\lambda \in \left\{0, \frac{1}{2}, 1\right\}$.

One of the axioms of a Euclidean Jordan algebra says that L_c is self-adjoint with respect to $\langle \cdot, \cdot \rangle$, so the spectral theorem for linear algebra says that V is an orthogonal direct sum of the eigenspaces of L_c. There may be elements of $\left\{0, \frac{1}{2}, 1\right\}$ that are *not* eigenvalues of L_c, for example when $c = 1_V$ and $\lambda = 1$ is the only eigenvalue of L_{1_V}. However, by convention, the eigenspaces associated with the "unused" eigenvalues are the trivial space $\{0\}$, and we can include them in the orthogonal direct sum without changing its value.

Chapter 12

Quadratic representations

If you remember its history from way back in Section 6.1, the Jordan product operation arose as a generalization of the matrix operation $L_A \coloneqq X \mapsto (AX + XA)/2$ defined on the space of real-symmetric or complex-Hermitian matrices. This operation was chosen as the prototype because it preserves symmetry (or conjugate-symmetry), unlike regular matrix multiplication, and therefore results in a bilinear algebra multiplication that is closed: if you multiply two elements of a Jordan algebra, you get another one back.

There is another matrix operation that takes one symmetric matrix to another, and has several other nice properties as well. For any $A \in \mathcal{S}^n$, define the map $P_A \coloneqq X \mapsto AXA$. If we take the domain of P_A to be $\mathcal{S}^n$, then clearly its codomain is also $\mathcal{S}^n$, since

$$(P_A(X))^T = (AXA)^T = A^T X^T A^T = AXA = P_A(X).$$

When A is invertible, this is called a *matrix congruence*.

Definition 72. Two matrices $X, Y \in \mathbb{R}^{n\times n}$ are *congruent* if there exists an invertible $A \in \mathbb{R}^{n\times n}$ such that $Y = A^T XA$.

Matrix congruence has several properties that look nice to us:

- It is an equivalence relation on $\mathcal{S}^n$.
- *Sylvester's law of inertia* states that two real symmetric matrices have the same number of positive, negative, and zero eigenvalues if and only if they are congruent.
- Diagonalizing a real symmetric matrix as in the spectral theorem for linear algebra is a special case of congruence where the invertible matrix happens to be orthogonal.
- *Unitary similarity invariance*: if U is any orthogonal matrix, then X and UXU have the same eigenvalues.

Recall the change-of-basis formula from Example 21. If you start with a representation $\mathbf{e}(L)$ of a linear operator $L \in \mathcal{B}(V)$ with respect to a basis $\mathbf{e} \subseteq V$, then its representation $\mathbf{b}(L)$ with respect to another basis $\mathbf{b}$ can be found by applying the similarity transformation $X \mapsto \mathbf{e}\left(A^{-1}\right) X \mathbf{e}(A)$ to the matrix $X = \mathbf{e}(L)$. Here, as in Example 21, $A \in \mathcal{B}(V)$ is the invertible operator that sends $\mathbf{e}$ to $\mathbf{b}$.

Congruence captures this same notion of a "change of basis," but for an inner-product rather than a linear operator. Every inner product on a finite-dimensional real vector space is of the form $(x, y) \mapsto \langle \mathbf{b}(L)\mathbf{b}(x), \mathbf{b}(y)\rangle_{\mathbb{R}^n}$ for some self-adjoint positive-definite $L \in \mathcal{B}(V)$ and basis $\mathbf{b}$ of V (we prove this later in Proposition 48.) Since $\mathbf{e}\left(A^{-1}(z)\right) = \mathbf{b}(z)$ for all z in V,

$$\begin{aligned}
&\langle \mathbf{b}(L)\mathbf{b}(x), \mathbf{b}(y)\rangle_{\mathbb{R}^n} \\
&= \left\langle \mathbf{b}(L)\mathbf{e}\left(A^{-1}x\right), \mathbf{e}\left(A^{-1}y\right)\right\rangle_{\mathbb{R}^n} \\
&= \left\langle \mathbf{b}(L)\mathbf{e}\left(A^{-1}\right)\mathbf{e}(x), \mathbf{e}\left(A^{-1}\right)\mathbf{e}(y)\right\rangle_{\mathbb{R}^n} \\
&= \left\langle \mathbf{e}\left(A^{-1}\right)^T \mathbf{b}(L)\mathbf{e}\left(A^{-1}\right)\mathbf{e}(x), \mathbf{e}(y)\right\rangle_{\mathbb{R}^n}.
\end{aligned}$$

As you may suspect, all of these concepts can be extended to complex inner-product spaces whose representation matrices have entries in $\mathbb{C}$, and where the conjugate-transpose is used in place of the transpose. One nice property that P_X does *not* have, however, is linearity. Clearly, $X \mapsto P_X$ is not a linear function, and thus $(X, Y) \mapsto P_X(Y)$ is not bilinear, since for any $\alpha \in \mathbb{R}$,

$$P_{(\alpha X)}(Y) = (\alpha X)\, Y\, (\alpha X) = \alpha^2 P_X(Y).$$

The appearance of a squared term there is where the name *quadratic representation* comes from. Is there a way to express P_X in terms of the Jordan product L_X on $\mathcal{S}^n$, and vice-versa? Indeed there is.

Definition 73 (Quadratic representation)**.** If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then then *quadratic representation* of x is the operator,

$$\begin{aligned}
P_x &: V \to V \\
P_x &\coloneqq 2L_x^2 - L_{x^2}.
\end{aligned}$$

In other words, P_x is the map $y \mapsto 2(x \circ (x \circ y)) - x^2 \circ y$.

As you should expect by now, the quadratic representation of X in the Real Symmetric EJA is nothing other than the map $Y \mapsto X^T Y X$. Note that, unlike $x \mapsto L_x$, the map $x \mapsto P_x$ is *not* linear. The resulting operator P_x is however linear on V for any x.

Example 68. If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $X, Y \in V$,

then

$$\begin{aligned} P_X(Y) &= 2(X \circ (X \circ Y)) - X^2 \circ Y \\ &= 2\left(X \circ \frac{XY + YX}{2}\right) - \frac{X^2Y + YX^2}{2} \\ &= \frac{X^2Y + XYX + XYX + YX^2}{2} - \frac{X^2Y + YX^2}{2} \\ &= XYX. \end{aligned}$$

Since X is symmetric, we could just as well have written this result as X^TYX.

So this not only shows that P_x can be expressed in terms of L_x, but it also motivates our definition of P_x in a general Euclidean Jordan algebra: it's a generalization of matrix conjugation. The quadratic representation also shares several nice properties with matrix conjugation.

Exercise 31 (properties of the quadratic representation). Suppose that $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra, that $\alpha \in \mathbb{R}$, and that $x, y \in V$. Prove the following easy properties of the quadratic representation using the definitions and (in one case) the polarization identity Equation (11.1).

1. P_x and L_x commute as operators.
2. $P_{\alpha x} = \alpha^2 P_x$.
3. $P_x(1_V) = x^2$.
4. If x is invertible, then $P_x\left(x^{-1}\right) = x$.
5. If x is invertible, then $P_x L_{(x^{-1})} = L_x$.

Proposition 46 (Inverse of quadratic representation)**.** *If $(V, \circ, \langle\cdot,\cdot\rangle)$ is a Euclidean Jordan algebra and if $x \in V$, then x is invertible if and only if P_x is invertible; and in either case, we have $(P_x)^{-1} = P_{(x^{-1})}$.*

Proof. Suppose x is invertible. Set $z := x^{-2}$ in Equation (11.1) and simplify,

$$\begin{aligned} 2L_xL_{x^{-2}}L_x + L_{(x^2 \circ x^{-2})} &= 2L_{(x \circ x^{-2})}L_x + L_{(x^2)}L_{x^{-2}} \\ &\iff \\ L_{1_V} &= 2L_xL_{x^{-2}}L_x + 2L_{(x \circ x^{-2})}L_x + L_{(x^2)}L_{x^{-2}} \\ &\iff \\ \mathrm{id}_V &= 2L_xL_{x^{-2}}L_x + 2L_{x^{-1}}L_x + L_{(x^2)}L_{x^{-2}}. \end{aligned}$$

Now rearrange things a bit using the fact that L_x, L_{x^2} and $L_{x^{-2}}$ all commute by Corollaries 11 and 22:

$$\begin{gathered}
\mathrm{id}_V = 2L_xL_{x^{-2}}L_x + 2L_{x^{-1}}L_x + L_{(x^2)}L_{x^{-2}} \\
\Longleftrightarrow \\
\mathrm{id}_V = 2L_x^2L_{x^{-2}} + L_{(x^2)}L_{x^{-2}} + 2L_{x^{-1}}L_x \\
\Longleftrightarrow \\
\mathrm{id}_V = \left[2L_x^2 + L_{(x^2)}\right]L_{x^{-2}} + 2L_{x^{-1}}L_x.
\end{gathered}$$

Observe now that the grouped expression above is simply P_x. Moreover, using the result from Exercise 31, we can replace L_x by $P_xL_{x^{-1}}$:

$$\mathrm{id}_V = P_xL_{x^{-2}} + 2L_{x^{-1}}P_xL_{x^{-1}}$$

Once more we note that P_x commutes with $L_{x^{-1}}$, since both L_x and L_{x^2} do. Thus we can factor this as,

$$\begin{aligned}
\mathrm{id}_V &= P_xL_{x^{-2}} + 2L_{x^{-1}}P_xL_{x^{-1}} \\
&= P_x\left[L_{x^{-2}} + 2L_{x^{-1}}L_{x^{-1}}\right] \\
&= P_xP_{x^{-1}},
\end{aligned}$$

showing that $P_{x^{-1}}$ acts as an inverse to P_x.

For the other direction we assume that P_x^{-1} exists, and start by showing that $P_x^{-1}\left(\mathrm{alg}\left(\{x\}\right)\right) = \mathrm{alg}\left(\{x\}\right)$. From the definition of P_x it is clear that $P_x\left(\mathrm{alg}\left(\{x\}\right)\right) \subseteq \mathrm{alg}\left(\{x\}\right)$, but the dimensions of the two vector spaces must be the same if P_x is invertible. If one vector space of dimension n is contained in another vector space of dimension n, then they must be equal; hence $P_x\left(\mathrm{alg}\left(\{x\}\right)\right) = \mathrm{alg}\left(\{x\}\right)$, and we can apply P_x^{-1} to both sides.

Next we note that L_x and P_x^{-1} commute. We already know that P_x and L_x commute from Exercise 31, so write both

$$L_x = P_x^{-1}P_xL_x = P_x^{-1}L_xP_x$$

and

$$L_x = L_xP_x^{-1}P_x.$$

Hitting both of these on the right with P_x^{-1} shows that L_x and P_x^{-1} commute.

Finally, Exercise 31 shows that $P_x\left(1_V\right) = x^2$ which is equivalent to $1_V = P_x^{-1}x^2 = P_x^{-1}L_x\left(x\right)$. Commuting the two operators gives

$$L_xP_x^{-1}\left(x\right) = x \circ \left[P_x^{-1}\left(x\right)\right] = 1_V,$$

implying that $P_x^{-1}\left(x\right)$ acts as an inverse to x. Since $x \in \mathrm{alg}\left(\{x\}\right)$, the argument above shows that $P_x^{-1}\left(x\right) \in \mathrm{alg}\left(\{x\}\right)$ as well, so it is indeed the inverse of x, meaning that x is invertible. The other direction in this proof combined with the uniqueness of the inverse now shows that $P_x^{-1} = P_{x^{-1}}$. □

12.1 Solutions to exercises

Solution to Exercise 31 (properties of the quadratic representation). Item 1 follows immediately from the Jordan identity, which, as in Example 47, says that x and x^2 operator-commute. Item 2 is similarly trivial given that the Jordan product is bilinear by definition, and the map $x \mapsto L_x$ is linear by Proposition 25. Item 3 is simply $P_x(1_V) = 2L_x^2(1_V) - L_{x^2}(1_V) = 2x^2 - x^2 = x^2$. Item 4 is not much harder. Using the fact that x^{-1} lives in the associative subalgebra $\operatorname{alg}(\{x\})$ by Definition 66, $P_x\left(x^{-1}\right) = 2L_x^2\left(x^{-1}\right) - L_{x^2}\left(x^{-1}\right) = 2x - \left(x^2 \circ x^{-1}\right) = 2x - x \circ \left(x \circ x^{-1}\right) = 2x - x = x$. For Item 5, we again need to use the fact that x and x^{-1} operator-commute, which follows since x^{-1} lives in the associative subalgebra $\operatorname{alg}(\{x\})$. With that in mind, simply set $z \coloneqq x^{-1}$ in Equation (11.1) and rearrange.

Chapter 13

The cone of squares

Way back in Section 6.1, we mentioned that Euclidean Jordan algebras are popular in optimization because of something called a *symmetric cone*. It turns out that every symmetric cone comes from some Euclidean Jordan algebra, so if you want to study symmetric cones, you are essentially studying Euclidean Jordan algebras. We have already encountered dual cones in Definition 48. A self-dual cone is a cone K that is equal to its own dual (with $K = K^*$) and a symmetric cone is a just a self-dual cone with one additional property.

Definition 74 (symmetric cone)**.** A cone K in a finite-dimensional real Hilbert space V is *homogeneous* if for all x and y in the interior of K, there exists an invertible $L \in \mathcal{B}(V)$ such that $L(K) = K$ and $L(x) = y$. If K is both self-dual and homogeneous, then it is *symmetric*.

We note that every self-dual cone is proper as in Definition 47, so all symmetric cones (being themselves self-dual) are proper cones too.

13.1 Examples

Recall our three examples of closed convex cones: the nonnegative orthant, the Lorentz cone, and the PSD cone. These will turn out to be self-dual and homogeneous, which means that they must arise from a Euclidean Jordan algebra in some way. The nonnegative orthant arises from the Hadamard EJA, the Lorentz cone arises from the Jordan Spin EJA, and the PSD cone arises from the Real Symmetric EJA. Without knowing any details, a few exercises should still suffice to demonstrate how this happens.

Exercise 32 (nonnegative orthant bijection). In the Hadamard EJA, show that $x \mapsto x \circ x$ is a bijection when restricted to the nonnegative orthant.

Exercise 33 (PSD cone bijection). In the Real Symmetric EJA, show that $x \mapsto x \circ x$ is a bijection when restricted to the PSD cone. For this, you will want to use the unique decomposition in the spectral theorem for linear algebra.

13.2 Solutions to exercises

Solution to Exercise 32 (nonnegative orthant bijection). The operation $x \mapsto x^2$ is easily seen to be surjective, because for all $x \in \mathbb{R}^n_+$, we have

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sqrt{x_1} \\ \sqrt{x_2} \\ \vdots \\ \sqrt{x_n} \end{bmatrix} \circ \begin{bmatrix} \sqrt{x_1} \\ \sqrt{x_2} \\ \vdots \\ \sqrt{x_n} \end{bmatrix}$$

where $\sqrt{x_i}$ is interpreted to mean the unique nonnegative square root of the nonnegative number x_i.

And it's injective, because if $x \neq y$ in $\mathbb{R}^n_+$, then $x_i \neq y_i$ for some index i. But then $\left(x^2\right)_i = x_i^2$ and $\left(y^2\right)_i = y_i^2$ are unequal as real numbers, because x_i and y_i were nonnegative: the only way you can square two different real numbers and get the same real number is if they're negations of one another. Thus $x^2 \neq y^2$, and we conclude that squaring is injective.

Solution to Exercise 33 (PSD cone bijection). To see that $x \mapsto x^2$ is surjective, suppose $x \in \mathcal{S}^n_+$ has the spectral decomposition

$$x = \sum_{i=1}^{I} \lambda_i P_i, \tag{13.1}$$

where the set of pairs $\{(\lambda_i, P_i)\}$ is unique and so on by the spectral theorem for linear algebra. Each λ_i here is nonnegative by Proposition 20, and so it has a unique nonnegative square root $\sqrt{\lambda_i}$. Working in the other direction, that same proposition and the spectral theorem now tell us that

$$\hat{x} \coloneqq \sum_{i=1}^{I} \sqrt{\lambda_i} P_i$$

belongs to $\mathcal{S}^n_+$ because it's symmetric (it's the sum of symmetric projectors) and its eigenvalues are the nonnegative real numbers $\sqrt{\lambda_i}$. Using the fact that Jordan-algebraic squaring is the same thing as matrix-multiplication squaring,

that $P_iP_i = P_i$, and that $P_iP_j = 0$ when $i \neq j$, we conclude that

$$\begin{aligned}
\hat{x}^2 &= \left[\sum_{i=1}^{I} \sqrt{\lambda_i} P_i\right] \left[\sum_{i=1}^{I} \sqrt{\lambda_i} P_i\right] \\
&= \sum_{i=1}^{I} \sum_{j=1}^{I} \sqrt{\lambda_i}\sqrt{\lambda_j} P_i P_j \\
&= \sum_{i=1}^{I} \sqrt{\lambda_i}\sqrt{\lambda_i} P_i P_i + \underbrace{\sum_{i=1}^{I} \sum_{j\neq i} \sqrt{\lambda_i}\sqrt{\lambda_j} P_i P_j}_{=0} \\
&= x.
\end{aligned}$$

For injectivity, it will help to order the eigenvalues. Suppose that x has the same decomposition, except now with its eigenvalues ordered $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_I$—this requires rearranging the projections, but that doesn't invalidate the uniqueness of the whole set of pairs. Now further suppose that

$$y = \sum_{j=1}^{J} \sigma_j Q_j, \tag{13.2}$$

where (σ_j, Q_j) are its (eigenvalue,projection) pairs and $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_J$. Clearly,

$$x = y \iff \{(\lambda_i, P_i)\}_{i=1}^{I} = \{(\sigma_j, Q_j)\}_{j=1}^{J} \tag{13.3}$$

because those sets are uniquely associated with x and y respectively. By squaring both Equations (13.1) and (13.2), we find that

$$x^2 = \sum_{i=1}^{I} \lambda_i^2 P_i \quad \text{and} \quad y^2 = \sum_{j=1}^{J} \sigma_j^2 Q_j.$$

The order of the eigenvalues has not changed here; so, for example, $\lambda_1^2 \geq \lambda_2^2 \geq \cdots \geq \lambda_I^2$. It follows that $\left(\lambda_k^2, P_k\right) \neq \left(\sigma_k^2, Q_k\right)$ in the decompositions of x^2 and y^2, which by Equation (13.3) again shows that $x^2 \neq y^2$. Thus, squaring is injective.

Chapter 14

The classification theorem

The goal of this chapter is to classify, up to isomorphism, every Euclidean Jordan algebra. This incredible result appeared in the original 1934 paper by Jordan, von Neumann, and Wigner. The first step towards proving such a result is to state what we mean by isomorphism—a word that is always context-dependent.

Definition 75. If $(V, \circ, \langle\cdot,\cdot\rangle_V)$ and $(W, \bullet, \langle\cdot,\cdot\rangle_W)$ are two Euclidean Jordan algebras, then $L \in \mathcal{B}(V, W)$ is a Euclidean Jordan algebra *isomorphism* between V and W if it is invertible and if $L(x \circ y) = L(x) \bullet L(y)$ for all $x, y \in V$. Two Euclidean Jordan algebras are said to be *isomorphic* if there exists an isomorphism between them.

Warning 12: Isomorphisms aren't isometries

Typically the word "isomorphism" is used to mean an invertible transformation between two instances of an algebraic structure that preserves the operations defining that structure. For example, a group isomorphism is invertible and preserves group multiplication; a ring isomorphism is invertible and preserves both addition and multiplication, and so on. The inner product is crucial to our definition of a Euclidean Jordan algebra but EJA isomorphisms need not preserve the inner products!

This incongruity stems from the fact that Definition 53 is not the original definition of a Euclidean Jordan algebra. Historically, formally-real Jordan algebras were studied first, and it only later became apparent that they were equivalent to what we call a Euclidean Jordan algebra. As a result, what we're really talking

about are formally-real Jordan algebra isomorphisms, and in a formally-real Jordan algebra there is no a priori inner product for the transformation to preserve.

One easy consequence of this definition of "isomorphism" is that the inner product doesn't affect whether or not two Euclidean Jordan algebras are isomorphic to one another.

Proposition 47. *If $(V, \circ, \langle\cdot,\cdot\rangle_1)$ is a Euclidean Jordan algebra and if $\langle\cdot,\cdot\rangle_2$ is any other inner product on V such that $(V, \circ, \langle\cdot,\cdot\rangle_2)$ is also a Euclidean Jordan algebra, then $(V, \circ, \langle\cdot,\cdot\rangle_1)$ and $(V, \circ, \langle\cdot,\cdot\rangle_2)$ are isomorphic.*

Proof. The identity map on V is linear, invertible, and clearly preserves the Jordan multiplication. Thus it constitutes an isomorphism between $(V, \circ, \langle\cdot,\cdot\rangle_1)$ and $(V, \circ, \langle\cdot,\cdot\rangle_2)$, emphasizing that the inner product does not factor into the concept of Euclidean Jordan algebra isomorphism. □

Every Euclidean Jordan algebra will turn out to be isomorphic to a (finite) Cartesian product of "simple" algebras, and those, in turn, are known to come in only five different flavors. Before we continue, let's look at an additional example of a Euclidean Jordan algebra. We've used the Jordan Spin EJA as an example up until now for simplicity, but the general form of a rank-two "simple" algebra involves a bit more freedom.

14.1 Bilinear forms

Example 69 (Bilinear Form EJA)**.** Let $(W, \langle\cdot,\cdot\rangle_W)$ be a finite-dimensional real inner-product space, and define the Cartesian product space $V \coloneqq \mathbb{R}\times W$. Recall from the discussion preceding Example 46 that the natural inner product on V is

$$\left\langle \begin{bmatrix} x_1 \\ \bar{x} \end{bmatrix}, \begin{bmatrix} y_1 \\ \bar{y} \end{bmatrix} \right\rangle_V = x_1 y_1 + \langle \bar{x}, \bar{y} \rangle_W .$$

If we let $x \coloneqq (x_1, \bar{x})^T$ and $y \coloneqq (y_1, \bar{y})^T$, then we can define a Jordan product on V by

$$x \circ y \coloneqq \begin{bmatrix} x_1 \\ \bar{x} \end{bmatrix} \circ \begin{bmatrix} y_1 \\ \bar{y} \end{bmatrix} = \begin{bmatrix} x_1 y_1 + \langle \bar{x}, \bar{y} \rangle_W \\ y_1 \bar{x} + x_1 \bar{y} \end{bmatrix} = \begin{bmatrix} \langle x, y \rangle_V \\ y_1 \bar{x} + x_1 \bar{y} \end{bmatrix}.$$

With these definitions, $(V, \circ, \langle\cdot,\cdot\rangle_V)$ forms a Euclidean Jordan algebra *regardless* of the inner product on W. The Jordan Spin EJA of dimension n is obtained as a special case by choosing some orthonormal basis $\mathbf{b}$ for W and then taking $\langle \bar{x}, \bar{y} \rangle_W \coloneqq \langle \mathbf{b}(\bar{x}), \mathbf{b}(\bar{y}) \rangle_{\mathbb{R}^{n-1}}$ to be the standard inner product of the basis representations of $\bar{x}$ and $\bar{y}$ in $\mathbb{R}^{n-1}$. The added generality comes from the ability to choose a different inner product on W, if we so choose.

It's fairly easy to characterize the possible inner products that we can put on the space W in the Bilinear Form EJA, which in turn makes it easy to characterize what those algebras look like. To explain the name, we recall the definition of a bilinear form.

Definition 76. If V is a real vector space, then a *bilinear form* on V is a bilinear function $\mathcal{B} : V \times V \to \mathbb{R}$. A bilinear form $\mathcal{B}$ is said to be symmetric if $\mathcal{B}(x, y) = \mathcal{B}(y, x)$ for all $x, y \in V$, and is said to be positive-definite if $\mathcal{B}(x, x) > 0$ for all nonzero $x \in V$.

One can readily define bilinear forms on complex vector spaces; however, the connection between inner products and bilinear forms evinced in the following proposition means that we are usually more interested in the concept of a *sesquilinear form* when our vector spaces are complex.

Proposition 48. *If $(V, \langle \cdot, \cdot \rangle_V)$ is an n-dimensional real vector space and if $\mathcal{B} : (V \times V) \to \mathbb{R}$, then the following are equivalent:*

1. *$\mathcal{B}$ is an inner product on V.*
2. *$\mathcal{B}$ is a symmetric positive-definite bilinear form on V.*
3. *For any basis $\mathbf{b}$ of V, there exists a symmetric positive-definite matrix $B \in \mathbb{R}^{n \times n}$ such that $\mathcal{B} = (x, y) \mapsto \langle B\mathbf{b}(x), \mathbf{b}(y) \rangle_{\mathbb{R}^n}$.*

Proof. The equivalence between inner products and symmetric positive-definite bilinear forms comes straight from Definition 13 and the note in Simplification 1.

To show that the second and third items are equivalent, suppose $\mathcal{B}$ is a bilinear form on V and that $\mathbf{b} \coloneqq \{b_1, b_2, \ldots, b_n\}$ is a basis for V. Then any $x, y \in V$ can be written as $x = \sum_{i=1}^{n} x_i b_i$ and $y = \sum_{j=1}^{n} y_j b_j$, and we have by bilinearity,

$$\mathcal{B}(x, y) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_i \mathcal{B}(b_i, b_j).$$

After we've chosen the basis $\mathbf{b}$, each $\mathcal{B}(b_i, b_j)$ above is some fixed real number; call it b_{ij}, and let $B = \left[B_{ij}\right]$ be the matrix whose i, jth entry is $B_{ij} \coloneqq b_{ji}$. One can now simply compute

$$\langle B\mathbf{b}(x), \mathbf{b}(y) \rangle_{\mathbb{R}^n} = \sum_{j=1}^{n} \left(B\mathbf{b}(x)\right)_j \mathbf{b}(y)_j = \sum_{j=1}^{n} \sum_{i=1}^{n} B_{ji} x_i y_j = \sum_{i=1}^{n} \sum_{j=1}^{n} b_{ij} x_i y_j,$$

which is nothing other than $\mathcal{B}(x, y)$. Thus the two functions $(x, y) \mapsto \mathcal{B}(x, y)$ and $(x, y) \mapsto \langle B\mathbf{b}(x), \mathbf{b}(y) \rangle_{\mathbb{R}^n}$ are identical after fixing the basis $\mathbf{b}$. The fact that B is a symmetric matrix if and only if $\mathcal{B}$ is a symmetric function follows from

$$\underbrace{\forall \mathbf{b}(x), \mathbf{b}(y) \in \mathbb{R}^n}_{\forall x, y \in V} : \underbrace{\langle B\mathbf{b}(x), \mathbf{b}(y) \rangle_{\mathbb{R}^n}}_{\mathcal{B}(x,y)} = \underbrace{\langle \mathbf{b}(x), B\mathbf{b}(y) \rangle_{\mathbb{R}^n}}_{\mathcal{B}(y,x)} \iff B = B^T,$$

By similar reasoning, the matrix B is positive-definite if and only if the bilinear form $\mathcal{B}$ is positive-definite. Thus the second item implies the third.

Conversely, if we are handed a basis $\mathbf{b}$ and the symmetric positive-definite matrix B such that $\mathcal{B} = (x, y) \mapsto \langle B\mathbf{b}(x), \mathbf{b}(y)\rangle_{\mathbb{R}^n}$, then it's fairly evident that $\mathcal{B}$ defines a symmetric positive-definite bilinear form on V. □

Corollary 24. *For every Bilinear Form EJA $\mathcal{A}_1 \coloneqq \left(\mathbb{R} \times W, \circ, \langle\cdot,\cdot\rangle_{\mathbb{R}\times W}\right)$ there exists an orthonormal basis $\mathbf{b}$ of W and symmetric positive-definite matrix $B \in \mathbb{R}^{n-1\times n-1}$ such that $\mathcal{A}_1$ is isomorphic to a Euclidean Jordan algebra $\mathcal{A}_2 \coloneqq \left(\mathbb{R}^n, \bullet, \langle\cdot,\cdot\rangle_{\mathcal{A}_2}\right)$ where*

$$\begin{bmatrix} u_1 \\ \bar{u} \end{bmatrix} \bullet \begin{bmatrix} v_1 \\ \bar{v} \end{bmatrix} \coloneqq \begin{bmatrix} u_1 v_1 + \langle B\bar{u}, \bar{v}\rangle_{\mathbb{R}^{n-1}} \\ v_1\bar{u} + u_1\bar{v} \end{bmatrix}$$

and

$$\left\langle \begin{bmatrix} u_1 \\ \bar{u} \end{bmatrix}, \begin{bmatrix} v_1 \\ \bar{v} \end{bmatrix} \right\rangle_{\mathcal{A}_2} \coloneqq u_1 v_1 + \langle B\bar{u}, \bar{v}\rangle_{\mathbb{R}^{n-1}} .$$

Conversely, every algebra of that form is a Bilinear Form EJA.

Proof. Let $\mathcal{A}_1$ be given; then Proposition 48 says that there exists a basis $\mathbf{b}$ and a symmetric positive-definite matrix $B \in \mathbb{R}^{n-1\times n-1}$ such that $\langle \bar{x}, \bar{y}\rangle_W = \langle B\mathbf{b}(\bar{x}), \mathbf{b}(\bar{y})\rangle_{\mathbb{R}^{n-1}}$. Thus for $x, y \in \mathcal{A}_1$,

$$\begin{aligned} x \circ y &\coloneqq \begin{bmatrix} x_1 y_1 + \langle \bar{x}, \bar{y}\rangle_W \\ y_1\bar{x} + x_1\bar{y} \end{bmatrix} \\ &= \begin{bmatrix} x_1 y_1 + \langle B\mathbf{b}(\bar{x}), \mathbf{b}(\bar{y})\rangle_{\mathbb{R}^{n-1}} \\ y_1\bar{x} + x_1\bar{y} \end{bmatrix} \\ &= \begin{bmatrix} x_1 \\ \mathbf{b}(\bar{x}) \end{bmatrix} \bullet \begin{bmatrix} y_1 \\ \mathbf{b}(\bar{y}) \end{bmatrix} . \end{aligned} \tag{14.1}$$

If we define the map

$$\begin{aligned} \phi &: (\mathbb{R} \times W) \to \mathbb{R}^n \\ \phi &= \begin{bmatrix} x_1 \\ \bar{x} \end{bmatrix} \mapsto \begin{bmatrix} x_1 \\ \mathbf{b}(\bar{x}) \end{bmatrix} , \end{aligned}$$

then it's relatively clear that ϕ is invertible and linear, and is in fact an isometry since $\mathbf{b}$ was chosen to be an orthonormal basis. Equation (14.1) then shows that ϕ preserves the multiplication between the two algebras, and the inner product on $\mathcal{A}_2$ satisfies Equation (6.1) since, using the fact that the inner product on $\mathcal{A}_1$ does,

$$\begin{aligned} \langle x \bullet y, z\rangle_{\mathcal{A}_2} &= \left\langle \phi^{-1}(x \bullet y), \phi^{-1}(z)\right\rangle_{\mathbb{R}\times W} \\ &= \left\langle \phi^{-1}(x) \circ \phi^{-1}(y), \phi^{-1}(z)\right\rangle_{\mathbb{R}\times W} \\ &= \left\langle \phi^{-1}(y), \phi^{-1}(x) \circ \phi^{-1}(z)\right\rangle_{\mathbb{R}\times W} \\ &= \left\langle \phi^{-1}(y), \phi^{-1}(x \circ z)\right\rangle_{\mathbb{R}\times W} \\ &= \langle y, x \bullet z\rangle_{\mathcal{A}_2} . \end{aligned}$$

The converse follows rather easily by letting $W := \mathbb{R}^{n-1}$, and by noting that if we're given any symmetric positive-definite matrix $B \in \mathbb{R}^{n-1\times n-1}$, then $(\bar{u}, \bar{v}) \mapsto \langle B\bar{u}, \bar{v}\rangle_{\mathbb{R}^{n-1}}$ defines an inner product $\langle\cdot,\cdot\rangle_W$ on W by Proposition 48. Thus $(\mathbb{R}^n, \bullet, (u, v) \mapsto u_1 v_1 + \langle B\bar{u}, \bar{v}\rangle_{\mathbb{R}^{n-1}})$ satisfies the definition of a Bilinear Form EJA. □

14.2 Octonions

The Cayley-Dickson construction can be continued. Just as complex numbers can be represented as a pair of real ones—and quaternions can be represented as a pair of complex numbers—we can construct something called an *octonion* as a pair of quaternions. Since quaternions have four real coordinates (two for each complex coordinate), octonions wind up having eight real coordinates. Oct is twice quat; it all makes sense.

Definition 77 (Octonions)**.** If $\{e_1, e_2, \ldots, e_8\}$ is the standard basis in $\mathbb{R}^8$, then the *octonions* is the eight-dimensional non-associative and non-commutative algebra $\mathbb{O}$ obtained by endowing $\mathbb{R}^8$ with the multiplication $\star$ whose action on the standard basis is,

$\star$	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
e_1	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
e_2	e_2	$-e_1$	e_4	$-e_3$	e_6	$-e_5$	$-e_8$	e_7
e_3	e_3	$-e_4$	$-e_1$	e_2	e_7	e_8	$-e_5$	$-e_6$
e_4	e_4	e_3	$-e_2$	$-e_1$	e_8	$-e_7$	e_6	$-e_5$
e_5	e_5	$-e_6$	$-e_7$	$-e_8$	$-e_1$	e_2	e_3	e_4
e_6	e_6	e_5	$-e_8$	e_7	$-e_2$	$-e_1$	$-e_4$	e_3
e_7	e_7	e_8	e_5	$-e_6$	$-e_3$	e_4	$-e_1$	$-e_2$
e_8	e_8	$-e_7$	e_6	e_5	$-e_4$	$-e_3$	e_2	$-e_1$

The *real part* of $x = x_1e_1 + x_2e_2 + \cdots + x_8e_8 \in \mathbb{O}$ is $\Re(x) := x_1e_1$, and its *imaginary part* is the rest of it, namely $\Im(x) := x_2e_2 + x_3e_3 + \cdots + x_8e_8$. Keeping in mind that $x = \Re(x) + \Im(x)$, the *conjugate* of x is $\overline{x} := \Re(x) - \Im(x)$. A norm on $\mathbb{O}$ is given by $\|x\| := \sqrt{x \star \overline{x}}$.

It follows from this definition that $1_{\mathbb{O}} = e_1$ is a multiplicative unit element for the octonions, and that every non-zero $x \in \mathbb{O}$ has an inverse $x^{-1} = \overline{x}/\|x\|^2$. These concepts are essentially the same as the ones for the complex numbers and quaternions, except with the number 8 replacing 2 or 4 respectively. While octonion multiplication is not associative, it is power-associative, so $\mathbb{O}$ is one of the Power-associative algebras.

Convention 14: Octonion notation

From here on out, we denote octonion (and quaternion, and complex, and real) multiplication by simple juxtaposition, omitting the explicit $\star$ operation.

If $\mathbb{O}^{n\times n}$ is the set of square matrices with octonion entries, then with componentwise scaling by real numbers, $\mathbb{O}^{n\times n}$ forms a non-commutative and non-associative algebra over $\mathbb{R}$. The fact that matrix multiplication is not commutative is not a surprise, but it is usually associative when the entries come from a nicer structure. In this algebra we can define the conjugate transpose of a matrix exactly how we did for complex matrices. If $A \in \mathbb{O}^{n\times n}$ has entries a_{ij}, then the conjugate-transpose of A is written A^* and has entries $\overline{a_{ji}}$. We can then say that A is Hermitian if $A^* = A$. The set of Hermitian matrices with octonion entries give rise to a family of Euclidean Jordan algebras just like they did with real, complex, and quaternion entries.

Example 70 (Octonion Hermitian EJA)**.** Let $\mathcal{H}^n(\mathbb{O}) \subseteq \mathbb{O}^{n\times n}$ denote the space of n-by-n Hermitian matrices with octonion entries. If $n \in \{0,1,2,3\}$, then the operation

$$X \circ Y \coloneqq \frac{XY + YX}{2}$$

defines a Jordan product on $\mathcal{H}^n(\mathbb{O})$, and the function

$$(X,Y) \mapsto \Re(\operatorname{trace}(XY))$$

defines an inner-product on $\mathcal{H}^n(\mathbb{O})$ that is compatible with the Jordan product and makes the entire structure into a Euclidean Jordan algebra. We call this the *Octonion Hermitian EJA*.

A few things here deserve comment. We take the real part of the trace in the inner-product because Definition 13 says that the values of the inner-product must lie in the scalar field, and the scalar field here is $\mathbb{R}$. The real part of any octonion will actually be of the form $x_1 e_1$ for $x_1 \in \mathbb{R}$; we are therefore using the canonical embedding $\alpha \mapsto \alpha e_1$ of $\mathbb{R}$ into $\mathbb{O}$ to treat $\Re(x) = x_1 e_1$ as if it were the real number $x_1 \in \mathbb{R}$.

Perhaps more glaring is the fact that we have restricted n to a few specific values, unlike in the past. This is for the non-obvious but straightforward reason that those are the only values of n that work. And three out of the four cases are actually redundant. When $n = 0$, you get the Trivial EJA. When $n = 1$, you get the one-dimensional Hadamard EJA or the Jordan Spin EJA on $\mathbb{R}$ (they're the same thing). And finally, when $n = 2$, you get the Jordan spin algebra on $\mathbb{R}^{10}$.

This is not immediately clear. Define the following basis $\mathbf{b} = \{b_1, b_2, \ldots, b_{10}\}$ for $\mathcal{H}^2(\mathbb{O})$:

$$b_1 \coloneqq \begin{bmatrix} e_1 & 0 \\ 0 & e_1 \end{bmatrix}, b_{10} \coloneqq \begin{bmatrix} e_1 & 0 \\ 0 & -e_1 \end{bmatrix}, \text{ and } b_i \coloneqq \begin{bmatrix} 0 & e_i \\ e_i & 0 \end{bmatrix} \text{ for } i \in \{2, 3, \ldots, 9\}.$$

Notice that $\mathcal{H}^2(\mathbb{O})$ is ten-dimensional over $\mathbb{R}$, and not three-dimensional like you would expect if the entries came from the same place as the scalars. At any rate, now simply compute the multiplication table $b_i \circ b_j$:

$\circ$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}
b_1	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}
b_2	b_2	b_1	0	0	0	0	0	0	0	0
b_3	b_3	0	b_1	0	0	0	0	0	0	0
b_4	b_4	0	0	b_1	0	0	0	0	0	0
b_5	b_5	0	0	0	b_1	0	0	0	0	0
b_6	b_6	0	0	0	0	b_1	0	0	0	0
b_7	b_7	0	0	0	0	0	b_1	0	0	0
b_8	b_8	0	0	0	0	0	0	b_1	0	0
b_9	b_9	0	0	0	0	0	0	0	b_1	0
b_{10}	b_{10}	0	0	0	0	0	0	0	0	b_1

This is exactly the same multiplication table that you get for the Jordan spin algebra on $\mathbb{R}^{10}$ using the standard basis. You don't actually have to check that; just extrapolate the pattern you saw in Example 58. This shows that the two are isomorphic as (Euclidean) Jordan algebras, leaving only $\mathcal{H}^3(\mathbb{O})$ as a possibly new and interesting example.

Definition 78 (Albert EJA)**.** $\mathcal{H}^3(\mathbb{O})$ is called the *Albert algebra*. It's not isomorphic to any of our other examples.

14.3 Simple algebras

The meaning of a simple algebra has something to do with ideals, again.

Definition 79. If M is a commutative algebra over R, then an *algebra ideal* in M is a subset $I \subseteq M$ such that (after restricting the domain and codomain of the algebra operations appropriately),

- I is closed under the addition, multiplication, and scaling operations inherited from M.
- $\forall x \in I, \forall y \in M : x \circ y \in I$.

This is similar to Definition 6 of a ring ideal, except that we require the substructure to be closed under scalar multiplication as well. As with ring ideals, we have been careful not to say that I should be a subalgebra, because

if M has a unit element 1_M, we don't want to require that $1_M \in I$ for I to be an algebra ideal. I believe (but have not personally checked) that this situation is analogous to ring ideals, in that the definition is precisely what we need for the quotient M/I to form an algebra itself.

Definition 80. A Euclidean Jordan algebra is *simple* if its only algebra ideals are the entire space and $\{0\}$.

Jordan, von Neumann, and Wigner refer instead to "irreducible" algebras, where irreducibility means that an algebra cannot be decomposed into a direct sum of two or more proper nontrivial subalgebras. These terms will turn out to mean the same thing in a Euclidean Jordan algebra, but we choose to work with simple algebras at first because doing so requires less justification, and is possibly more familiar from other contexts like Lie algebras where irreducibility and simplicity are quite different.

Theorem 37. *Every Euclidean Jordan algebra is isomorphic to a Cartesian Product EJA whose factors are simple.*

Theorem 38. *Every simple Euclidean Jordan algebra is isomorphic to one of the following:*

1. *a Bilinear Form EJA,*
2. *a Real Symmetric EJA,*
3. *a complex Hermitian EJA,*
4. *a quaternion Hermitian EJA, or*
5. *an Octonion Hermitian EJA.*

More precisely, the only rank-one Euclidean Jordan algebra is the Bilinear Form EJA on $\mathbb{R}$—basically the real numbers with the usual multiplication as its Jordan product and a scalar-multiple of the usual multiplication as its inner-product. Any rank-two algebra is isomorphic to a Bilinear Form EJA of higher dimension, including all of the two-by-two symmetric/Hermitian matrix algebras.

Exercise 34 (complex skew-symmetric EJA). Fix an integer $m \in \mathbb{N}$, and let $n = 2m$. Define the matrix

Faraut and Korányi, Exercise III.1.b

$$J \coloneqq \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \in \mathbb{C}^{2m \times 2m} = \mathbb{C}^{n \times n}$$

(with m-by-m blocks) and consider the *real* vector space,

$$V \coloneqq \left\{ X \in \mathbb{C}^{n \times n} \;\middle|\; X^T = -X \text{ and } XJ = J\overline{X} \right\}.$$

Here, $\overline{X}$ denotes the entrywise complex conjugate. The condition $X^T = -X$ states that these matrices are skew-symmetric but *not* skew-*Hermitian*, as would be more common with matrices whose entries are complex.

Show that this vector space forms a Euclidean Jordan algebra under the Jordan and inner products,

$$X \circ Y \coloneqq (XJY + YJX)/2,$$
$$\langle X, Y \rangle \coloneqq \operatorname{trace}(X^*Y).$$

Compute its dimension, and hazard a guess as to which simple algebra it is Jordan-isomorphic.

Lemma 12. *Suppose that* $(V, \circ, \langle \cdot, \cdot \rangle_V)$ *and* $(W, \bullet, \langle \cdot, \cdot \rangle_W)$ *are two Euclidean Jordan algebras. If* $\{c_1, c_2, \ldots, c_r\}$ *is a Jordan frame for* V *and if* $\{d_1, d_2, \ldots, d_s\}$ *is a Jordan frame for* W*, then*

$$\mathcal{F} \coloneqq \{(c_1, 0), (c_2, 0), \ldots, (c_r, 0)\} \cup \{(0, d_1), (0, d_2), \ldots, (0, d_s)\}$$

is a Jordan frame for the Cartesian product algebra $V \times W$*.*

Proof. It's fairly easy to check that $\mathcal{F}$ is a complete system of orthogonal idempotents using Definition 58. It remains only to show that each element of $\mathcal{F}$ is primitive. Without loss of generality, we show that $(c_1, 0)$ is primitive; the proof for any other element is essentially the same.

Suppose that $(c_1, 0) = (a_1, b_1) + (a_2, b_2)$ for two idempotents $(a_1, b_1) \in V \times W$ and $(a_2, b_2) \in V \times W$. Right away we see that $0 = b_1 + b_2$, implying that $b_1 = -b_2$. But from the pair's idempotence, we also have

$$(a_1, b_1) = (a_1, b_1)^2 \coloneqq \left(a_1^2, b_1^2\right),$$

implying that a_1 and b_1 are themselves idempotent. By the same reasoning, both a_2 and b_2 are idempotent. Squaring both sides of $b_1 = -b_2$ now gives $b_1 = b_2$. Combinining that with the original equation $b_1 = -b_2$ then gives $2b_1 = 0$, or $b_1 = 0$. It follows that $b_2 = -b_1 = 0$ as well.

So, as soon as we wrote $(c_1, 0) = (a_1, b_1) + (a_2, b_2)$, we forced $b_1 = b_2 = 0$. What about a_1 and a_2? Recall that $c_1 = a_1 + a_2$ was not only idempotent, but primitive, since it belongs to a Jordan frame for V. Thus from the idempotence of a_1 and a_2 we conclude that one of either a_1 or a_2 must be zero. Putting everything together, either (a_1, b_1) or (a_2, b_2) must be zero, showing that $(c_1, 0)$ is primitive. □

Theorem 39. *If* $V \coloneqq \bigtimes_{i=1}^m V_i$ *is a Cartesian Product EJA, then* $\operatorname{rank}(V) = \sum_{i=1}^m \operatorname{rank}(V_i)$*. In other words, the rank is additive on a Cartesian product of Euclidean Jordan algebras.*

Proof. We showed in Proposition 43 that every Jordan frame in V has $\operatorname{rank}(V)$ elements. Apply Lemma 12 repeatedly to obtain a Jordan frame for V consisting of $\sum_{i=1}^m \operatorname{rank}(V_i)$ elements and you're done. □

Corollary 25. *If* $V \times W$ *is a Cartesian Product EJA and if* $(x, y) \in V \times W$*, then*

$$\det((x, y)) = \det(x) \det(y).$$

Proof. If $x = \sum_{i=1}^{r} \lambda_i c_i$ is the full spectral decomposition of $x \in V$ and if $y = \sum_{j=1}^{s} \mu_j d_j$ is the full spectral decomposition of $y \in W$, then Lemma 12 and Theorem 39 show that

$$(x, y) = \sum_{i=1}^{r} \lambda_i (c_i, 0) + \sum_{j=1}^{s} \mu_j (0, d_j)$$

is the full spectral decomposition of (x, y). Recalling from Corollary 19 that the determinant of an element is simply the product of its eigenvalues, the spectral decompositions of x, y, and (x, y) make the result obvious. □

14.4 Solutions to exercises

Solution to Exercise 34 (complex skew-symmetric EJA). First, note that V is actually a vector space. It's not quite obvious, but it follows from the fact that both $X^T = -X$ and $XJ = J\overline{X}$ are linear conditions, so V must be a subspace of the *real* vector space $\mathbb{C}^{n\times n}$.

The given Jordan product is "obviously" commutative, so first we check that V is closed under it. Notice that J itself is skew-symmetric; thus we can pull out $(-1)^3$ in

$$(X \circ Y)^T = \left(Y^T J^T X^T + X^T J^T Y^T\right)/2 = -(X \circ Y).$$

Moreover, using $XJ = J\overline{X}$ and likewise for Y,

$$(X \circ Y) J = (XJYJ + YJXJ)/2 = \left(J\overline{X}J\overline{Y} + J\overline{Y}J\overline{X}\right)/2 = J\overline{(X \circ Y)}.$$

Next we check the Jordan identity, using for convenience the identity

$$X^2 \circ Z = \left(X^2 JZ + ZJX^2\right)/2 = (XJXJZ + ZJXJX)/2.$$

Now,

$$X \circ X^2 \circ Y = \frac{XJXJXJY + XJYJXJX + XJXJYJX + YJXJXJX}{4}$$

and

$$X^2 \circ (X \circ Y) = \frac{XJXJXJY + XJXJYJX + XJYJXJX + YJXJXJX}{4}$$

whose terms are equal. The given inner product satisfies the definition of an inner product on any real or complex matrix space (note that the conjugate-transpose is used here), so all that remains is to check that it is associative,

Equation (6.1). Using skew-symmetry and $J\overline{X} = XJ \iff JX = \overline{X}J$,

$$\begin{aligned}
\langle X \circ Y, Z \rangle &= \frac{\operatorname{trace}\left((XJY)^* Z\right) + \operatorname{trace}\left((YJX)^* Z\right)}{2} \\
&= -\frac{\operatorname{trace}\left(\overline{Y}J\overline{X}Z\right) + \operatorname{trace}\left(\overline{X}J\overline{Y}Z\right)}{2}, \\
\langle Y, X \circ Z \rangle &= \frac{\operatorname{trace}\left(Y^* XJZ\right) + \operatorname{trace}\left(Y^* ZJX\right)}{2} \\
&= -\frac{\operatorname{trace}\left(\overline{Y}XJZ\right) + \operatorname{trace}\left(\overline{Y}ZJX\right)}{2} \\
&= -\frac{\operatorname{trace}\left(\overline{Y}J\overline{X}Z\right) + \operatorname{trace}\left(\overline{Y}Z\overline{X}J\right)}{2}.
\end{aligned}$$

Recalling again that $\operatorname{trace}(AB) = \operatorname{trace}(BA)$ for two matrices A and B, these expressions are seen to be equal term-wise.

Finally, we observe that $-J$ serves as the multiplicative unit element in this algebra. It's easy to see that both $-J \in V$ and that $-JJ = I$, so

$$\forall X \in V : -J \circ X = \left[(-JJ)\,X + X\,(-JJ)\right]/2 = X.$$

To ascertain the dimension of V, a little algebra will show that any $X \in V$ has the block form,

$$X = \begin{bmatrix} x_1 & x_2 \\ -\overline{x_2} & \overline{x_1} \end{bmatrix},$$

where x_1 is skew-symmetric and x_2 is Hermitian. (This representation follows from only skew-symmetry and the condition $XJ = J\overline{X}$.) Since x_1 and x_2 are m-by-m, the dimension of V is the sum of the dimensions of the spaces of complex m-by-m skew-symmetric and Hermitian matrices, considered independently as real vector spaces.

For the skew-symmetric block, we have zeros on the diagonal, and thus $\frac{1}{2}\left[(m-1)^2 + (m-1)\right]$ free coordinates, into each of which we can insert either a 1 or an i (the set $\{1, i\}$ forms a basis for $\mathbb{C}$ over $\mathbb{R}$). Thus this block contributes

$$2\frac{(m-1)^2 + (m-1)}{2} = m^2 - m$$

degrees of freedom.

For the Hermitian matrices, there are also $\frac{1}{2}\left[(m-1)^2 + (m-1)\right]$ completely free coordinates, but there's an additional m degrees of freedom on the diagonal where the entries must real. Thus this block contributes m^2 to the total.

Adding these up, we get $\dim(V) = 2m^2 - m$. This is the same dimension as the Quaternion Hermitian EJA of order m, so it is a reasonable guess that the two are Jordan isomorphic.

Chapter 15

Spectral sets and functions

Forthcoming.

Appendices

Appendix A

Convex optimization

A.1 Convex functions

Definition 81. If V is a real vector space and if $X \subseteq V$ is a convex set, then the function $f : X \to \mathbb{R}$ is a *convex function* (on X) if

$$\forall x, y \in X, \forall \alpha \in [0,1] : f(\alpha x + (1-\alpha) y) \leq \alpha f(x) + (1-\alpha) f(y).$$

Note that we need the domain X to be a convex set before we can even state the property above—otherwise how do we know that $\alpha x + (1-\alpha) y$ is in the domain of f?

The importance of Definition 81 is not clear at first, but this next result should clear things up.

Theorem 40. *Suppose that V is a real vector space and that $f : X \to \mathbb{R}$ is differentiable. Then f is convex if and only if* *Boyd, 3.1.3*

$$\forall x, z \in X : f(x+z) \geq f(x) + \langle \nabla f(x), z \rangle.$$

In particular this theorem says that if $x \in X$ is a local minimum (that is, if we have $\nabla f(x) = 0$), then x is in fact the global minimum of f on X.

Example 71. If V is a real vector space and if $f : V \to V$ is linear, then f is convex on V.

This is fairly trivial: if $x, y \in V$ and if $\alpha \in [0,1]$, then of course we have

$$f(\alpha x + (1-\alpha) y) \leq \alpha f(x) + (1-\alpha) f(y)$$

in Definition 81, because the Definition 32 of a linear operator says that

$$f(\alpha x + (1-\alpha) y) = \alpha f(x) + (1-\alpha) f(y).$$

Nevertheless, linear functions are probably the most important examples of convex functions.

Exercise 6. *Prove that affine functions are convex, too.*

Proposition 49. *If V is a real vector space and if $f : V \to \mathbb{R}$ is convex on a convex subset X of V, then the set*

Boyd, 3.1.6

$$f^{-1}([-\infty, \alpha]) = \{x \in X \mid f(x) \leq \alpha\}$$

is convex for any $\alpha \in \mathbb{R}$.

Definition 82. If V is a real vector space, if $X \subseteq V$ is a convex set, and if $f : X \to \mathbb{R}$ and $g_1, g_2, \ldots, g_m : V \to \mathbb{R}$ are convex functions, then

Boyd, 1.3 and 4.1.1

$$\begin{aligned} &\text{minimize } f(x) \\ &\text{subject to } g_1(x) \leq 0 \\ &\qquad\qquad g_2(x) \leq 0 \\ &\qquad\qquad \vdots \\ &\qquad\qquad g_m(x) \leq 0 \end{aligned} \tag{COPT}$$

is a (constrained) convex optimization problem.

You will also see Definition 82 written with equality constraints; however, any equality constraint $g(x) = 0$ can be written as $-g_1(x) \leq 0, g_2(x) \leq 0$ where both $g_1 = g_2 = g$. As a result, the equality constraints are technically redundant in the definition. To see that this is really minimizing a convex function over a convex set, we need only note that the set of feasible points is

$$X \cap g_1^{-1}([-\infty, 0]) \cap g_2^{-1}([-\infty, 0]) \cap \cdots \cap g_m^{-1}([-\infty, 0]),$$

which by Propositions 24 and 49 is convex.

A.2 Linear programming

Definition 83. If $f, g_1, g_2, \ldots, g_m$ are affine on $V = \mathbb{R}^n$ and if we take $X = \mathbb{R}^n_+$, then the convex optimization problem in Definition 82 is called a *linear program*. Since any linear function from $\mathbb{R}^n$ to $\mathbb{R}$ can be expressed as an inner product, we commonly let

$$\begin{aligned} f &= x \mapsto \langle c, x \rangle + d \\ g_1 &= x \mapsto \langle -a_1, x \rangle + b_1 \\ g_2 &= x \mapsto \langle -a_2, x \rangle + b_2 \\ &\vdots \\ g_m &= x \mapsto \langle -a_m, x \rangle + b_m \end{aligned}$$

where $c, a_1, a_2, \ldots, a_m \in \mathbb{R}^n$ and $d, b_1, b_2, \ldots, b_m \in \mathbb{R}$ are whatever vectors/numbers make things work (and the negative sign is just for convenience in the definition of A that follows). Now if we let $A \in \mathbb{R}^{n \times n}$ be the matrix whose ith row

is a_i and $b = (b_1, b_2, \ldots, b_m)^T$, then Problem (COPT) can be rewritten in the more familiar form,

$$\begin{aligned} &\text{minimize} && \langle c, x\rangle \\ &\text{subject to} && Ax \geq b \\ & && x \geq 0 \\ & && \Updownarrow \\ &\text{minimize} && \langle c, x\rangle \\ &\text{subject to} && Ax - b \in \mathbb{R}^n_+ \\ & && x \in \mathbb{R}^n_+. \end{aligned} \tag{LP}$$

Here we have dropped the constant d because it does not change the optimal point, if there is one. We also have to specify that $x \in \mathbb{R}^n_+$ now, because otherwise that restriction is not clear from the domain of the function $x \mapsto \langle c, x\rangle$.

This is essentially the same form as Boyd's (4.29), since the sign doesn't matter and even the constraint $x \geq 0 \iff x \in \mathbb{R}^n_+$ can be embedded in the matrix if you're willing to add some extra dimensions to the problem.

We won't go into the details of linear programming here. It's probably the most important optimization problem of the 20th century. Section 4.3 in Boyd describes several important applications. For us, what we want to focus on is that Problem (LP) expresses this important problem in terms of a self-dual proper cone.

SageMath can solve linear programs, of course; but beware, there are a lot of options to play around with. For example, the default linear program in SageMath is a *maximization* problem, and it supports integer variables.

```
sage: # http://people.brunel.ac.uk/~mastjjb/jeb/or/morelp.html
sage: LP = MixedIntegerLinearProgram()
sage: x = LP.new_variable(real=True, nonnegative=True)
sage: LP.add_constraint(50*x[0] + 24*x[1] <= 40*60)
sage: LP.add_constraint(30*x[0] + 33*x[1] <= 35*60)
sage: LP.add_constraint(x[0] >= 45)
sage: LP.add_constraint(x[1] >= 5)
sage: LP.set_objective(x[0] + x[1] - 50)
sage: LP.show()
Maximization:
  x_0 + x_1 - 50.0
Constraints:
  50.0 x_0 + 24.0 x_1 <= 2400.0
  30.0 x_0 + 33.0 x_1 <= 2100.0
  - x_0 <= -45.0
  - x_1 <= -5.0
Variables:
  x_0 is a continuous variable (min=0.0, max=+oo)
  x_1 is a continuous variable (min=0.0, max=+oo)
sage: LP.solve()
1.25
```

Every linear programming problem has a *dual problem*, that tries to compute the same optimal value through different means. If you're familiar with the Lagrange multiplier theorem, you may recall the Lagrangian function associated with Definition 82,

$$\begin{aligned} &\mathcal{L} : (X, \mathbb{R}^m) \to \mathbb{R} \\ &\mathcal{L} \coloneqq (x, \lambda) \mapsto f(x) + \sum_{i=1}^{m} \lambda_i g_i(x). \end{aligned} \tag{A.1}$$

The m variables $\lambda_1, \lambda_2, \ldots, \lambda_m$ are called *dual* variables, and they play an important part in solving Problem (COPT). For our purposes, though, we'll be interested in the *Lagrangian dual function*, which eliminates the variable x from the Function (A.1) by taking an infimum over the domain of x:

$$\begin{aligned} &d : \mathbb{R}^m \to \mathbb{R} \cup \{-\infty\} \\ &d \coloneqq \lambda \mapsto \inf(\{\mathcal{L}((x, \lambda)) \mid x \in X\}). \end{aligned} \tag{A.2}$$

When $\lambda \geq 0$, it's not hard to see that $d(\lambda)$ is less than or equal to the optimal value of Problem (COPT).

Proposition 50. *If d is the Lagrangian dual function associated with the convex optimization problem in Definition 82 and if $\lambda \geq 0$, then $d(\lambda) \leq f(x)$ for all* *Boyd, 5.1.3*

$x \in X$, and in particular $d(\lambda)$ is a lower bound on the optimal objective function value in Problem (COPT).

Proof. By definition we have

$$d(\lambda) = \inf \left(\left\{ f(x) + \underbrace{\sum_{i=1}^{m} \lambda_i g_i(x)}_{\leq 0} \;\middle|\; x \in X \right\} \right),$$

where each term $\lambda_i g_i(x)$ is nonpositive because $\lambda_i \geq 0$ by assumption and $g_i(x)$ from the problem constraints. □

This leads to an interesting question: if we try to maximize d over the set $\{\lambda \in \mathbb{R}^m \mid \lambda \geq 0\}$, will we reach the optimal value of Problem (COPT)? This is a deep question, whose answer is "maybe." But in the case of a linear program, things are pretty nice.

Definition 84. The *dual linear program* (with slack variables) associated to Problem (LP) in Definition 83 is

Boyd, Section 5.2

$$\begin{aligned} \text{maximize} \quad & \langle b, y \rangle \\ \text{subject to} \quad & A^T y + s = c \\ & y \geq 0 \\ & s \geq 0. \end{aligned} \tag{dLPs}$$

In this problem we are maximizing over $(y, s)^T \in \mathbb{R}^{2n}$. The dual problem is obtained in a straightforward manner by trying to maximize the Lagrangian dual Function (A.2) of the original linear programming problem. If we eliminate the slack variables, we obtain another, equivalent, form of the same problem.

$$\begin{aligned} \text{maximize} \quad & \langle b, y \rangle \\ \text{subject to} \quad & A^T y \leq c \\ & y \geq 0 \end{aligned} \tag{dLP}$$

This latter form exhibits a nice symmetry with Problem (LP).

Exercise 7. *Derive Problem (dLP) yourself by expressing Problem (LP) in the same form as Boyd's (5.21). The dual problem to (5.21) is then given in (5.22), which you can show is equivalent to Problem (dLP).*

I promised you that things were nice for linear programs, and they are:

Theorem 41 (strong duality for linear programming)**.** *If either the primal Problem (LP) or the dual Problem (dLP) are feasible, then their optimal values are equal.*

Boyd gives this theorem as an example in section 5.2.4, but that's a bit disingenuous: it's not at all easy to prove. Nevertheless, the strong duality theorem tells us why we care about the dual linear program: we can use it to solve the original (primal) problem! Here's an example in SageMath, computing the optimal value of the dual to the example that we did earlier. We see that its optimal value is essentially the same—the tiny difference is due to floating-point roundoff errors.

```
sage: LP_dual = MixedIntegerLinearProgram(maximization=False)
sage: y = LP_dual.new_variable(real=True, nonnegative=True)
sage: LP_dual.add_constraint(50*y[0] + 30*y[1] - y[2] >= 1)
sage: LP_dual.add_constraint(24*y[0] + 33*y[1] - y[3] >= 1)
sage: LP_dual.set_objective( 40*60*y[0] + 35*60*y[1]
....:                      - 45*y[2] - 5*y[3] - 50 )
sage: LP_dual.solve()
1.250000000000007
```

A.3 Cone programming

While linear programming held center stage throughout most of the 20th century, symmetric cone programming took over in the 1990s. A "cone program" (or "conic program") is like the linear program in Problem (LP), but with the constraints $Ax - b \in \mathbb{R}^n_+$ and $x \in \mathbb{R}^n_+$ replaced by $Ax - b \in K$ and $x \in K$ respectively, for some proper cone K. For the moment, we won't worry about whether or not this even makes sense.

Definition 85. If K is a proper cone in a finite-dimensional real inner-product space V and if $b, c \in V$ and $A \in \mathcal{B}(V)$, then Boyd, 4.6.1

$$\begin{array}{ll} \text{minimize} & \langle c, x \rangle \\ \text{subject to} & A(x) \succcurlyeq_K b \\ & x \succcurlyeq_K 0 \end{array} \tag{CP}$$

is the standard form of a (primal) cone programming problem.

The similarity between Problem (LP) and Problem (A.3) should be obvious: aside from leaving A written as an operator (as opposed to a matrix), all we've done is replace $\mathbb{R}^n_+$ with K. The objective function is still linear (so it is convex), and its domain can be restricted to the feasible set K which is also convex. Thus we almost have a convex optimization problem a la Definition 82, if we can figure out what to do with the constraints $A(x) \succcurlyeq_K b$.

Let's be sneaky. This strategy is discussed in section 4.1.3 of Boyd. Define $J := \{x \in V \mid A(x) \succcurlyeq_K b\}$. I claim that this set is convex. Suppose that

$x_1, x_2 \in J$ and that $\alpha \in [0,1]$, and note that $b = \alpha b + (1-\alpha) b$. Then,

$$\begin{aligned} & A(\alpha x_1 + (1-\alpha) x_2) - b \\ = \; & \alpha A(x_1) + (1-\alpha) A(x_2) - b \\ = \; & \alpha A(x_1) - \alpha b + (1-\alpha) A(x_2) - (1-\alpha) b \\ = \; & \alpha (A(x_1) - b) + (1-\alpha)(A(x_2) - b), \end{aligned}$$

which is a convex combination of the elements $A(x_1) - b \in K$ and $A(x_2) - b \in K$. Since K is convex, the combination of the two is back in K. Thus, J is convex. Now without loss of generality, we can reword the problem. Let L represent the function $x \mapsto \langle c, x \rangle$ but with its domain restricted to $K \cap J$, which is a convex set by Proposition 24. Then Problem (A.3) is not the same as, but is completely equivalent to

$$\text{minimize } L(x),$$

which satisfies Definition 82 since there are no constraints and the domain of L is a convex set. Thus we conclude that—at least in spirit—the primal cone program is a convex optimization problem.

Finding the dual cone program is a tiny bit more involved than it was in the linear case; but basically, the reason we work with convex cones and why cone programming is a thing is because this process all comes together rather nicely.

Definition 86. The *dual cone program* (with slack variables) associated to Problem (A.3) in Definition 85 is

Boyd, Example 5.12

$$\begin{array}{ll} \text{maximize} & \langle b, y \rangle \\ \text{subject to} & A^*(y) + s = c \\ & y \succcurlyeq_{K^*} 0 \\ & s \succcurlyeq_{K^*} 0. \end{array} \tag{dCPs}$$

And in exactly the same way we did in the linear case, the slack variables can be eliminated to obtain an equivalent problem that exhibits a nice symmetry with Problem (A.3).

$$\begin{array}{ll} \text{maximize} & \langle b, y \rangle \\ \text{subject to} & A^*(y) \preccurlyeq_{K^*} c \\ & y \succcurlyeq_{K^*} 0. \end{array} \tag{dCP}$$

The only thing that really needs an explanation here is the switch from K to its dual, K^*. The first thing we need to do is figure out what we mean by the "Lagrangian" Function (A.1) when generalized cone inequalities are involved. Since we no longer have a system of m real-number inequalities, we have to do something else. Notice that if we define $\mathbf{g}(x) = (g_1(x), g_2(x), \ldots, g_m(x))^T$, then the constraints in Problem (COPT) can be written as simply $\mathbf{g}(x) \leq 0$, and we then have

$$\sum_{i=1}^{m} \lambda_i g_i(x) = \langle \mathbf{g}(x), \lambda \rangle$$

in the Function (A.1). This situation can now be generalized to the case of conic inequalities like $\mathbf{g}(x) \succcurlyeq_K 0$, at least when $\mathbf{g}$ is linear. In that case, we are essentially dealing with Problem (A.3); so, we define the Lagrangian function associated to problem to be

$$\begin{aligned} &\mathcal{L} : (X, V) \to \mathbb{R} \\ &\mathcal{L} \coloneqq (x, \lambda) \mapsto \langle c, x \rangle - \langle A(x) - b, \lambda \rangle , \end{aligned} \tag{A.3}$$

where $A(x) - b$ now plays the role of $\mathbf{g}(x)$ in our analogy. Ultimately, the analogy is not all that important—we can prove things about the function in Function (A.3), and that's all that matters.

Proposition 51. *If d is the Lagrangian dual function associated with Problem (A.3) and Function (A.3) and if $\lambda \in K^*$, then $d(\lambda) \leq \langle c, x \rangle$ for all $x \in X$, and in particular $d(\lambda)$ is a lower bound on the optimal objective function value in Problem (A.3).*

Proof. By definition we have

$$d(\lambda) = \inf \left(\left\{ \langle c, x \rangle - \underbrace{\langle A(x) - b, \lambda \rangle}_{\geq 0} \;\middle|\; x \in K \right\} \right),$$

where $\langle A(x) - b, \lambda \rangle$ is nonnegative from $A(x) - b \in K$, and the definition of the dual cone. □

(That's why we defined the dual cone the way that we did.)

So, weak duality holds for cone programs, as do a lot of other results. There is also a strong duality, but it requires us to impose some additional conditions on the constraint functions called "constraint qualifications." These are discussed briefly in Section 5.9 of Boyd. One common constraint qualification is *Slater's condition*, which insists that there be some point in the relative interior of the feasible set. There's a list of them on the Wikipedia page for the Karush-Kuhn-Tucker conditions.

The theory of cone programming (being a generalization of linear programming) is very similar to that of linear programming. We won't go into depth, but we will mention one other important result that extends to the conic setting.

Boyd, 5.5.2 and 5.9.2

Theorem 42 (complementary slackness)**.** *Let x^* and y^* be optimal solutions for the primal and dual cone programming problems Problem (A.3) and Problem (dCP), respectively. If $\langle c, x^* \rangle = \langle b, y^* \rangle$ (that is, if strong duality holds), then $\langle x^*, y^* \rangle = 0$.*

While most of the linear programming theory still works in the conic setting, the proofs are much harder and the theorems are more intricate. The tradeoff is that much harder optimization problems can be solved.

Example 72. If $K = \mathcal{L}^n_+$, the cone from Example 35, then Problem (A.3) is called a *second-order cone program*, or *SOCP*. Baes, Example 1.4.1; Boyd, 4.4.2

Second-order cone programs can be used to solve linear programs where the objective function is quadratic (these are called quadratic programs). They can also be used to solve problems where the objective function is still affine, but the constraints are elliptical instead of linear. A few examples:

- Constrained least-squares approximation.
- Minimum distance between two polyhedra.
- Robust linear programming, where there's a ball (or ellipse) of uncertainty around the cost vector and/or constraint vectors.

Example 73. If $K = \mathcal{S}^n_+$, the cone from Example 36, then Problem (A.3) is called a *semidefinite program*, or *SDP*. Technically, all second-order cone programs (SOCPs) can be expressed as semidefinite programs (SDPs). However, from a practical perspective, it's usually better to exploit the structure of an SOCP than it is to think of it as an SDP. Baes, Example 1.4.2; Boyd, 4.6.2

Semidefinite programs are surprisingly powerful. In many cases, NP-hard problems have "SDP relaxations," which are semidefinite programs that give you an approximate answer to a problem that would otherwise be combinatorially hard. For example,

- Linear programs with a binary variable (in $\mathbb{F}_2 \times \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$), as in section 7.3 of Alizadeh's lecture notes.
- The "max cut" problem for a graph (section 1.2 in Alizadeh's lecture notes).
- The traveling salesman problem (TSP); see e.g. *On semidefinite programming relaxations of the traveling salesman problem* by Etienne de Klerk, Dmitrii V. Pasechnik, and Renata Sotirov (free on arXiv).

Second-order and semidefinite programming are popular because they model interesting problems, of course. But we have yet to mention an important detail: we can actually solve them in practice! Most cone programs cannot be solved yet. Linear, second-order, and semidefinite programs are the ones that we've had the most success with, and this is due to *interior point methods*.

At a high level, an interior point method solves a convex optimization problem by solving a series of sub-problems that move you through the interior of the feasible set, towards the optimal solution. Often this is accomplished with a *barrier function* that has nice analytic properties. For example, if we're trying to minimize f over some set $K \subseteq V$, then we might try to minimize $f + b$ over all of V, where b is a function that "blows up," or goes to infinity, on outside of K. This lets us turn our constrained optimization problem into an unconstrained one with a different objective function.

Naturally, the barrier function plays an important part in these methods, and is why symmetric cones and Euclidean Jordan algebras are so useful.

Definition 87. If K is a proper cone in a finite-dimensional real inner-product space V, then a *barrier function* for K is a function $\beta : \operatorname{int}(K) \to \mathbb{R}$ that is convex, nonnegative, differentiable at least twice, and which tends to infinity as its argument approaches $\operatorname{bdy}(K)$.

Definition 88 (log-homogeneous barrier function [6])**.** A barrier function b for a proper cone K in a finite-dimensional real inner-product space V is said to be *logarithmically-homogenous* (or *log-homogeneous*, for short) with parameter ν if

$$\exists \nu > 0 : \forall x \in V : b(\alpha x) = b(x) - \nu \ln(\alpha).$$

If you start at a point x inside of the cone K and if you start to move "up" into the cone by a scaling factor of $\alpha \geq 0$, then, intuitively, the point αx is further away from the boundary of the cone than x was. The definition of log-homogeneity is meant to impose this intuition on the barrier function, which otherwise could remain constant or even increase as you move "into" the cone. Likewise, in the other direction (towards zero), the choice of the log function means that for $\alpha < 1$, the value of the barrier function goes to infinity.

Without going into the details of interior point methods, let's just see what happens if we modify our primal cone program by adding some positive multiple $\mu > 0$ of a log-homogeneous barrier function β to the objective value. To simplify our use of the gradient, let's assume that the ambient inner-product space is $\mathbb{R}^n$ (this is true anyways up to isometry).

$$\begin{array}{ll} \text{minimize} & \langle c, x \rangle + \mu\beta(x) \\ \text{subject to} & A(x) \succcurlyeq_K b. \end{array} \tag{A.4}$$

(The domain of the barrier function now forces $x \in \operatorname{int}(K)$.) If we compute the Lagrangian function for this problem as in Function (A.3), we obtain

$$\mathcal{L} \coloneqq (x, \lambda) \mapsto \langle c, x \rangle + \mu\beta(x) - \langle A(x) - b, \lambda \rangle,$$

and (if we have strong duality) the necessary condition for optimality here follows from the KKT conditions. We use isomorphism to pretend that the inner-product space V

$$\nabla\mathcal{L}(x, \lambda) = \begin{bmatrix} c + \mu\nabla\beta(x) - A^*(\lambda) \\ b - A(x) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \tag{A.5}$$

A solution (x, λ) to this system is called μ-optimal.

Proposition 52. *If (x, y) is a solution to Equation (A.5) and if we define $s_\mu \coloneqq -\mu\nabla\beta(x)$, then $s_\mu \in -\operatorname{int}(K^*)$. As a result, the pair (y, s_μ) is feasible for a barrier formulation of Problem (dCPs) defined on $\operatorname{int}(K^*)$.*

Proof. Recall that we artificially restricted the domain of y to be K^* so that $d(y)$ would be a lower bound on the primal objective function; otherwise it doesn't make much sense to try to maximize $d(y)$. (This is the setting in which

weak/strong duality hold, and we assumed strong duality.) Moreover we have $A^*(y) + s_\mu = c$ by the definition of s_μ and the first equation in Equation (A.5). It remains only to show that $s_\mu \in \operatorname{int}(K^*)$.

Recall Rockafellar's definition of the Legendre conjugate [12] prior to Theorem 26.4. If we set $f = \beta$ and $C = \operatorname{int}(\operatorname{int}(K)) = \operatorname{int}(K)$, then the Legendre conjugate of (C, f) is the pair (D, g) where $g = \beta^*$ and $D = \nabla\beta(\operatorname{int}(K))$. Theorem 26.4 then tells us that

$$-s_\mu \in D = \nabla\beta(\operatorname{int}(K)) \subseteq \operatorname{dom}(\beta^*),$$

where $\operatorname{dom}(\beta^*)$ is the "effective domain" of the convex conjugate of β,

$$\begin{aligned}\beta^* &\coloneqq y \mapsto \sup(\{\langle y, x\rangle - \beta(x) \mid x \in \mathbb{R}^n\}) \\ &= y \mapsto \sup(\{\langle y, x\rangle - \beta(x) \mid x \in \operatorname{int}(K)\})\end{aligned}$$

The effective domain of a function is the set of points where, if we interpret it as an extended-real function, its value is not equal to $+\infty$. Thus this problem comes down to showing that the effective domain of β^* is contained in $-\operatorname{int}(K^*)$. Suppose that $y \in \operatorname{dom}(\beta^*)$ so that

$$\sup(\{\langle y, x\rangle - \beta(x) \mid x \in \operatorname{int}(K)\}) \neq \infty.$$

Scaling by positive real numbers doesn't change the interior of the cone, so

$$\begin{aligned}&\sup(\{\langle y, \alpha x\rangle - \beta(\alpha x) \mid x \in \operatorname{int}(K), \alpha > 0\}) \\ =&\sup(\{\alpha\langle y, x\rangle - \beta(x) + \nu\ln(\alpha) \mid x \in \operatorname{int}(K), \alpha > 0\}) \\ \neq&\infty.\end{aligned}$$

as well. Now we notice that if $\langle y, x_0\rangle \geq 0$ for any $x_0 \in \operatorname{int}(K)$, then we get a contradiction: this supremum would be ∞, since we could let $\alpha \to \infty$. Therefore it must be the case that, for all $x \in \operatorname{int}(K)$, we have $\langle y, x\rangle < 0$. In other words,

$$y \in -\operatorname{int}\left((\operatorname{int}(K))^*\right) = -\operatorname{int}(K^*). \qquad \square$$

Remark 6. Alizadeh [3] states that the preceding proposition is "easy to deduce" without log-homogeneity. I have imposed the additional log-homogeneity condition because I see no way to prove the result without it.

Our barrier functions should have not only nice theoretical properties, but also practical ones. Can we solve Problem (A.4) numerically in a reasonable amount of time? To address that issue, Nesterov and Nemirovskii [10] introduced what is called a self-concordant barrier function. These are barrier functions defined in just such a way that makes Problem (A.4) succeptible to Newton's method. The authors also show that a "universal" self-concordant barrier function exists for any open convex set, and for a proper cone K it is log-homogeneous. The problem is, we don't *really* know the universal barrier function (it's an integral we don't know how to compute).

Güler showed that the universal barrier function of Nesterov and Nemirovskii is related to the characteristic function of the cone [6]. He then used the theory of homogenous cones in a Jordan algebra to show that the universal barrier function can actually be calculated for homogeneous cones, and points out that the self-dual homogeneous cones (called *symmetric cones*) correspond exactly to the cones of squares in Euclidean Jordan algebras.

Around the same time, Nesterov and Todd [11] showed that particularly efficient algorithms exist for *self-scaled cones*, which turn out to be nothing other than self-dual homogeneous cones. Thus, the most efficient interior-point barrier methods apply to symmetric cones, which are cones of squares in Euclidean Jordan algebras.

Appendix B

Rational function functions

In what follows, our goal will be to show that a few types of rational functions (that don't induce division by zero) can be made into actual functions. We'll show that in each case, the map from the algebraic object to the function is additive, multiplicative, and injective in a limited sense. We avoid the word "homomorphism" because we don't know that these things form a ring. To keep the notation simple, we let $R \coloneqq \mathbb{R}[X_1, X_2, \ldots, X_n]$ throughout this appendix. The map $f \mapsto f\restriction_{\mathbb{R}^n}$ on R is an injective ring homomorphism and serves as a sort of "base case" for what's coming.

If $f = a/b \in \operatorname{Frac}(R)$ and $D \subseteq \mathbb{R}^n$ is the subset where $b\restriction_{\mathbb{R}^n}$ is non-zero, then D is dense by Theorem 29 and

$$f\restriction_D : D \to \mathbb{R}$$
$$f\restriction_D = x \mapsto \frac{a\restriction_{\mathbb{R}^n}(x)}{b\restriction_{\mathbb{R}^n}(x)}$$

defines a valid function on D. However, there is a problem with this definition. Keeping in mind that our goal is to study the correspondence $f \mapsto f\restriction_D$, recall that the elements of $\operatorname{Frac}(R)$ are equivalence classes. If $f \mapsto f\restriction_D$ is going to itself define a valid function, then we should have $f\restriction_D = g\restriction_D$ whenever $f = g$. This doesn't work using the definition above! For example, if $c \in R$ is any other polynomial with $c\restriction_{\mathbb{R}^n}(x) = 0$ for some $x \in D$, then $\frac{a}{b} = \frac{ac}{bc}$ in $\operatorname{Frac}(R)$, but the latter fraction will cause division by zero when applied to x if we try to turn it into a function.

Fixing this problem takes some work.

Theorem 43. *If $a/b \in \operatorname{Frac}(R)$, then there exists a unique representative $(c, d) \in a/b$ with d monic, $\gcd(c, d) = 1$, and $a = ce$ and $b = de$ for a common nonzero divisor $e \in R$. The representative (c, d) is the* unique reduced lowest-terms representative *of a/b, henceforth abbreviated "lowest-terms."*

Proof. First we note that the notion of a greatest common divisor (GCD) exists in $\mathbb{R}[X]$. This is usually demonstrated before Euclid's division algorithm in

kindergarten. Citing Theorem 4 and Theorem 1 of Anderson and Hasse [2], it follows that R itself is a GCD domain, a *unique lowest-terms domain*, and a *reduced lowest-terms domain*. The "unique" here is only "essentially unique," which means up to multiplication by a unit. The units of R are non-zero real numbers, so we can make the "lowest-terms" truly unique by insisting that the lowest-terms representative (c, d) have d monic. The fact that R is a *reduced* lowest-terms domain means that we can actually find the e to factor out. □

Suppose c/d is a/b written in lowest-terms. Then $b = ed$ for some $e \in R$, and it follows that $b\restriction_{\mathbb{R}^n}$ has at least as many roots as $d\restriction_{\mathbb{R}^n}$ because it's got the roots from $d\restriction_{\mathbb{R}^n}$ and also the roots from $e\restriction_{\mathbb{R}^n}$. This leads to the following obvervation: if we can make a function out of the representative a/b, then we can also make a function out of its unique lowest-terms representative.

Proposition 53. *Suppose $f = a/b \in \operatorname{Frac}(R)$ and that D is an open dense set on which $b\restriction_{\mathbb{R}^n}$ is nonzero and that (a', b') is the unique lowest-terms representative of a/b. Then the correspondence $f \mapsto f\restriction_D$ where*

$$f\restriction_D : D \to \mathbb{R}$$
$$f\restriction_D = x \mapsto \frac{a'\restriction_{\mathbb{R}^n}(x)}{b'\restriction_{\mathbb{R}^n}(x)}$$

is a well-defined function on $\operatorname{Frac}(R)$.

Proof. Suppose that $a/b = c/d$ for some other representative (c, d). Then since our lowest-terms are truly unique, the lowest-terms representative of c/d is also (a', b'); it follows that

$$\forall x \in D : \left(\frac{a}{b}\right)\restriction_D (x) = \frac{a'\restriction_D (x)}{b'\restriction_D x} = \left(\frac{c}{d}\right)\restriction_D (x),$$

showing that $(a/b)\restriction_D = (c/d)\restriction_D$. □

The user must beware however that the set D should be determined before applying the preceding proposition. If D is fixed, then the mapping $f \mapsto f\restriction_D$ is well-defined, but D itself cannot be determined uniquely from f because it depends on the denominator. This means that you will need to know at least one representative of the class $f \in \operatorname{Frac}(R)$ before you can turn it into a function.

Another crucial property is that reducing to lowest-terms doesn't invalidate any equations that a representative satisfies on an open dense set.

Proposition 54. *If $a/b \in \operatorname{Frac}(R)$ and if D is an open dense set on which $b\restriction_{\mathbb{R}^n}$ is non-zero, then*

$$\forall x \in D : \frac{a\restriction_{\mathbb{R}^n}(x)}{b\restriction_{\mathbb{R}^n}(x)} = \left(\frac{a}{b}\right)\restriction_D (x).$$

Proof. Suppose that (a', b') is the lowest-terms representative for a/b. Then there exists some $e \in R$ such that $a = ea'$ and $b = eb'$. Thus,

$$\forall x \in D : \frac{a\restriction_D(x)}{b\restriction_D(x)} = \frac{(ea')\restriction_D(x)}{(eb')\restriction_D(x)} = \frac{e\restriction_D(x)\, a'\restriction_D(x)}{e\restriction_D(x)\, b'\restriction_D(x)} = \left(\frac{a}{b}\right)\restriction_D(x).$$

We can cancel $e\restriction_D(x)$ above because it is nonzero, and it must be nonzero because the entire denominator is nonzero. □

This is important because—among other things—it means that when we solve equations that are valid on an open dense set through polynomial division, reducing to lowest terms "on the fly" won't invalidate the fact that the corresponding functions solve the original problem (on the same open dense set). In particular, this is crucial to our ability to claim that a Cramer's-rule solution must be valid if we stick an x into the result on both sides.

We also want to show that this map has an "injective-like" property, but we can't say that it's injective on all of $\mathrm{Frac}(R)$, because the safe domain D that we specified depends on the element of $\mathrm{Frac}(R)$ that we're working with. So instead we'll have to say something weaker. Leave $f = a/b$ alone, but now let D_1 be an open dense set where $b\restriction_{\mathbb{R}^n}$ is nonzero. Define $g \coloneqq c/d$, and let D_2 be an open dense set where $d\restriction_{\mathbb{R}^n}$ is nonzero. Then $D \coloneqq D_1 \cap D_2$ is also open and dense, and both $b\restriction_{\mathbb{R}^n}$ and $d\restriction_{\mathbb{R}^n}$ are non-zero on all of D. We will suppose again that (a', b') is the lowest-terms representative of a/b, and now that (c', d') is the lowest-terms representative of c/d.

Remark 7. We insist that D_1 and D_2 be open and dense so that their intersection will again be dense. The intersection of two dense sets is not dense in general: the rationals and irrationals are both dense in $\mathbb{R}$. Even a countable intersection of open dense sets will again be dense; although it will perhaps not be open.

In this scenario, we claim that $f \neq g \implies f\restriction_D \neq g\restriction_D$. If $a/b \neq c/d$, then of course $a'/b' \neq c'/d'$, since otherwise $a/b = a'/b'$ and $c/d = c'/d'$ would be a contradiction. Thus by definition $a'd' \neq c'd'$ and we must have

$$\exists x \in D : a'\restriction_D(x)\, d'\restriction_D(x) \neq b'\restriction_D(x)\, c'\restriction_D(x).$$

Otherwise, from the density of D and the continuity of all functions involved, we would conclude that $a'd' = b'c'$. From the above it follows that

$$\frac{a'\restriction_D(x)}{b'\restriction_D(x)} \neq \frac{c'\restriction_D(x)}{d'\restriction_D(x)}$$

for that same $x \in D$, meaning that the two functions $f\restriction_D$ and $g\restriction_D$ are different.

We have to show that $f \mapsto f\restriction_D$ is additive and multiplicative in the same limited sense. For additivity, note the following two equalities,

$$\forall x \in D : \left(\frac{a}{b}\right)\restriction_D(x) + \left(\frac{c}{d}\right)\restriction_D(x) \coloneqq \left(\frac{a'}{b'}\right)\restriction_D(x) + \left(\frac{c'}{d'}\right)\restriction_D(x), \tag{B.1}$$

and

$$\forall x \in D : \left(\frac{a}{b} + \frac{c}{d}\right)\restriction_D (x) = \left(\frac{a'}{b'} + \frac{c'}{d'}\right)\restriction_D (x) = \left(\frac{a'd' + b'c'}{b'd'}\right)\restriction_D (x)\,.$$

The first equality above comes from the well-definedness of the map and the fact that both $a/b = a'/b'$ and $c/d = c'/d'$. Beware that in the last expression, $\frac{a'd'+b'c'}{b'd'}$ may not be in lowest terms! So we can't just apply the numerator and denominator to x blindly. But we *can* refer to Proposition 54 to conclude that

$$\forall x \in D : \left(\frac{a'd' + b'c'}{b'd'}\right)\restriction_D (x) = \frac{a'd' + b'c'\restriction_D (x)}{b'd'\restriction_D (x)}$$

Now $p \mapsto p\restriction_D$ is a homomorphism on R, so this expands into the same expression that we derived in Equation (B.1). Thus we conclude (again, under some awkward conditions) that $(f+g)\restriction_D = f\restriction_D + g\restriction_D$.

The proof of multiplicativity is identical. Step one is to note that

$$\forall x \in D : \left(\frac{a}{b}\right)\restriction_D (x) \left(\frac{c}{d}\right)\restriction_D (x) = \frac{a'\restriction_D (x)\, b'\restriction_D (x)}{c'\restriction_D (x)\, d'\restriction_D (x)}.$$

Step two uses Proposition 54 and the multiplicativity of $p \mapsto p\restriction_D$ for $p \in R$ to deduce that

$$\forall x \in D : \left(\frac{a}{b}\frac{c}{d}\right)\restriction_D (x) = \left(\frac{a'}{b'}\frac{c'}{d'}\right)\restriction_D (x) = \frac{a'\restriction_D (x)\, b'\restriction_D (x)}{c'\restriction_D (x)\, d'\restriction_D (x)}.$$

Combining the steps shows that $(fg)\restriction_D = f\restriction_D g\restriction_D$.

Having achieved our goal in $\mathrm{Frac}\,(R)$, we now look onwards to $\mathrm{Frac}\,(R)\,[\Lambda]$. Fortunately, most of the hard work is behind is—things in $\mathrm{Frac}\,(R)\,[\Lambda]$ will reduce easily to $\mathrm{Frac}\,(R)$ where we've already proved everything. Suppose from now on that $f, g \in \mathrm{Frac}\,(R)\,[\Lambda]$ with

$$f \coloneqq \sum_{i=0}^{I} \left(\frac{a_i}{b_i}\right) \Lambda^i, \qquad g \coloneqq \sum_{j=0}^{J} \left(\frac{c_j}{d_j}\right) \Lambda^j.$$

Here each coefficient a_i/b_i or c_j/d_j lives in $\mathrm{Frac}\,(R)$, where we already know that the map $a_i/b_i \mapsto (a_i/b_i)\restriction_D$ is well-defined, injective, additive, and multiplicative in the precise limited sense discussed earlier.

Now, suppose that D is an open dense set on which all $b_i\restriction_{\mathbb{R}^n}$ are non-zero. Then, abusing the same notation,

$$f\restriction_D \coloneqq x \mapsto \sum_{i=0}^{I} \left(\frac{a_i}{b_i}\right)\restriction_D (x)\, \Lambda^i$$

defines a valid function from D to $\mathbb{R}\,[\Lambda]$, and the mapping $f \mapsto f\restriction_D$ is well-defined. (Again, the set D must be fixed *before* we do anything else, so you have to know at least one representative for each coefficient of f.) To see

that this mapping is well-defined, suppose $f = g$, and simply note that by definition that means that $I = J$ and that $a_i/b_i = c_i/d_i$ for each $i \in \{0, 1, \ldots, I\}$. The result then follows immediately from the well-definedness of the mapping $a_i/b_i \mapsto (a_i/b_i)\restriction_D$.

In general, we will let D_f be an open dense set on which all $b_i\restriction_{\mathbb{R}^n}$ are non-zero, and D_g be an open sense set on which all $d_i\restriction_{\mathbb{R}^n}$ are non-zero. Then $D \coloneqq D_f \cap D_g$ is open and dense, and both $f\restriction_D$ and $g\restriction_D$ are defined. In this setting, suppose that $f \neq g$. By definition, that means that for some i we have $a_i/b_i \neq c_i/d_i$. From the pseudo-injectivity of $a_i/b_i \mapsto (a_i/b_i)\restriction_D$ in $\operatorname{Frac}(R)$, we deduce that the ith coefficients of f and g differ on some $x \in D$. Thus, $f\restriction_D \neq g\restriction_D$, and we have the same sort of pseudo-injectivity in $\operatorname{Frac}(R)[\Lambda]$.

Additional is similarly easy. By definition,

$$f + g = \sum_{i=0}^{\max(I,J)} \left(\frac{a_i}{b_i} + \frac{c_i}{d_i}\right) \Lambda^i,$$

so in $(f+g)\restriction_D$ one simply needs to expand $(a_i/b_i + c_i/d_i)\restriction_D$ using the additivity that we showed exists in $\operatorname{Frac}(R)$.

Finally, for multiplicativity, we will refer back to the formula for polynomial multiplication in Equation (3.2):

$$\begin{aligned}\forall x \in D : (fg)\restriction_D (x) &= \left(\sum_{\ell=0}^{\max(I,J)} \left[\sum_{i=0}^{\ell} \frac{a_i}{b_i}\frac{c_{\ell-i}}{d_{\ell-i}}\right] \Lambda^\ell\right)\restriction_D (x) \\ &\coloneqq \sum_{\ell=0}^{\max(I,J)} \left[\sum_{i=0}^{\ell} \frac{a_i}{b_i}\frac{c_{\ell-i}}{d_{\ell-i}}\right]\restriction_D (x)\, \Lambda^\ell\end{aligned}$$

Using the additivity and multiplicativity in $\operatorname{Frac}(R)$, we deduce from this that

$$\forall x \in D : (fg)\restriction_D (x) = \sum_{\ell=0}^{\max(I,J)} \left[\sum_{i=0}^{\ell} \left(\frac{a_i}{b_i}\right)\restriction_D (x) \left(\frac{c_{\ell-i}}{d_{\ell-i}}\right)\restriction_D (x)\right] \Lambda^\ell,$$

and this is precisely $f\restriction_D (x)\, g\restriction_D (x)$.

Bibliography

[1] Alen Alexanderian. *On continuous dependence of roots of polynomials on coefficients*. 2013. URL https://aalexan3.math.ncsu.edu/articles/polyroots.pdf.

[2] Daniel D. Anderson and Erik Hasse. *Reducing fractions to lowest terms*. In Marco Fontana, Sophie Frisch, Sarah Glaz, Francesca Tartarone, and Paolo Zanardo (eds.), *Rings, Polynomials, and Modules*, 1–11. Springer International Publishing, Cham, Switzerland, 2017. ISBN 9783319658728, doi:10.1007/978-3-319-65874-2_1.

[3] Miguel F. Anjos and Jean B. Lasserre. *Handbook on Semidefinite, Conic and Polynomial Optimization*, vol. 166 of *International Series in Operations Research & Management Science*. Springer, New York, 2012. ISBN 9781461407683, doi:10.1007/978-1-4614-0769-0.

[4] John A. Beachy and William D. Blair. *Abstract Algebra*. Waveland Press, Long Grove, Illinois, fourth ed., 2019. ISBN 9781478638698.

[5] Jacques Faraut and Adam Korányi. *Analysis on Symmetric Cones*. Clarendon Press, Oxford, 1994. ISBN 9780198534778.

[6] Osman Güler. *Barrier functions in interior point methods*. Mathematics of Operations Research, 21(4):860–885, 1996, doi:10.1287/moor.21.4.860.

[7] Pascual Jordan, John von Neumann, and Eugene Wigner. *On an algebraic generalization of the quantum mechanical formalism*. Annals of Mathematics, 35:29–64, 1934, doi:10.2307/1968117.

[8] Max Koecher. *The Minnesota Notes on Jordan Algebras and Their Applications*, vol. 1710 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin Heidelberg, 1999. ISBN 9783540663607, doi:10.1007/BFb0096285.

[9] Sauders Mac Lane and Garrett Birkhoff. *Algebra*. AMS Chelsea Publishing, Providence, Rhode Island, third ed., 1999. ISBN 9780821816462.

[10] Yurii E. Nesterov and Arkadii Nemirovskii. *Interior-Point Polynomial Algorithms in Convex Programming*, vol. 13 of *SIAM Studies in Applied and Numerical Mathematics*. Society for Industrial and Applied Mathematics, Philadelphia, 1994. ISBN 0898713196.

[11] Yurii E. Nesterov and Michael J. Todd. *Self-scaled barriers and interior-point methods for convex programming.* Mathematics of Operations Research, 22(1):1–42, 1997, doi:10.1287/moor.22.1.1.

[12] Ralph Tyrrell Rockafellar. *Convex Analysis.* Princeton University Press, Princeton, 1970. ISBN 9780691015866.

[13] Steven Roman. *Advanced Linear Algebra*, vol. 135 of *Graduate Texts in Mathematics.* Springer Science+Business Media, New York, third ed., 2008. ISBN 9780387728285, doi:10.1007/978-0-387-72831-5.

[14] Walter Rudin. *Functional Analysis.* International Series in Pure and Applied Mathematics. McGraw-Hill, Inc., United States, second ed. ISBN 0070542368.

[15] Frank Sottile. *Discrete and Applicable Algebraic Geometry.* Texas A&M University, College Station, Texas, 2009. URL https://www.math.tamu.edu/~sottile/conferences/Summer_IMA07/Sottile.pdf.

Index