Algebra: Monomials and Polynomials

John Perry
University of Southern Mississippi
john.perry@usm.edu
http://www.math.usm.edu/perry/

Table of Contents

Part III. Rings

Part III. Appendices

Reference sheet for notation

$[r]$	the element $r + n\mathbb{Z}$ of $\mathbb{Z}_n$
$\langle g \rangle$	the group (or ideal) generated by g
A_3	the alternating group on three elements
$A \triangleleft G$	for G a group, A is a normal subgroup of G
$A \triangleleft R$	for R a ring, A is an ideal of R
$\mathbb{C}$	the complex numbers $\{a + bi : a, b \in \mathbb{C} \text{ and } i = \sqrt{-1}\}$
$[G, G]$	commutator subgroup of a group G
$[x, y]$	for x and y in a group G, the commutator of x and y
$\mathrm{Conj}_a(H)$	the group of conjugations of H by a
$\mathrm{conj}_g(x)$	the automorphism of conjugation by g
D_3	the symmetries of a triangle
$d \mid n$	d divides n
$\deg f$	the degree of the polynomial f
D_n	the dihedral group of symmetries of a regular polygon with n sides
$D_n(\mathbb{R})$	the set of all diagonal matrices whose values along the diagonal is constant
$d\mathbb{Z}$	the set of integer multiples of d
$f(G)$	for f a homomorphism and G a group (or ring), the image of G
$\mathrm{Frac}(R)$	the set of fractions of a commutative ring R
G/A	the set of left cosets of A
$G\backslash A$	the set of right cosets of A
gA	the left coset of A with g
$G \cong H$	G is isomorphic to H
$\mathrm{GL}_m(\mathbb{R})$	the general linear group of invertible matrices
$\prod_{i=1}^{n} G_i$	the ordered n-tuples of $G_1, G_2, \ldots, G_n$
$G \times H$	the ordered pairs of elements of G and H
g^z	for G a group and $g, z \in G$, the conjugation of g by z, or zgz^{-1}
$H < G$	for G a group, H is a subgroup of G
$\ker f$	the kernel of the homomorphism f
$\mathrm{lcm}(t, u)$	the least common multiple of the monomials t and u
$\mathrm{lm}(p)$	the leading monomial of the polynomial p
$\mathrm{lv}(p)$	the leading variable of a linear polynomial p
$\mathbb{M}$	the set of monomials in one variable
$\mathbb{M}_n$	the set of monomials in n variables
$\mathbb{N}^+$	the positive integers
$N_G(H)$	the normalizer of a subgroup H of G
$\mathbb{N}$	the natural or counting numbers $\{0, 1, 2, 3 \ldots\}$
Ω_n	the nth roots of unity; that is, all roots of the polynomial $x^n - 1$
$\mathrm{ord}(x)$	the order of x

P_∞	the point at infinity on an elliptic curve
Q_8	the group of quaternions
$\mathbb{Q}$	the rational numbers $\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\}$
R/A	for R a ring and A an ideal subring of R, R/A is the quotient ring of R with respect to A
$\langle r_1, r_2, \ldots, r_m \rangle$	the ideal generated by $r_1, r_2, \ldots, r_m$
$\mathbb{R}$	the real numbers, those that measure any length along a line
$\mathbb{R}^{m \times m}$	$m \times m$ matrices with real coefficients
$\mathbb{R}[x]$	polynomials in one variable with real coefficients
$\mathbb{R}[x_1, x_2, \ldots, x_n]$	polynomials in n variables with real coefficients
$R[x_1, x_2, \ldots, x_n]$	the ring of polynomials whose coefficients are in the ground ring R
S_n	the group of all permutations of a list of n elements
$S \times T$	the Cartesian product of the sets S and T
$\text{tts}(p)$	the trailing terms of p
$Z(G)$	centralizer of a group G
$\mathbb{Z}_n^*$	the set of elements of $\mathbb{Z}_n$ that are *not* zero divisors
$\mathbb{Z}/n\mathbb{Z}$	quotient group (resp. ring) of $\mathbb{Z}$ modulo the subgroup (resp. ideal) $n\mathbb{Z}$
$\mathbb{Z}$	the integers $\{\ldots, -1, 0, 1, 2, \ldots\}$
$\mathbb{Z}\left[\sqrt{-5}\right]$	the ring of integers, adjoin $\sqrt{-5}$
$\mathbb{Z}_n$	the quotient group $\mathbb{Z}/n\mathbb{Z}$

0

A few acknowledgements

These notes are inspired from some of my favorite algebra texts: [AF05, CLO97, HA88, KR00, Lau03, LP98, Rot06, Rot98]. The heritage is hopefully not too obvious, but in some places I felt compelled to cite the source.

Thanks to the students who found typos, including (in no particular order) Jonathan Yarber, Kyle Fortenberry, Lisa Palchak, Ashley Sanders, Sedrick Jefferson, Shaina Barber, Blake Watkins, and others. Special thanks go to my graduate student Miao Yu, who endured the first drafts of Chapters 7, 8, and 10.

Rogério Brito of Universidade de São Paolo made several helpful comments, found some nasty errors[1], and suggested some of the exercises.

I have been lucky to have had great algebra professors; in chronological order:

- Vanessa Job at Marymount University;
- Adrian Riskin at Northern Arizona University;
- and at North Carolina State University:
  - Kwangil Koh,
  - Hoon Hong,
  - Erich Kaltofen,
  - Michael Singer, and
  - Agnes Szanto.

Boneheaded innovations of mine that looked good at the time but turned out bad in practice should not be blamed on any of the individuals or sources named above. After all, they evaluated previous work of mine, so the concept that I might say something dumb won't come as a surprise to them, and they tried very hard to cure me of that habit. *This is not a peer-reviewed text*, which is why you have a supplementary text in the bookstore.

The following software helped prepare these notes:

- Sage 3.*x* and later[Ste08];
- Lyx [Lyx] (and therefore LaTeX [Lam86, Grä04] (and therefore TeX [Knu84])), along with the packages
  - `cc-beamer` [Pip07],
  - `hyperref` [RO08],
  - AMS-LaTeX[Soc02],
  - `mathdesign` [Pic06], and
  - `algorithms` (modified slightly from version 2006/06/02) [Bri]; and
- Inkscape [Bah08].

I've likely forgotten some other non-trivial resources that I used. Let me know if another citation belongs here.

My wife forebore a number of late nights at the office (or at home) as I worked on these. *Ad maiorem Dei gloriam.*

[1] In one egregious example, I connected too many dots regarding the origin of the Chinese Remainder Theorem.

0

Preface

This is not a textbook.

Okay, you ask, *what is it, then?*

These are notes I use when teaching class.

But it looks like a textbook.

Fine. So sue me. — no, wait. Let me try to explain. A two-semester sequence on modern algebra ought to introduce students to the fundamental aspects of groups and rings. That's already a bite more than most can chew, and I have difficulty covering even the stuff I think is necessary. Unfortunately, most every algebra text I've encountered expend far too much effort in the first 50–100 pages *with material that is not algebra*. The usual culprit is number theory, but it is by no means the sole offender. Who has that kind of time?

Then there's the whole argument about whether to start with groups, rings, semigroups, or monoids. Desiring a mix of simplicity and utility, I decided to write out some notes that would get me into groups as soon as possible. *Voilà.*

You still haven't explained why it looks like a textbook.

That's because I wanted to organize, edit, rearrange, modify, and extend my notes easily. I also wanted them in digital form, so that (a) I could read them,[2] and (b) I'd be less likely to lose them. I used a software program called Lyx, which builds on LaTeX; see the Acknowledgments.

What if I'd prefer an actual textbook?

See the syllabus.

Overview

These notes have two major parts: in one, we focus on an algebraic structure called a *group*; in the other, we focus on a special kind of group, a *ring*. In the first semester, therefore, we want to cover Chapters 2–5. Since a rigorous approach requires *some* sort of introduction, we review some basics of the integers and the natural numbers – but only to solidify the foundation of what students have already learned; we do not delve into number theory proper.

Some of these ideas fit well with monomials, which I study "on occasion". In algebra, a boring discussion of integers and monomials naturally turns into a fascinating story of the basics of monoids, which actually makes for a gentle introduction to groups. I yielded to temptation and threw that in. That should makes life easier later on, anyway; a *brief* glance at monoids, focusing on commutative monoids without requiring commutativity, allows us to introduce prized ideas that will be developed in much more depth with groups, only in a context with which students are far more familiar. *Repetitio mater studiorum,* and all that.[3] We restrict ourselves to the

[2] You think you have problems reading my handwriting? I have to *live* with it!

[3] University students would do well to remember another Latin proverb, *Vinum memoriæmors.* I won't provide a translation here; look it up, you chumps! Once upon a time, a proper education included familiarity with the wisdom of our ancestors; these days, you can get away with Googling it. Oddly, recent studies suggest that the Latin phrase should be updated: *Google memoriæmors.*

easier notions, since the point is to get to groups, and quickly.

Ideally, we'd also cover Chapter 6, but one of the inexorable laws of life is that the older one gets, the faster time passes. *Tempus fugit,* and all that.[4] The corollary for a professor is that a semester grows shorter with each passing year, which implies that we cover less every year. I have no idea why.

In the second semester, we definitely cover Chapters 6 through 8, along with at least one of Chapter 9 or 10. Chapter 11 is not a part of either course, but I included it for students (graduate or undergraduate) who want to pursue a research project, and need an introduction that builds on what came before. As of this writing, some of those chapters still need major debugging, so don't take anything you read there too seriously.

Not much of the material can be omitted. Within each chapter, many examples are used and reused; this applies to exercises, as well. Textbooks often avoid this, in order to give instructors more flexibility; I don't care about other instructors' points of view, so I don't mind putting into the exercises problems that I return to later in the notes. We try to concentrate on a few important examples, re-examining them in the light of each new topic. One consequence is that rings cannot be taught independently from groups using these notes.

To give you a heads-up, the following material will probably be omitted.

- I really like the idea of placing elliptic curves (Section 2.5) early in the class. Previous editions of these notes had them in the section immediately after the introduction of groups! It gives students an immediate insight into how powerful abstraction can be. Unfortunately, I haven't yet been able to get going fast enough to get them done.
- Groups of automorphisms (Section 4.4) are generally considered optional.
- I have not in the past taught solvable groups (Section 3.6), but hope to do so eventually.
- I have sometimes not made it past alternating groups (Section 5.5). Considering that I used to be able to make it to the RSA algorithm (Section 6.5), that does not mean we won't get there, especially since I've simplified the beginning. That was before I added the stuff on monoids, though...
- The discussion of the 15-puzzle is simplified from other places I've found it, nonstandard, and definitely optional.

[4] Latin is not a prerequisite of this course, but it should be. Google it!

0

Three interesting problems

We'd like to motivate this study of algebra with three problems that we hope you will find interesting. Although we eventually solve them in this text, it might surprise you that in this class, we're interested not in the solutions, but in *why the solutions work*. I could in fact tell you how to to solve them right here, and we'd be done soon enough; on to vacation! But then you wouldn't have learned what makes this course so beautiful *and important.* It would be like walking through a museum with me as your tour guide. I can summarize the purpose of each displayed article, but you can't learn enough in a few moments to appreciate it in the same way as someone with a foundational background in that field. The purpose of this course is to give you at least a foundational background in algebra.

Still, let's take a preliminary stroll through the museum, and consider three exhibits.

A card trick.

Take twelve cards. Ask a friend to choose one, to look at it without showing it to you, then to shuffle them thoroughly. Arrange the cards on a table face up, in rows of three. Ask your friend what column the card is in; call that number α.

Now collect the cards, making sure they remain in the same order as they were when you dealt them. Arrange them on a a table face up again, in rows of four. It is essential that you maintain the same order; the first card you placed on the table in rows of three must be the first card you place on the table in rows of four; likewise the last card must remain last. The only difference is where it lies on the table. Ask your friend again what column the card is in; call that number β.

In your head, compute $x = 4\alpha - 3\beta$. If x does not lie between 1 and 12 inclusive, add or subtract 12 until it is. Starting with the first card, and following the order in which you laid the cards on the table, count to the xth card. This will be the card your friend chose.

Mastering this trick takes only a little practice. *Understanding* it requires quite a lot of background! We get to it in Chapter 6.

Internet commerce.

Let's go shopping!!! This being the modern age of excessive convenience, *let's go shopping online!!!* Before the online compnay sends you your product, however, they'll want payment. This requires you to submit some sensitive information, namely, your credit card number. Once you submit that number, it will bounce happily around a few computers on its way to the company's server. Some of those computers might be in foreign countries. (It's quite possible. Don't ask.) Any one of those machines could have a snooper. How can you communicate the information in *securely?*

The solution is *public-key cryptography*. The bank's computer tells your computer how to send it a message. It supplies a special number used to encrypt the message, called an *encryption*

key. Since the bank broadcasts this in the clear over the internet, anyone in the world can see it. What's more, anyone in the world can look up the method used to decrypt the message.

You might wonder, *How on earth is this secure?!?* Public-key cryptography works because there's the *decryption key* remains with the company, hopefully secret. Secret? Whew! ... or so you think. A snooper could reverse-engineer this key using a "simple" mathematical procedure that you learned in grade school: factoring an integer into primes, like, say, $21 = 3 \cdot 7$.

*How on earth is **this** secure?!?* Although the procedure is "simple", the size of the integers in use now is about 40 digits. Believe it or not, even a 40 digit integer takes even a computer far too long to factor! So your internet commerce is completely safe. For now.

Factorization.

How can we factor polynomials like $p(x) = x^6 + 7x^5 + 19x^4 + 27x^3 + 26x^2 + 20x + 8$? There are a number of ways to do it, but the most efficient ways involve *modular arithmetic*. We discuss the theory of modular arithmetic later in the course, but for now the general principle will do: pretend that the only numbers we can use are those on a clock that runs from 1 to 51. As with the twelve-hour clock, when we hit the integer 52, we reset to 1; when we hit the integer 53, we reset to 2; and in general for any number that does not lie between 1 and 51, we divide by 51 and take the remainder. For example,

$$20 \cdot 3 + 8 = 68 \rightsquigarrow 17.$$

How does this help us factor? When looking for factors of the polynomial p, we can simplify multiplication by working in this modular arithmetic. This makes it easy for us to reject many possible factorizations before we start. In addition, the set $\{1, 2, \ldots, 51\}$ has many interesting properties under modular arithmetic that we can exploit further.

Conclusion.

Abstract algebra is a theoretical course: we wonder more about *why things are true* than about *how we can do things*. Algebraists can at times be concerned more with elegance and beauty than applicability and efficiency. You may be tempted on many occasions to ask yourself the point of all this abstraction and theory. *Who needs this stuff?*

Keep the examples above in mind; they show that algebra is not only useful, but necessary. Its applications have been profound and broad. Eventually you will see how algebra addresses the problems above; for now, you can only start to imagine.

The class "begins" here. Wipe your mind clean: unless it says otherwise here or in the following pages, everything you've learned until now is suspect, and cannot be used to explain anything. You should adopt the Cartesian philosophy of doubt.[5]

[5]Named after the mathematician and philosopher René Descartes, who inaugurated modern philosophy and claimed to have spent a moment wondering whether he even existed. *Cogito, ergo sum* and all that.

Part I
Monoids

Chapter 1:
From integers to monoids

Until now, your study of mathematics focused on several sets:

- numbers, of which you have seen
  - the **natural numbers** $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, with which we can easily associate
    - the **positive integers** $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$;
    - the **integers** $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$;[6] and
    - the **rational numbers** $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\right\}$;[7]
  - the **real numbers** $\mathbb{R}$;
  - the **complex numbers** $\mathbb{C} = \left\{a + bi : a, b \in \mathbb{R} \text{ and } i = \sqrt{-1}\right\}$, which add a second, "imaginary", dimension to the reals;
- polynomials, of which you have seen
  - monomials in one variable $\mathbb{M} = \{x^a : a \in \mathbb{N}\} = \{1, x, x^2, x^3, \ldots\}$;
  - monomials in n variables $\mathbb{M}_n = \left\{x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} : a_1, \ldots, a_n \in \mathbb{N}\right\}$;
  - polynomials in one variable $\mathbb{R}[x]$;
  - polynomials in more than one variable $\mathbb{R}[x, y]$, $\mathbb{R}[x, y, z]$, $\mathbb{R}[x_1, x_2, \ldots, x_n]$;
- square matrices $\mathbb{R}^{m \times m}$.

Each set is useful for certain problems. Natural numbers are useful for problems related to discrete objects we count: apples, people, planks of flooring.[8] Real numbers are useful for problems related to continuous objects that we measure: the amount of water in a cup, the energy in a particle, the length of the hypotenuse of a right triangle. Monomials and polynomials allow us to create expressions which describe more than one value simultaneously.

Each set is important, and will be used at some point in this course. In this chapter, we focus on two fundamental structures of algebra: the integers and the monomials. They share a number of important parallels that lay a foundation for later study. Before we investigate them in detail, let's turn to some general tools of mathematics that you should have seen before now.[9]

Definition 1.1: Let S and T be two sets. The **Cartesian product of S and T** is the set

$$S \times T = \{(s, t) : s \in S, t \in T\}.$$

Example 1.2: You already know $\mathbb{R} \times \mathbb{R}$ as the set of all ordered pairs whose entries are real numbers; geometrically, it forms the x-y plane.

[6] The integers are denoted by $\mathbb{Z}$ from the German word *Zählen*.
[7] The Pythagoreans believed that the rational numbers were the only possible numbers.
[8] Yes, I was working on my house when I wrote that. How did you guess?
[9] In particular, you should have seen these in MAT 340, Discrete Mathematics.

Definition 1.3: A **relation on the sets** S **and** T is any subset of $S \times T$. An **equivalence relation** on S is a subset R of $S \times S$ that satisfies the properties

reflexive:	for all $a \in S$, $(a,a) \in R$;
symmetric:	for all $a, b \in S$, if $(a,b) \in R$ then $(b,a) \in R$; and
transitive:	for all $a, b, c \in S$, if $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$.

Notation 1.4: We usually write aRb instead of $(a,b) \in R$. For example, in a moment we will discuss the relation $\subseteq$, and we always write $a \subseteq b$ instead of "$(a,b) \in \subseteq$".

Example 1.5: Let $S = \{1, \text{cat}, a\}$ and $T = \{-2, \text{mouse}\}$. Then

$$S \times T = \{(1,-2), (1,\text{mouse}), (\text{cat},-2), (\text{cat},\text{mouse}), (a,-2), (a,\text{mouse})\}$$

and the subset

$$\{(1,\text{mouse}), (1,-2), (a,-2)\}$$

is a relation on S and T.

One of the most fundamental relations is among sets.

Definition 1.6: Let A and B be sets. We say that A is a **subset** of B, and write $A \subseteq B$, if every element of A is also an element of B. If A is a subset of B but not equal to B, we say that A is a **proper subset** of B, and write $A \subsetneq B$.[a]

[a] The notation for subsets has suffered from variety. Some authors use $\subset$ to indicate a subset; others use the same to indicate a proper subset. To avoid confusion, we eschew this symbol altogether.

Notation 1.7: Notice that both $\mathbb{N} \subseteq \mathbb{Z}$ and $\mathbb{N} \subsetneq \mathbb{Z}$ are true.

Another important relation is defined by an operation.

Definition 1.8: Let S and T be sets. An **binary operation from** S **to** T is a function $f : S \times S \to T$. If $S = T$, we say that f is a binary operation **on** S. A binary operation f on S is **closed** if $f(a,b)$ is defined for all $a, b \in S$.

Example 1.9: Addition of the natural numbers is a map $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$; the sentence, $2+3=5$ can be thought of as $+(2,3) = 5$. Hence addition is a binary operation on $\mathbb{N}$. Addition is defined for all natural numbers, so it is closed.

Subtraction of natural numbers can be viewed as a map as well: $- : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$. However, while subtraction is a binary operation, it is not closed, since it is not "on $\mathbb{N}$": the range ($\mathbb{Z}$) is not the same as the domain ($\mathbb{N}$). This is the reason we need the integers: they "close" subtraction of natural numbers.

Likewise, the rational numbers "close" division for the integers. In advanced calculus you learn that the real numbers "close" limits for the rationals, and in complex analysis (or advanced algebra) you learn that complex numbers "close" algebra for the reals.

1.1: Some facts about the integers

In each set described above, you can perform arithmetic: add, subtract, multiply, and (in most cases) divide.

Definition 1.10: We define the following terms and operations.

- Addition of positive integers is defined in the usual way: for all $a, b \in \mathbb{N}^+$, $a+b$ is the total number of objects obtained from a union between a set of a objects and a set of b objects, with all the objects distinct. We assert without proof that such an addition is always defined, and that it satisfies the following properties:
  commutative: $a+b=b+a$ for all $a, b \in \mathbb{N}^+$;
  associative: $a+(b+c)=(a+b)+c$ for all $a, b, c \in \mathbb{N}^+$.
- 0 is the number such that $a+0=a$ for all $a \in \mathbb{N}^+$.
- For any $a \in \mathbb{N}^+$, we define its negative integer, $-a$, with the property that $a+(-a)=0$.
- Addition of positive and/or negative integers is defined in the usual way. For an example, let $a, b \in \mathbb{N}^+$ and consider $a+(-b)$:
  - If $a=b$, then substitution implies that $a+(-b)=b+(-b)=0$.
  - Suppose that A is a set with a objects.
    - ⋆ If I can remove a set with b objects from A, and have at least one object left over, let $c \in \mathbb{N}^+$ such that $a=b+c$; then we define $a+(-b)=c$.
    - ⋆ If I *cannot* remove a set with b objects from A, then let $c \in \mathbb{N}^+$ be the number of objects I would need to add to A so that I could remove at least b objects. This satisfies the equation $a+c=b$; we then define $a+(-b)=-c$.
- Multiplication is defined in the usual way: Let $a \in \mathbb{N}^+$ and $b \in \mathbb{Z}$.
  - $0 \cdot b = 0$ and $b \cdot 0 = 0$;[a]
  - $a \cdot b$ is the result of adding a list of a copies of b;
  - $(-a) \cdot b = -(a \cdot b)$.

[a] We show in Chapter 7 that this property is a consequence of properties already considered!

Notation 1.11: For convenience, we usually write $a-b$ instead of $a+(-b)$.

Notice that we say nothing about the "ordering" of these numbers; that is, we do not "know" yet whether 1 comes before 2 or vice versa. A natural ordering is implied by the question of whether we can "take elements away"; we will see this shortly in Definition 1.12, but this requires some preliminaries.

It is possible to construct $\mathbb{Z}$ and show that it satisfies the properties above using a smaller number of assumptions, but that is beyond the scope of this course.[10] Instead, we will assume that $\mathbb{Z}$ exists with its arithmetic operations as you know them. We will *not* assume the ordering relations on $\mathbb{Z}$.

Definition 1.12: We define the following relations on $\mathbb{Z}$. For any two elements $a, b \in \mathbb{Z}$, we say that:

- $a \leq b$ if $b - a \in \mathbb{N}$;
- the negation of $a \leq b$ is $a > b$—that is, $a > b$ if $b - a \notin \mathbb{N}$;
- $a < b$ if $b - a \in \mathbb{N}^+$;
- the negation of $a < b$ is $a \geq b$; that is, $a \geq b$ if $b - a \notin \mathbb{N}^+$.

So $3 < 5$ because $5 - 3 \in \mathbb{N}^+$. Notice how the negations work: the negation of $<$ is *not* $>$.

Remark 1.13: You should not assume certain "natural" properties of these orderings. For example, it is true that if $a \leq b$, then either $a < b$ or $a = b$. But why? You can reason to it from the definitions given here, so you should do so.

More importantly, you cannot yet assume that if $a \leq b$, then $a + c \leq b + c$. You can reason to this property from the definitions, and you will do so in the exercises.

The relations $\leq$ and $\subseteq$ have something in common: just as $\mathbb{N} \subseteq \mathbb{Z}$ and $\mathbb{N} \subsetneq \mathbb{Z}$ are simultaneously true, both $3 \leq 5$ and $3 < 5$ are simultaneously true. However, there is one important difference between the two relations. Given two distinct integers (such as 3 and 5) you have always been able to order them using $\leq$. You *cannot* always order any two distinct sets using $\subseteq$. For example, $\{a, b\}$ and $\{c, d\}$ cannot be ordered.

This seemingly unremarkable observation leads to an important question: can you *always* order *any* two integers? Relations satisfying this property merit a special status.

Definition 1.14: Let S be any set. A **linear ordering** on S is a relation $\sim$ where for any $a, b \in S$ one of the following holds:

$$a \sim b,\ a = b, \text{ or } b \sim a.$$

The subset relation is *not* a linear ordering, since

$$\{a, b\} \not\subseteq \{c, d\},\ \{a, b\} \neq \{c, d\}, \text{ and } \{c, d\} \not\subseteq \{a, b\}.$$

However, we *can* show that the orderings of $\mathbb{Z}$ are linear.

Theorem 1.15: *The relations $<$, $>$, $\leq$, and $\geq$ are linear orderings of $\mathbb{Z}$.*

Before giving our proof, we must point out that it relies on some unspoken assumptions: in particular, the arithmetic on $\mathbb{Z}$ that we described before. Try to identify where these assumptions

[10] For a taste: the number 0 is defined to represent the empty set $\emptyset$; the number 1 is defined to represent the set $\{\emptyset, \{\emptyset\}\}$; the number 2 is defined to represent the set $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$, and so forth. The arithmetic operations are subsequently defined in appropriate ways, leading to negative numbers, etc.

are used, because when you write your own proofs, you have to ask yourself constantly: Where am I using unspoken assumptions? In such places, either the assertion must be something accepted by the audience (me!), or you have to cite a reference your audience accepts, or you have to prove it explicitly. It's beyond the scope of this course to explain the holes in this proof, but you should at least try to find them.

PROOF: We show that $<$ is linear; the rest are proved similarly.

Let $a, b \in \mathbb{Z}$. Subtraction is closed for $\mathbb{Z}$, so $b-a \in \mathbb{Z}$. By definition, $\mathbb{Z} = \mathbb{N}^+ \cup \{0\} \cup \{-1,-2,\ldots\}$. By the principle of the excluded middle, $b-a$ must be in one of those three subsets of $\mathbb{Z}$.[11]

- If $b-a \in \mathbb{N}^+$, then $a < b$.
- If $b-a = 0$, then $a = b$.
- Otherwise, $b-a \in \{-1,-2,\ldots\}$. By the properties of arithmetic, $-(b-a) \in \mathbb{N}^+$. Again by the properties of arithmetic, $a-b \in \mathbb{N}^+$. So $b < a$.

We have shown that $a < b$, $a = b$, or $b < a$. Since a and b were arbitrary in $\mathbb{Z}$, $<$ is a linear ordering. □

It should be easy to see that the orderings and their linear property apply to all subsets of $\mathbb{Z}$, in particular $\mathbb{N}^+$ and $\mathbb{N}$.[12] Likewise, we can generalize these orderings to the sets $\mathbb{Q}$ and $\mathbb{R}$ in the way that you are accustomed, and you will do so for $\mathbb{Q}$ in the exercises. That said, this relation behaves differently in $\mathbb{N}$ than it does in $\mathbb{Z}$.

Definition 1.16: Let S be a set and $\prec$ a linear ordering on S. We say that $\prec$ is a **well-ordering** if

Every nonempty subset T of S has a **smallest element** a;
that is, there exists $a \in T$ such that for all $b \in T$, $a \prec b$ or $a = b$.

Example 1.17: The relation $<$ is *not* a well-ordering of $\mathbb{Z}$, because $\mathbb{Z}$ itself has no smallest element under the ordering.

Why not? Proceed by way of contradiction. Assume that $\mathbb{Z}$ has a smallest element, and call it a. Certainly $a-1 \in \mathbb{Z}$ also, but

$$(a-1)-a = -1 \notin \mathbb{N}^+,$$

so $a \not< a-1$. Likewise $a \neq a-1$. This contradicts the definition of a smallest element, so $\mathbb{Z}$ is not well-ordered by $<$.

We now assume, *without proof*, the following principle.

[11] In logic, the *principle of the excluded middle* claims, "If we know that the statement A or B is true, then if A is false, B must be true." There are logicians who do not assume it, including a field of mathematics and computer science called "fuzzy logic". This principle is another unspoken assumption of algebra. In general, you do not have to cite the principle of the excluded middle, but you ought to be aware of it.

[12] If you don't think it's easy, ***good***. Whenever an author writes that something is "easy", he's being a little lazy, which exposes the possibility of an error. So it might not be so easy after all, because it could be false. Saying that something is "easy" is a way of weaseling out of a proof *and* intimidating the reader out of doubting it. So whenever you read something like, "It should be easy to see that…" ***stop*** and ask yourself why it's true.

The relations $<$ and $\leq$ are well-orderings of $\mathbb{N}$.

That is, any subset of $\mathbb{N}$, ordered by these orderings, has a smallest element. This may sound obvious, but it is very important, and what is remarkable is that *no one can prove it.*[13] It is an assumption about the natural numbers. This is why we state it as a principle (or axiom, if you prefer). In the future, if we talk about the well-ordering of $\mathbb{N}$, we mean the well-ordering $<$.

A consequence of the well-ordering property is the principle of:

Theorem 1.18 (Mathematical Induction): *Let P be a subset of $\mathbb{N}^+$. If P satisfies (IB) and (IS) where*
(IB) $1 \in P$;
(IS) *for every $i \in P$, we know that $i+1$ is also in P;*
then $P = \mathbb{N}^+$.

PROOF: Let $S = \mathbb{N}^+ \backslash P$. We will prove the contrapositive, so assume that $P \neq \mathbb{N}^+$. Thus $S \neq \emptyset$. Note that $S \subseteq \mathbb{N}^+$. By the well-ordering principle, S has a smallest element; call it n.

- If $n = 1$, then $1 \in S$, so $1 \notin P$. Thus P does not satisfy (IB).
- If $n \neq 1$, then $n > 1$ by the properties of arithmetic. Since n is the smallest element of S and $n-1 < n$, we deduce that $n-1 \notin S$. Thus $n-1 \in P$. Let $i = n-1$; then $i \in P$ and $i+1 = n \notin P$. Thus P does not satisfy (IS).

We have shown that if $P \neq \mathbb{N}^+$, then P fails to satisfy at least one of (IB) or (IS). This is the contrapositive of the theorem. □

Induction is an enormously useful tool, and we will make use of it from time to time. You may have seen induction stated differently, and that's okay. There are several kinds of induction which are all equivalent. We use the form given here for convenience.

Before moving to algebra, we need one more property of the integers.

Theorem 1.19 (The Division Theorem for Integers): *Let $n, d \in \mathbb{Z}$ with $d \neq 0$. There exist unique $q, r \in \mathbb{Z}$ satisfying (D1) and (D2) where*
(D1) $n = qd + r$;
(D2) $0 \leq r < |d|$.

PROOF: We consider two cases: $0 < d$, and $d < 0$. First we consider $0 < d$. We must show two things: first, that q and r exist; second, that r is unique.

Existence of q and r: First we show the existence of q and r that satisfy (D1). Let $S = \{n - qd : q \in \mathbb{Z}\}$ and $M = S \cap \mathbb{N}$. Exercise 1.29 shows that M is non-empty. By the well-ordering of $\mathbb{N}$, M has a smallest element; call it r. By definition of S, there exists $q \in \mathbb{Z}$ such that $n - qd = r$. Properties of arithmetic imply that $n = qd + r$.

Does r satisfy (D2)? By way of contradiction, assume that it does not; then $|d| \leq r$. We had assumed that $0 < d$, so Exercise 1.25 implies that $0 \leq r - d < r$. Rewrite property (D1)

[13] You might try to prove the well-ordering of $\mathbb{N}$ using induction. But you can't, because it is equivalent to induction. Whenever you have one, you get the other.

using properties of arithmetic:

$$\begin{aligned} n &= qd + r \\ &= qd + d + (r - d) \\ &= (q+1)\,d + (r-d)\,. \end{aligned}$$

Hence $r - d = n - (q+1)\,d$. This form of $r-d$ shows that $r - d \in S$. Recall $0 \leq r - d$; by definition, $r - d \in \mathbb{N}$, so $r - d \in M$. This contradicts the choice of r as the *smallest* element of M.

Hence $n = qd + r$ and $0 \leq r < d$; q and r satisfy (D1) and (D2).

Uniqueness of q and r: Suppose that there exist $q', r' \in \mathbb{Z}$ such that $n = q'd + r'$ and $0 \leq r' < d$. By definition of S, $r' = n - q'd \in S$; by assumption, $r' \in \mathbb{N}$, so $r' \in S \cap \mathbb{N} = M$. Since r is minimal in M, we know that $0 \leq r \leq r' < d$. By substitution,

$$\begin{aligned} r' - r &= (n - q'd) - (n - qd) \\ &= (q - q')\,d. \end{aligned}$$

Moreover, $r \leq r'$ implies that $r' - r \in \mathbb{N}$, so by substitution $(q - q')\,d \in \mathbb{N}$. Similarly, $0 \leq r \leq r'$ implies that $0 \leq r' - r \leq r'$. Thus $0 \leq (q - q')\,d \leq r'$. From properties of arithmetic, $0 \leq q - q'$. If $0 \neq q - q'$, then $1 \leq q - q'$, so $d \leq (q - q')\,d$, so $d \leq (q - q')\,d \leq r' < d$, a contradiction. Hence $q - q' = 0$, and by substitution, $r - r' = 0$.

We have shown that if $0 < d$, then there exist unique $q, r \in \mathbb{Z}$ satisfying (D1) and (D2). We still have to show that this is true for $d < 0$. In this case, $0 < |d|$, so we can find unique $q, r \in \mathbb{Z}$ such that $n = q\,|d| + r$ and $0 \leq r < |d|$. By properties of arithmetic, $q\,|d| = q\,(-d) = (-q)\,d$, so $n = (-q)\,d + r$. □

Definition 1.20 (terms associated with division): Let $n, d \in \mathbb{Z}$ and suppose that $q, r \in \mathbb{Z}$ satisfy the Division Theorem. We call n the **dividend**, d the **divisor**, q the **quotient**, and r the **remainder**.
Moreover, if $r = 0$, then $n = qd$. In this case, we say that d **divides** n, and write $d \mid n$. We also say that n is **divisible by** d. If on the other hand $r \neq 0$, then d **does not divide** n, and we write $d \nmid n$.

Exercises.

Exercise 1.21: Show that we can order any subset of $\mathbb{Z}$ linearly by $<$.

Exercise 1.22: Identify the quotient and remainder when dividing:
(a) 10 by -5;
(b) -5 by 10;
(c) -10 by -4.

Exercise 1.23: Let $a \in \mathbb{Z}$. Show that:
(a) $a \leq a+1$;
(b) if $a \in \mathbb{N}$, then $0 \leq a$; and
(c) if $a \in \mathbb{N}^+$, then $1 \leq a$.

Exercise 1.24: Let $a, b \in \mathbb{Z}$.
(a) Prove that if $a \leq b$, then $a = b$ or $a < b$.
(b) Prove that if both $a \leq b$ and $b \leq a$, then $a = b$.

Exercise 1.25: Let $a, b \in \mathbb{N}$ and assume that $0 < a < b$. Let $d = b - a$. Show that $d < b$.

Exercise 1.26: Let $a, b, c \in \mathbb{Z}$ and assume that $a \leq b$. Prove that
(a) $a + c \leq b + c$;
(b) if $a, c \in \mathbb{N}^+$, $a \leq ac$; and
(c) if $c \in \mathbb{N}^+$, then $ac \leq bc$.

Exercise 1.27: Prove that if $a \in \mathbb{Z}$, $b \in \mathbb{N}^+$, and $a \mid b$, then $a \leq b$.

Note: You may henceforth assume this for *all* the inequalities given in Definition 1.12.

Exercise 1.28: Let $S \subseteq \mathbb{N}$. We know from the well-ordering property that S has a smallest element. Prove that this smallest element is unique.

Exercise 1.29: Let $n, d \in \mathbb{Z}$, where $d \in \mathbb{N}^+$. Define $M = \{n - qd : q \in \mathbb{Z}\}$. Prove that $M \cap \mathbb{N} \neq \emptyset$.

Exercise 1.30: Show that $>$ is not a well-ordering of $\mathbb{N}$.

Exercise 1.31: Show that the ordering $<$ of $\mathbb{Z}$ generalizes "naturally" to an ordering $<$ of $\mathbb{Q}$ that is also a linear ordering.

Exercise 1.32: Show that divisibility is transitive for the integers; that is, if $a, b, c \in \mathbb{Z}$, $a \mid b$, and $b \mid c$, then $a \mid c$.

1.2: Integers, monomials, and monoids

By "monomials", we mean

$$\mathbb{M} = \{x^a : a \in \mathbb{N}\} \quad \text{or} \quad \mathbb{M}_n = \left\{ \prod_{i=1}^{m} \left(x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_n^{a_{in}} \right) : m, a_{ij} \in \mathbb{N} \right\}.$$

Notice that we consider only those products with nonnegative exponents, and do not allow coefficients in monomials. The definition of $\mathbb{M}_n$ indicates that any of its elements is a "product of products".

Example 1.33: The following are monomials:

$$x^2, \quad 1 = x^0 = x_1^0 x_2^0 \cdots x_n^0, \quad x^2 y^3 x y^4.$$

The following, however, are *not* monomials:

$$x^{-1} = \frac{1}{x}, \quad \sqrt{x} = x^{\frac{1}{2}}, \quad \sqrt[3]{x^2} = x^{\frac{2}{3}}.$$

We are interested in similarities between $\mathbb{N}$ and $\mathbb{M}$. Why? Suppose that we can identify a structure common to the two sets. If we make the obvious properties of this structure precise, we can determine non-obvious properties that must be true about $\mathbb{N}$, $\mathbb{M}$, and any other set that adheres to the structure.

If we can prove a fact about a structure,
then we don't have to re-prove that fact for all its elements.
This ***saves*** *time and* ***increases*** *understanding.*

Admittedly, it's harder at first to think about general structures rather than concrete objects, but time, effort, and determination bring agility.

To begin with, what operation(s) should we normally associate with $\mathbb{M}$? We normally associate addition and multiplication with the natural numbers, but the monomials are *not* closed under addition. After all, $x^2 + x^4$ is a *polynomial*, not a monomial. On the other hand, $x^2 \cdot x^4$ is a monomial, and in fact $x^a x^b \in \mathbb{M}$ for any choice of $a, b \in \mathbb{N}$. In fact, this is true about monomials in any number of variables.

Lemma 1.34: *Let $n \in \mathbb{N}^+$. Both $\mathbb{M}$ and $\mathbb{M}_n$ are closed under multiplication.*

PROOF: We show this is true for $\mathbb{M}$, and leave $\mathbb{M}_n$ to the exercises. Let $t, u \in \mathbb{M}$. By definition, there exist $a, b \in \mathbb{N}$ such that $t = x^a$ and $u = x^b$. By definition of monomial multiplication and by closure of addition in $\mathbb{N}$, we see that

$$t u = x^{a+b} \in \mathbb{M}.$$

□

Thanks to this lemma, we henceforth associate the monomials with the operation of multiplication.

Next, is multiplication commutative or associative? That depends on what the variables represent!

Example 1.35: Suppose that x_1 and x_2 represent matrices. There exist abundant examples where $x_1 x_2 \neq x_2 x_1$.

So multiplication of monomials should not in general be considered commutative. This is, in fact, why we defined $\mathbb{M}_n$ as a product of products, rather than combining the factors into one product in the form $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$.

On the other hand, they *are* associative, and this is easy to show.

Lemma 1.36: *Let $n \in \mathbb{N}^+$. Multiplication in $\mathbb{M}$ satifies the commutative property. Multiplication in both $\mathbb{M}$ and $\mathbb{M}_n$ satisfies the associative property.*

PROOF: Again, we show this to be true for $\mathbb{M}$, and leave the proof for $\mathbb{M}_n$ to the exercises. Let $t, u, v \in \mathbb{M}$. By definition, there exist $a, b, c \in \mathbb{N}$ such that $t = x^a$, $u = x^b$, and $v = x^c$. By definition of monomial multiplication and by the commutative property of addition in $\mathbb{M}$, we see that

$$tu = x^{a+b} = x^{b+a} = ut.$$

By definition of monomial multiplication and by the associative property of addition in $\mathbb{N}$, we see that

$$t(uv) = x^a\left(x^b x^c\right) = x^a x^{b+c} = x^{a+(b+c)} = x^{(a+b)+c} = x^{a+b}x^c = (tu)v.$$

□

You might ask yourself, *Do I have to show* every *step?* That depends on what the reader needs to understand the proof. In the equation above, it *is* essential to show that the commutative and associative properties of multiplication in $\mathbb{M}$ depend strictly on the commutative and associative properties of addition in $\mathbb{N}$. Thus, the steps

$$x^{a+b} = x^{b+a} \quad \text{and} \quad x^{a+(b+c)} = x^{(a+b)+c},$$

with the parentheses as indicated, are absolutely crucial, and cannot be omitted from a good proof.[14]

Another property the natural numbers have is that of an identity: both additive and multiplicative. Since we associate only multiplication with the monomials, we should check whether they have a multiplicative identity. Of course, you know this one:

Lemma 1.37: *Both $\mathbb{M}$ and $\mathbb{M}_n$ have $1 = x^0 = x_1^0 x_2^0 \cdots x_n^0$ as a multiplicative identity.*

We won't bother proving this one, but leave it to the exercises.

There are quite a few other properties that the integers and the monomials share, but the three properties we have mentioned here are already quite interesting, and as such are precisely the ones we want to highlight. This motivates the following definition.

[14]Of course, a professional mathematician would not even prove these things in a paper, because they are well-known and easy. On the other hand, a good professional mathematician *would* feel compelled to include in a proof steps that include novel and/or difficult information.

Definition 1.38: Let M be a set, and $\circ$ an operation on M. We say that the pair $(M,\circ)$ is a **monoid** if it satisfies the following properties:

(closure) for any $x,y \in M$, we have $x \circ y \in M$;

(associativity) for any $x,y,z \in M$, we have $(x \circ y) \circ z = x \circ (y \circ z)$; and

(identity) there exists an **identity element** $e \in M$ such that for any $x \in M$, we have $e \circ x = x \circ e = x$.

We may also say that M is a **monoid under** $\circ$.

So far, then, we know the following:

Theorem 1.39: *$\mathbb{N}$ is a monoid under addition and multiplication, while , $\mathbb{M}$ and $\mathbb{M}_n$ are monoids under multiplication.*

PROOF: For $\mathbb{N}$, this is part of Definition 1.10. For $\mathbb{M}$ and $\mathbb{M}_n$, see Lemmas 1.34, 1.36, and 1.37. □

Generally, we don't write the operation in conjunction with the set; we write the set alone, leaving it to the reader to infer the operation. In some cases, this might lead to ambiguity; after all, both $(\mathbb{N},+)$ and $(\mathbb{N},\times)$ are monoids, so which should we prefer? We will prefer $(\mathbb{N},+)$ as the usual monoid associated with $\mathbb{N}$. Thus, we can write that $\mathbb{N}$, $\mathbb{M}$, and $\mathbb{M}_n$ are examples of monoids: the first under addition, the others under multiplication.

What other mathematical objects are examples of monoids?

Example 1.40: You should have seen in linear algebra that the set of square matrices $\mathbb{R}^{m\times m}$ satisfies properties that make it a monoid under both addition and multiplication. Of course, your professor almost certainly didn't *call* it a monoid at the time.

Here's a more interesting example.

Example 1.41: Let S be a set, and let F_S be the set of all functions mapping S to itself, with the proviso that for any $f \in F_S$, $f(s)$ is defined for every $s \in S$. We can show that F_S is a monoid under composition of functions, since

- for any $f,g \in F_S$, we also have $f \circ g \in F_S$, where $f \circ g$ is the function h such that for any $s \in S$,
$$h(s) = (f \circ g)(s) = f(g(s))$$
(notice how important it was that $g(s)$ have a defined value regardless of the value of s);
- for any $f,g,h \in F_S$, we have $(f \circ g) \circ h = f \circ (g \circ h)$, since for any $s \in S$,
$$((f \circ g) \circ h)(s) = (f \circ g)(h(s)) = f(g(h(s)))$$
and
$$(f \circ (g \circ h))(s) = f((g \circ h)(s)) = f(g(h(s)));$$
- if we denote the identity function by $\iota \in F_S$, so that $\iota(s) = s$ for all $s \in S$, then for any $f \in F_S$, we have $\iota \circ f = f \circ \iota = f$, since for any $s \in S$,
$$(\iota \circ f)(s) = \iota(f(s)) = f(s) \quad \text{and} \quad (f \circ \iota)(s) = f(\iota(s)) = f(s)$$

(we can say that $\iota(f(s)) = f(s)$ because $f(s) \in S$).

Although monoids are useful, they are a bit too general for our purposes. Not all the properties we found for $\mathbb{N}$ will hold for all monoids. For example, the Division Theorem doesn't actually make sense in the context of a monoid; it requires *two* operations: multiplication (by the quotient) and addition (of the remainder). So, we will need a more specialized structure to talk about the Division Theorem in a general context, and we will actually meet one later! (in Section 7.4.)

Here is one useful property that we can prove already. A natural question to ask about monoids is whether the identity of a monoid is unique. It isn't hard to show that it is. We can also show a little more.

Theorem 1.42: *Suppose that M is a monoid, and there exist $e, i \in M$ such that $ex = x$ and $xi = x$ for all $x \in M$. Then $e = i$ and in fact the identity of a monoid is unique.*

"Unique" in mathematics means *exactly one*. To prove uniqueness of an object x, you consider a generic object y that shares all the properties of x, then reason to show that $x = y$. This is not a contradiction, because we didn't assume that $x \neq y$ in the first place; we simply wondered about a generic y. We did the same thing with the Division Theorem (Theorem 1.19 on page 9).

PROOF: Suppose that e is a left identity, and i is a right identity. Since i is a right identity, we know that

$$e = ei.$$

Since e is a left identity, we know that

$$ei = i.$$

By substitution,

$$e = i.$$

We chose an arbitrary left identity of M and an arbitrary right identity of M, and showed that they were in fact the same element. Hence left identities are also right identities. This implies in turn that there is only one identity: any identity is both a left identity and a right identity, so the argument above shows that any two identities are in fact identical. □

Exercises.

Exercise 1.43: Is $\mathbb{N}$ a monoid under:
(a) subtraction?
(b) multiplication?
(c) division?
Be sure to explain your answer.

Exercise 1.44: Is $\mathbb{Z}$ a monoid under:
(a) addition?

(b) subtraction?
(c) multiplication?
(d) division?
Be sure to explain your answer.

Exercise 1.45: Consider the set $B = \{F, T\}$ with the operation $\vee$ where

$$\begin{aligned} F \vee F &= F \\ F \vee T &= T \\ T \vee F &= T \\ T \vee T &= T. \end{aligned}$$

This operation is called **Boolean or**.

Is $(B, \vee)$ a monoid? If so, explain how it justifies each property.

Exercise 1.46: Consider the set $B = \{F, T\}$ with the operation $\oplus$ where

$$\begin{aligned} F \oplus F &= F \\ F \oplus T &= T \\ T \oplus F &= T \\ T \oplus T &= F. \end{aligned}$$

This operation is called **Boolean exclusive or**, or **xor** for short.

Is $(B, \oplus)$ a monoid? If so, explain how it justifies each property.

Exercise 1.47: Show that multiplication in $\mathbb{M}_n$ is both closed and associative.

Exercise 1.48:
(a) Show that $\mathbb{N}[x]$, the ring of polynomials in one variable with integer coefficients, is a monoid under addition.
(b) Show that $\mathbb{N}[x]$ is also a monoid if the operation is multiplication.
(c) Explain why we can replace $\mathbb{N}$ by $\mathbb{Z}$ and the argument would remain valid. (*Hint:* think about the *structure* of these sets.)

Definition 1.49: For any set S, let $P(S)$ denote the set of all subsets of S. We call this the **power set** of S.

Exercise 1.50: (a) Suppose $S = \{a, b\}$. Compute $P(S)$, and show that it is a monoid under $\cup$ (union).
(b) Let S be *any* set. Show that $P(S)$ is a monoid under $\cup$ (union).

Exercise 1.51: This problem uses the power set $P(S)$ from Exercise 1.50.
(a) Suppose $S = \{a, b\}$. Compute $P(S)$, and show that it is a monoid under $\cap$ (intersection).
(b) Show that $P(S)$ is a monoid under $\cap$ (intersection).

Definition 1.52: We define lcm, the **least common multiple** of two integers, as

$$\operatorname{lcm}(a,b) = \min\{n \in \mathbb{N} : n \geq |a|,\ n \geq |b|,\ a \mid n, \text{ and } b \mid n\}.$$

Exercise 1.53: Show that $(\mathbb{N}, \operatorname{lcm})$ is a monoid. Note that the operation here looks unusual: instead of something like $x \circ y$, you're looking at $\operatorname{lcm}(x,y)$.

Exercise 1.54: Recall the usual ordering $<$ on $\mathbb{M}$: $x^a < x^b$ if $a < b$. Show that this is a well-ordering.

Note: While we can define a well-ordering on $\mathbb{M}_n$, it is a much more complicated proposition, which we take up in Section 10.2.

Exercise 1.55: In Exercise 1.32, you showed that divisibility is transitive in the integers.

(a) Show that divisibility is transitive in *any* monoid; that is, if M is a monoid, $a, b, c \in M$, $a \mid b$, and $b \mid c$, then $a \mid c$.

(b) In fact, you don't need all the properties of a monoid for divisibility to be transitive! Which properties *do* you need?

1.3: Direct Products and Isomorphism

We've shown that several important sets share the monoid structure. In particular, $(\mathbb{N}, +)$ and $(\mathbb{M}, \times)$ are very similar. Is there some way of arguing that they are in fact identical *as monoids*? We ordinarily call this property *isomorphism*.

Let S and T be any two sets. A mapping $f : S \to T$ is a **function** if for every input $x \in S$ the output $f(x)$ has precisely one value in T. In high school algebra, you learned that this means that f passes the "vertical line test." The reader might suspect at this point—one could hardly blame you—that we are going to generalize the notion of function to something more general, just as we generalized $\mathbb{Z}$, $\mathbb{M}$, etc. to monoids. To the contrary; we will *specialize* the notion of a function in a way that tells us important information about a monoid.

Suppose M and N are monoids. We want a function *that preserves the behavior of the operation* between the domain, M, and the range, N. What does that mean? Let $x, y, z \in M$ and $a, b, c \in N$. Suppose that $f(x) = a$, $f(y) = b$, $f(z) = c$, and $xy = z$. If we are to preserve the operation's behavior:

- since $xy = z$,
- we want $ab = c$, or $f(x) f(y) = f(z)$.

Substituting z for xy suggests that we want the property

$$f(x) f(y) = f(xy).$$

Of course, we also want to preserve the identity.

Definition 1.56: Let $(M,\times)$ and $(N,+)$ be monoids. We say that M is **isomorphic** to N, and write $M \cong N$, if there exists a one-to-one and onto function $f : M \longrightarrow N$ such that

- $f(1_M) = 1_N$; *(f preserves the identity)*

and

- $f(xy) = f(x) + f(y)$ for every $x, y \in M$. *(f preserves the operation)*

We call f an **isomorphism**. (A function that is one-to-one and onto is often called a **bijection**.)

You may not remember the definitions of one-to-one and onto, or you may not understand how to prove them, so we provide them here as a reference.

Definition 1.57: Let $f : S \to U$ be a mapping of sets.

- We say that f is **one-to-one** if for every $a, b \in S$ where $f(a) = f(b)$, we have $a = b$.
- We say that f is **onto** if for every $x \in U$, there exists $a \in S$ such that $f(a) = x$.

Another way of saying that a function $f : S \to U$ is onto is to say that $f(S) = U$; that is, the image of S is *all* of U, or that *every* element of U corresponds via f to some element of S.

We used $(M,\times)$ and $(N,+)$ in the definition partly to suggest our goal of showing that $\mathbb{M}$ and $\mathbb{N}$ are isomorphic, but also because they could stand for *any* monoids. You will see in due course that not all monoids are isomorphic, but first let's show what we wanted to see.

Example 1.58: We claim that $(\mathbb{M},\times)$ is isomorphic to $(\mathbb{N},+)$. To see why, let $f : \mathbb{M} \longrightarrow \mathbb{N}$ by

$$f(x^a) = a.$$

First we show that f is a bijection.

To see that it is one-to-one, let $t, u \in \mathbb{M}$, and assume that $f(t) = f(u)$. By definition of $\mathbb{M}$, $t = x^a$ and $u = x^b$ for $a, b \in \mathbb{N}$. By definition of f, $f(x^a) = f\left(x^b\right)$; by substitution, $a = b$. In this case, $x^a = x^b$, so $t = u$. We assumed that $f(t) = f(u)$ for arbitrary $t, u \in \mathbb{M}$, and showed that $t = u$; that proves f is one-to-one.

To see that it is onto, let $a \in \mathbb{N}$. We need to find $t \in \mathbb{M}$ such that $f(t) = a$. Which t should we choose? The "natural" choice seems to be $t = x^a$; that would guarantee $f(t) = a$. Since $x^a \in \mathbb{M}$, we can in fact make this choice! We took an arbitrary element $a \in \mathbb{N}$, and showed that f maps some element of $\mathbb{M}$ to a; that proves f is onto.

So f is a bijection. Is it also an isomorphism? First we check that f preserves the operation. Let $t, u \in \mathbb{M}$.[15] By definition of $\mathbb{M}$, $t = x^a$ and $u = x^b$ for $a, b \in \mathbb{N}$. We now manipulate

[15]The definition uses the variables x and y, but those are just letters that stand for arbitrary elements of M. Here $M = \mathbb{M}$ and we can likewise choose any two letters we want to stand in place of x and y. It would be a very bad idea to use x when talking about an arbitrary element of $\mathbb{M}$, because there *is* an element of $\mathbb{M}$ called x. So we choose t and u instead.

$f(tu)$ using definitions and substitutions to show that the operation is preserved:

$$f(tu) = f\left(x^a x^b\right) = f\left(x^{a+b}\right) = a+b = f(x^a) + f\left(x^b\right) = f(t) + f(u).$$

Does f also preserve the identity? We usually write the identity of $M = \mathbb{M}$ as the symbol 1, but recall that this is a convenient stand-in for x^0. On the other hand, the identity (under addition) of $N = \mathbb{N}$ is the number 0. We use this fact to verify that f presernves the identity:

$$f(1_M) = f(1) = f\left(x^0\right) = 0 = 1_N.$$

(We don't usually write 1_M and 1_N, but I'm doing it here to show explicitly how this relates to the definition.)

We have shown that there exists a bijection $f : \mathbb{M} \longrightarrow \mathbb{N}$ that preserves the operation and the identity. We conclude that $\mathbb{M} \cong \mathbb{N}$.

On the other hand, is $(\mathbb{N}, +) \cong (\mathbb{N}, \times)$? The sets are the same, but the operations is different. Let's see what happens.

Example 1.59: In fact, $(\mathbb{N}, +) \ncong (\mathbb{N}, \times)$. To show this, we proceed by contradiction. Suppose there *does* exist an isomorphism f between the two monoids. What would have to be true about f?

We know that f preserves the identity; that is, $f(0) = 1$. After all, 0 is the identity of $(\mathbb{N}, +)$, while 1 is the identity of $(\mathbb{N}, \times)$. We also know that f preserves the operation, so for any $x, y \in \mathbb{N}$, we would *have* to have $f(x+y) = f(x) f(y)$. Let's see if that's actually possible. Let $a \in \mathbb{N}$ such that $f(1) = a$; after all, f has to map 1 to *something!* Then

$$\begin{aligned} &f(2) = f(1+1) = f(1) \times f(1) = a^2 \text{ and} \\ &f(3) = f(1+(1+1)) = f(1) \times f(1+1) = a^3, \text{ so that} \\ &f(n) = \cdots = f(1)^n \text{ for } \textit{any } n \in \mathbb{N}. \end{aligned}$$

So f sends *every* integer in $(\mathbb{N}, +)$to a power of a.

Think about what this implies. For f to be a bijection, it would have to be onto, so *every* element of $(\mathbb{N}, \times)$ would *have* to be an integer power of a. ***This is false!*** After all, 2 is not an integer power of 3, and 3 is not an integer power of 2.

The claim was correct: $(\mathbb{N}, +) \ncong (\mathbb{N}, \times)$.

You will show in the exercises that $\cong$ is an equivalence relation; thus, we can also conclude that $(\mathbb{N}, \times) \ncong (\mathbb{N}, +)$.

Let's look again at monomials. It might have occurred to you that we can view any element of $\mathbb{M}_n$ as a list of n elements of $\mathbb{M}$. (Pat yourself on the back if so.) If not, here's an example:

$$x_1^6 x_2^3 \text{ looks an awful lot like } \left(x^6, x^3\right).$$

We can do this with other sets, as well; creating new sets via lists of elements of old sets is very useful.

Definition 1.60: Let $r \in \mathbb{N}^+$ and $S_1, S_2, \ldots, S_r$ be sets. The **Cartesian product** of $S_1, \ldots, S_r$ is the set of all lists of r elements where the ith entry is an element of S_i; that is,

$$S_1 \times \cdots \times S_r = \{(s_1, s_2, \ldots, s_n) : s_i \in S_i\}.$$

Example 1.61: We already mentioned a Cartesian product of two sets in the introduction to this chapter. Another example would be $\mathbb{N} \times \mathbb{M}$; elements of $\mathbb{N} \times \mathbb{M}$ include $(2, x^3)$ and $(0, x^5)$. In general, $\mathbb{N} \times \mathbb{M}$ is the set of all ordered pairs where the first entry is a natural number, and the second is a monomial.

If we can preserve the structure of the underlying sets in a Cartesian product, we call it a *direct product*.

Definition 1.62: Let $r \in \mathbb{N}^+$ and $M_1, M_2, \ldots, M_r$ be monoids. The **direct product** of $M_1, \ldots, M_r$ is the pair

$$(M_1 \times \cdots \times M_r, \otimes)$$

where $M_1 \times \cdots \times M_r$ is the usual Cartesian product, and $\otimes$ is the "natural" operation on $M_1 \times \cdots \times M_r$.
What do we mean by the "natural" operation on $M_1 \times \cdots \times M_r$? Let $x, y \in M_1 \times \cdots \times M_r$; by definition, we can write

$$x = (x_1, \ldots, x_r) \quad \text{and} \quad y = (y_1, \ldots, y_r)$$

where each x_i and each y_i is an element of M_i. Then

$$x \otimes y = (x_1 y_1, x_2 y_2, \ldots, x_r y_r)$$

where each product $x_i y_i$ is performed according to the operation that makes the corresponding M_i a monoid.

Example 1.63: Recall that $\mathbb{N} \times \mathbb{M}$ is a Cartesian product; if we consider the monoids $(\mathbb{N}, \times)$ and $(\mathbb{M}, \times)$, we can show that the direct product is a monoid, much like $\mathbb{N}$ and $\mathbb{M}$! To see why, we check each of the properties.

(closure) Let $t, u \in \mathbb{N} \times \mathbb{M}$. By definition, we can write $t = (a, x^\alpha)$ and $u = \left(b, x^\beta\right)$ for appropriate $a, \alpha, b, \beta \in \mathbb{N}$. Then

$$tu = (a, x^\alpha) \otimes \left(b, x^\beta\right) \underset{\text{def of } \otimes}{=} \left(ab, x^\alpha x^\beta\right) = \left(ab, x^{\alpha+\beta}\right) \in \mathbb{N} \times \mathbb{M}.$$

We took two arbitrary elements of $\mathbb{N} \times \mathbb{M}$, multiplied them according to the new operation, and obtained another element of $\mathbb{N} \times \mathbb{M}$; the operation is therefore closed.

(associativity) Let $t, u, v \in \mathbb{N} \times \mathbb{M}$. By definition, we can write $t = (a, x^\alpha)$, $u = \left(b, x^\beta\right)$, and $v = (c, x^\gamma)$ for appropriate $a, \alpha, b, \beta, c, \gamma \in \mathbb{N}$. Then

$$\begin{aligned} t\,(uv) &= (a, x^\alpha) \otimes \left[\left(b, x^\beta\right) \otimes (c, x^\gamma)\right] \\ &= (a, x^\alpha) \otimes \left(bc, x^\beta x^\gamma\right) \\ &= \left(a\,(bc), x^\alpha \left(x^\beta x^\gamma\right)\right). \end{aligned}$$

To show that this equals $(t\,u)\,v$, we have to rely on the associative properties of $\mathbb{N}$ and $\mathbb{M}$:

$$\begin{aligned} t\,(uv) &= \left((ab)\,c, \left(x^\alpha x^\beta\right) x^\gamma\right) \\ &= \left(ab, x^\alpha x^\beta\right) \otimes (c, x^\gamma) \\ &= \left[(a, x^\alpha) \otimes \left(b, x^\beta\right)\right] \otimes (c, x^\gamma) \\ &= (t\,u)\,v. \end{aligned}$$

We took three elements of $\mathbb{N} \times \mathbb{M}$, and showed that the operation was associative for them. Since the elements were arbitrary, the operation is associative.

(identity) We claim that the identity of $\mathbb{N} \times \mathbb{M}$ is $(1,1) = \left(1, x^0\right)$. To see why, let $t \in \mathbb{N} \times \mathbb{M}$. By definition, we can write $t = (a, x^\alpha)$ for appropriate $a, \alpha \in \mathbb{N}$. Then

$$(1,1) \otimes t \underset{\text{subst.}}{=} (1,1) \otimes (a, x^\alpha) \underset{\text{def of } \otimes}{=} (1 \times a, 1 \times x^\alpha) \underset{\text{mult in } \mathbb{N},\mathbb{M}}{=} (a, x^\alpha) = t$$

and similarly $t \otimes (1,1) = t$. We took an arbitrary element of $\mathbb{N} \times \mathbb{M}$, and showed that $(1,1)$ acted as an identity under the operation $\otimes$ with that element. Since the element was arbitrary, $(1,1)$ must be *the* identity for $\mathbb{N} \times \mathbb{M}$.

Interestingly, if we had used $(\mathbb{N}, +)$ *instead* of $(\mathbb{N}, \times)$ in the previous example, we *still* would have obtained a direct product! Indeed, the direct product of monoids is *always* a monoid!

Theorem 1.64: *The direct product of monoids $M_1, \ldots, M_r$ is itself a monoid. Its identity element is $(e_1, e_2, \ldots, e_r)$, where each e_i denotes the identity of the corresponding monoid M_i.*

PROOF: You do it! See Exercise 1.71. □

We finally turn our attention the question of whether $\mathbb{M}_n$ and $\mathbb{M}^n$ are the same.

Admittedly, the two are not identical: $\mathbb{M}_n$ is the set of *products* of powers of *n distinct* variables, whereas $\mathbb{M}^n$ is a set of *lists* of powers of *one* variable. In addition, if the variables are *not* commutative (remember that this can occur), then $\mathbb{M}_n$ and $\mathbb{M}^n$ are not at all similar. Think about $(xy)^4 = xyxyxyxy$; if the variables are commutative, we can combine them into x^4y^4, which looks likes $(4,4)$. If the variables are not commutative, however, it is not at *all* clear how we could get $(xy)^4$ to correspond to an element of $\mathbb{N} \times \mathbb{N}$.

That leads to the following result.

Theorem 1.65: *The variables of* $\mathbb{M}_n$ *are commutative if and only if then* $\mathbb{M}_n \cong \mathbb{M}^n$.

PROOF: Assume the variables of $\mathbb{M}_n$ are commutative. Let $f : \mathbb{M}_n \longrightarrow \mathbb{M}^n$ by

$$f\left(x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}\right) = \left(x^{a_1}, x^{a_2}, \ldots, x^{a_n}\right).$$

The fact that we cannot combine a_i and a_j if $i \neq j$ shows that f is one-to-one, and any element $\left(x^{b_1}, \ldots, x^{b_n}\right)$ of $\mathbb{M}^n$ has a preimage $x_1^{b_1} \cdots x_n^{b_n}$ in $\mathbb{M}_n$; thus f is a bijection.

Is it also an isomorphism? To see that it is, let $t, u \in \mathbb{M}_n$. By definition, we can write $t = x_1^{a_1} \cdots x_n^{a_n}$ and $u = x_1^{b_1} \cdots x_n^{b_n}$ for appropriate $a_1, b_1 \ldots, a_n, b_n \in \mathbb{N}$. Then

$$\begin{aligned}
f(tu) &= f\left(\left(x_1^{a_1} \cdots x_n^{a_n}\right)\left(x_1^{b_1} \cdots x_n^{b_n}\right)\right) && \text{(substitution)} \\
&= f\left(x_1^{a_1+b_1} \cdots x_n^{a_n+b_n}\right) && \text{(commutative property)} \\
&= \left(x^{a_1+b_1}, \ldots, x^{a_n+b_n}\right) && \text{(definition of } f\text{)} \\
&= \left(x^{a_1}, \ldots, x^{a_n}\right) \otimes \left(x^{b_1}, \ldots, x^{b_n}\right) && \text{(operation of direct product)} \\
&= f(t) \otimes f(u). && \text{(definition of } f\text{)}
\end{aligned}$$

Hence f is an isomorphism, and we conclude that $\mathbb{M}_n \cong \mathbb{M}^n$.

Conversely, suppose $\mathbb{M}_n \cong \mathbb{M}^n$. By Exercise 1.68, $\mathbb{M}_n \cong \mathbb{M}^n$. By definition, there exists a bijection $f : \mathbb{M}^n \longrightarrow \mathbb{M}_n$ satisfying Definition 1.56. Let $t, u \in \mathbb{M}^n$; by definition, we can find $a_i, b_j \in \mathbb{N}$ such that $t = x_1^{a_1} \cdots x_n^{a_n}$ and $u = x_1^{b_1} \cdots x_n^{b_n}$. Since f preserves the operation, $f(tu) = f(t) \otimes f(u)$. Now, $f(t)$ and $f(u)$ are elements of $\mathbb{M}^n$, which is commutative by Exercise 1.67 (with the $S_i = \mathbb{M}$ here). Hence $f(t) \otimes f(u) = f(u) \otimes f(t)$, so that $f(tu) = f(u) \otimes f(t)$. Using the fact that f preserves the operation again, only in reverse, we see that $f(tu) = f(ut)$. Recall that f, as a bijection, is one-to-one! Thus $tu = ut$, and $\mathbb{M}^n$ is commutative. □

Notation 1.66: Although we used $\otimes$ in this section to denote the operation in a direct product, this is not standard; I was trying to emphasize that the product is different for the direct product than for the monoids that created it. In general, the product $x \otimes y$ is written simply as xy. Thus, the last line of the proof above would have $f(t) f(u)$ instead of $f(t) \otimes f(u)$.

Exercises.

Exercise 1.67: Suppose M_1, M_2, …, and M_n are *commutative* monoids. Show that the direct product $M_1 \times M_2 \times \cdots \times M_n$ is also a commutative monoid.

Exercise 1.68: Show that isomorphism is an equivalence relation.

Exercise 1.69: Show that $\mathbb{M}^n \cong \mathbb{N}^n$. What does this imply about $\mathbb{M}_n$ and $\mathbb{N}^n$?

Exercise 1.70: Show that the Boolean-or monoid and the Boolean-xor monoids from Exercises 1.45 and 1.46 are *not* isomorphic.

Exercise 1.71: Prove Theorem 1.64.

Exercise 1.72: Let $\mathbb{T}^n_S$ denote the set of terms in n variables whose coefficients are elements of the set S. For example, $2xy \in \mathbb{T}^2_{\mathbb{Z}}$ and $\pi x^3 \in \mathbb{T}^1_{\mathbb{R}}$.

(a) Show that if S is a monoid, then so is $\mathbb{T}^n_S$.

(b) Show that if S is a monoid, then $\mathbb{T}^n_S \cong S \times \mathbb{M}_n$.

Part II

Groups

Chapter 2:
Groups

In Chapter 1 we described monoids. In this chapter, we study a *group*, which is a kind of monoid; the property that distinguishes groups from other monoids is essential to a large number of mathematical phenomena. We describe a special class of groups called the cyclic groups (Section 2.3) and then look at two example groups related to problems in geometry. The first, D_3, describes symmetries of a triangle using groups (Section 2.2). The second, *elliptic curves*, has received attention in many areas in recent decades (Section 2.5).

2.1: Groups

A group is a monoid where each element has an inverse element. Stated precisely:

Definition 2.1: Let G be a set, and $\circ$ a binary operation on G. We say that the pair $(G,\circ)$ is a **group** if it satisfies the following properties.

(closure) for any $x,y \in G$, we have $x \circ y \in G$;

(associativity) for any $x,y,z \in G$, we have $(x \circ y) \circ z = x \circ (y \circ z)$;

(identity) there exists an **identity element** $e \in G$; that is, for any $x \in G$, we have $x \circ e = e \circ x = x$; and

(inverses) each element of the group has an **inverse**; that is for any $x \in G$ we can find $y \in G$ such that $x \circ y = y \circ x = e$.

We may also say that G is a **group under** $\circ$. We say that $(G,\circ)$ is an **abelian group**[a] if it also satisfies

(commutativity) the operation is commutative; that is, $xy = yx$ for all $x,y \in G$.

If the operation is addition, we may refer to the group as an **additive group** or a **group under addition**. We also write $-x$ instead of x^{-1}, and $x+(-y)$ or even $x-y$ instead of $x+y^{-1}$, keeping with custom. Additive groups are normally abelian.

If the operation is multiplication, we may refer to the group as a **multiplicative group** or a **group under multiplication**. The operation is usually understood from context, so we typically write G rather than $(G,+)$ or $(G,\times)$ or $(G,\circ)$. We will write $(G,+)$ when we want to emphasize that the operation is addition.

[a] Named after Niels Abel, a Norwegian high school mathematics teacher who made important contributions to group theory.

Example 2.2: Certainly $\mathbb{Z}$ is an additive group; in fact, it is abelian. Why?

- Adding two integers gives another integer.
- Addition of integers is associative.

- The additive identity is the number 0.
- Every integer has an additive inverse.
- Addition of integers is commutative. ◿

The same holds true for many of the sets we identified in Chapter 1, using the ordinary definition of addition in that set.

However, while $\mathbb{N}$ is a monoid under addition, it is not a group. Why not? The problem is with inverses. We know that every natural number has an additive inverse; after all, $2+(-2)=0$. Nevertheless, the inverse property is *not* satisfied because $-2 \notin \mathbb{N}$! It's not enough to have an inverse in *some* set; *the inverse be in the same set!* For this reason, $\mathbb{N}$ is not a group.

Example 2.3: Let $n \in \mathbb{N}^+$. The set of invertible $n \times n$ matrices is a multiplicative group. We leave much of the proof to the exercises, but this fact is a consequence of properties you learn in linear algebra.

Definition 2.4: We call the set of invertible $n \times n$ matrices the **general linear group of degree** n, and write $\mathrm{GL}_n(\mathbb{R})$ for this set. ◿

Mathematicians of the 20th century invested substantial effort in an attempt to classify all *finite, simple groups*. (You will learn later what makes a group "simple".) Replicating that achievement is far, far beyond the scope of these notes, but we can take a few steps in this area.

Definition 2.5: Let S be any set. We write $|S|$ to indicate the number of elements in S, and say that $|S|$ is the **size** of S. If there is an infinite number of elements in S, then we write $|S| = \infty$. We also write $|S| < \infty$ to indicate that $|S|$ is finite, if we don't want to state a precise number. For any group G, the **order of** G is the size of G. A group has finite order if $|G| < \infty$ and infinite order if $|G| = \infty$.

Here are three examples of finite groups; in fact, they are all of order 2.

Example 2.6: The sets

$$\{1,-1\}, \quad \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\}, \quad \text{and} \quad \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\}$$

are all groups under multiplication:

- In the first group, the identity is 1, and -1 is its own inverse; closure is obvious, and you know from arithmetic that the associative property holds.
- In the second and third groups, the identity is the identity matrix; closure is easy to verify, and you know from linear algebra that the associative property holds.

I will now make an extraordinary claim:

Claim 1: For all intents and purposes, there is only one group of order two.

This claim may seem preposterous on its face; after all, the example above has three completely different groups of order two. In fact, the claim is quite vague, because we're using vague language. After all, what is meant by the phrase, "for all intents and purposes"? Basically, we meant that:

- group theory cannot distinguish between the groups *as groups;* or,
- their multiplication table (or addition table, or whatever-operation table) has the same structure; or, more precisely,
- the groups are isomorphic.

By "isomorphic", we mean both "isomorphic when viewed as monoids" and "isomorphic when viewed as groups." We won't actually spend time with group isomorphisms until we get to Chapter 4, but Chapter 1 gave you a rough idea of what that meant: the groups are identical *as groups*.

We will prove the claim above in a "brute force" manner, by looking at the table generated by the operation of the group. Now, "the table generated by the operation of the group" is an ungainly phrase, and quite a mouthful. Since the name of the table depends on the operation (multiplication table, addition table, etc.), we have a convenient phrase that describes all of them.

Definition 2.7: The table defining the operation of a monoid is called a **Cayley table**. (Comparable to an addition or multiplication table.)

Since groups are monoids, we can call their table a Cayley table, too.

Back to our claim. We want to build a Cayley table for a "generic" group of order two. We will show that there is only one possible way to construct such a table. As a consequence, regardless of the set and its operation, every group of order 2 behaves exactly the same way. ***It does not matter one whit*** what the elements of G are, or the fancy name we use for the operation, or the convoluted procedure we use to simplify computations in the group. If there are only two elements, and it's a group, then ***it always works the same***. Why?

Example 2.8: Let G be an arbitrary group of order two. By definition, it has an identity, so write $G = \{e, a\}$ where e represents the known identity, and a the other element.

We did *not* say that e represents the *only* identity. For all we know, a might also be an identity; is that possible? In fact, it is not possible; why? Remember that a group is a monoid. We showed in Proposition 2.11 that the identity of a monoid is unique; thus, the identity of a group is unique; thus, there can be only one identity, e.

Now we build the addition table. We *have* to assign $a \circ a = e$. *Why?*

- To satisfy the identity property, we must have $e \circ e = e$, $e \circ a = a$, and $a \circ e = a$.
- To satisfy the inverse property, a must have an additive inverse. We know the inverse can't be e, since $a \circ e = a$; so the only inverse possible is a itself! That is, $a^{-1} = a$. (Read that as, "the inverse of a is a.") So $a \circ a^{-1} = a \circ a = e$.

So the Cayley table of our group looks like:

$\circ$	e	a
e	e	a
a	a	e

The only assumption we made about G is that it was a group of order two. That means this table applies to *any* group of order two, and we have determined the Cayley table of *all* groups of order two! ◿

In Definition 2.1 and Example 2.8, the symbol $\circ$ is a placeholder for any operation. We assumed nothing about its actual behavior, so it can represent addition, multiplication, or other operations that we have not yet considered. Behold the power of abstraction!

Notation 2.9: We adopt the following convention:

- If we know only that G is a group under some operation, we write $\circ$ for the operation and proceed as if the group were multiplicative, writing xy.
- If we know that G is a group and a symbol is provided for its operation, we *usually* use that symbol for the group, *but not always.* Sometimes we treat the group as if it were multiplicative, writing xy instead of the symbol provided.
- We reserve the symbol $+$ exclusively for additive groups.

The following fact looks obvious—but remember, we're talking about elements of *any* group, not merely the sets you have worked with in the past.

Proposition 2.10: *Let G be a group and $x \in G$. Then $\left(x^{-1}\right)^{-1} = x$. If G is additive, we write instead that $-(-x) = x$.*

Proposition 2.10 says that the inverse of the inverse of x is x itself; that is, if y is the inverse of x, then x is the inverse of y.

PROOF: You prove it! See Exercise 2.14. □

Proposition 2.11: *The identity of a group is both two-sided and unique; that is, every group has exactly one identity. Also, the inverse of an element is both two-sided and unique; that is, every element has exactly one inverse element.*

PROOF: Let G be a group. We already pointed out that, since G is a monoid, and the identity of a monoid is both two-sided and unique, the identity of G is unique.

We turn to the question of the inverse. First we show that any inverse is two-sided. Let $x \in G$. Let w be a left inverse of x, and y a right inverse of x. Since y is a right inverse,

$$xy = e.$$

By the identity property, we know that $ex = x$. So, substitution and the associative property give us

$$\begin{aligned}(xy)x &= ex\\ x(yx) &= x.\end{aligned}$$

Since w is a left inverse, $wx = e$, so substitution, the associative property, the identity property, and the inverse property give

$$\begin{aligned} w(x(yx)) &= wx \\ (wx)(yx) &= wx \\ e(yx) &= e \\ yx &= e. \end{aligned}$$

Hence y is a left inverse of x. We already knew that it was a right inverse of x, so right inverses are in fact two-sided inverses. A similar argument shows that left inverses are two-sided inverses.

Now we show that inverses are unique. Suppose that $y, z \in G$ are both inverses of x. Since y is an inverse of x,

$$xy = e.$$

Since z is an inverse of x,

$$xz = e.$$

By substitution,

$$xy = xz.$$

Multiply both sides of this equation on the left by y to obtain

$$y(xy) = y(xz).$$

By the associative property,

$$(yx)y = (yx)z,$$

and by the inverse property,

$$ey = ez.$$

Since e is the identity of G,

$$y = z.$$

We chose two arbitrary inverses of x, and showed that they were the same element. Hence the inverse of x is unique. □

In Example 2.8, the structure of a group compelled certain assignments for addition. We can infer a similar conclusion for any group of finite order.

Theorem 2.12: *Let G be a group of finite order, and let $a, b \in G$. Then a appears exactly once in any row or column of the Cayley table that is headed by b.*

It might surprise you that this is *not* necessarily true for a monoid; see Exercise 2.21.

PROOF: First we show that a cannot appear more than once in any row or column headed by b. In fact, we show it only for a row; the proof for a column is similar.

The element a appears in a row of the Cayley table headed by b any time there exists $c \in G$ such that $bc = a$. Let $c, d \in G$ such that $bc = a$ and $bd = a$. (We have *not* assumed that $c \neq d$.) Since $a = a$, substitution implies that $bc = bd$. Thus

$$c \underset{\text{id.}}{=} ec \underset{\text{inv.}}{=} \left(b^{-1}b\right)c \underset{\text{ass.}}{=} b^{-1}(bc) \underset{\text{subs.}}{=} b^{-1}(bd) \underset{\text{ass.}}{=} \left(b^{-1}b\right)d \underset{\text{inv.}}{=} ed \underset{\text{id.}}{=} d.$$

By the transitive property of equality, $c = d$. This shows that if a appears in one column of the row headed by b, then that column is unique; a does not appear in a different column.

We still have to show that a appears in at least one row of the addition table headed by b. This follows from the fact that each row of the Cayley table contains $|G|$ elements. What applies to a above applies to the other elements, so each element of G can appear at most once. Thus, if we do not use a, then only $n-1$ pairs are defined, which contradicts either the definition of an operation (bx must be defined for all $x \in G$) or closure (that $bx \in G$ for all $x \in G$). Hence a must appear at least once. □

Definition 2.13: Let $G_1, \ldots, G_n$ be groups. The **direct product** of $G_1, \ldots, G_n$ is the cartesian product $G_1 \times \cdots \times G_n$ together with the operation $\otimes$ such that for any $(g_1, \ldots, g_n)$ and $(h_1, \ldots, h_n)$ in $G_1 \times \cdots \times G_n$,

$$(g_1, \ldots, g_n) \otimes (h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n),$$

where each product $g_i h_i$ is performed according to the operation of G_i. In other words, the direct product of *groups* generalizes the direct product of *monoids*.

You will show in the exercises that the direct product of groups is also a group.

Exercises.

Exercise 2.14: Explain why $\left(x^{-1}\right)^{-1} = x$; or if the operation is addition, why $-(-x) = x$.

Exercise 2.15: Explain why $\mathbb{M}$ is not a group.

Exercise 2.16: Let G be a group, and $x, y, z \in G$. Show that if $xz = yz$, then $x = y$; or if the operation is addition, that if $x + z = y + z$, then $x = y$.

Exercise 2.17: Show in detail that $\mathbb{R}^{2\times 2}$ is an additive group.

Exercise 2.18: Recall the Boolean-or monoid $(B, \vee)$ from Exercise 1.45. Is it a group? If so, is it abelian? Explain how it justifies each property. If not, explain why not.

Exercise 2.19: Recall the Boolean-xor monoid $(B, \oplus)$ from Exercise 1.46. Is it a group? If so, is it abelian? Explain how it justifies each property. If not, explain why not.

Exercise 2.20: In Section 1.2, we showed that F_S, the set of all functions, is a monoid for any S.

(a) Show that $F_{\mathbb{R}}$, the set of all functions on the real numbers $\mathbb{R}$, is *not* a group.

(b) Describe a subset of $F_{\mathbb{R}}$ that *is* a group. Another way of looking at this question is: what restriction would you have to impose on any function $f \in F_S$ to fix the problem you found in part (a)?

Exercise 2.21: Indicate a monoid you have studied that does not satisfy Theorem 2.12. That is, find a monoid M such that (i) M is finite, and (ii) there exist $a, b \in M$ such that in the the Cayley table, a appears at least twice in a row or column headed by b.

Exercise 2.22: Show that the Cartesian product

$$\mathbb{Z} \times \mathbb{Z} := \{(a,b) : a, b \in \mathbb{Z}\}$$

is a group under the direct product's notion of addition; that is,

$$x + y = (a + c, b + d).$$

Exercise 2.23: Let $(G, \circ)$ and $(H, *)$ be groups, and define

$$G \times H = \{(a,b) : a \in G,\ b \in H\}.$$

Define an operation $\dagger$ on $G \times H$ in the following way. For any $x, y \in G \times H$, write $x = (a,b)$ and $y = (c,d)$; we say that

$$x \dagger y = (a \circ c, b * d).$$

(a) Show that $(G \times H, \dagger)$ is a group.

(b) Show that if G and H are both abelian, then so is $G \times H$.

Exercise 2.24: Let $n \in \mathbb{N}^+$. Let G_1, G_2, ..., G_n be groups, and consider

$$\prod_{i=1}^{n} G_i := G_1 \times G_2 \times \cdots \times G_n = \{(a_1, a_2, \ldots, a_n) : a_i \in G_i\ \forall i = 1, 2, \ldots, n\}$$

with the operation $\dagger$ where if $x = (a_1, a_2, \ldots, a_n)$ and $y = (b_1, b_2, \ldots, b_n)$, then

$$x \dagger y = (a_1 b_1, a_2 b_2, \ldots, a_n b_n),$$

where each product $a_i b_i$ is performed according to the operation of the group G_i. Show that $\prod_{i=1}^{n} G_i$ is a group, and notice that this shows that the direct product of groups is a group, as claimed above. (We used $\otimes$ instead of $\dagger$ there, though.)

Exercise 2.25: Let $m \in \mathbb{N}^+$.

(a) Show in detail that $\mathbb{R}^{m \times m}$ is a group under addition.

(b) Show by counterexample that $\mathbb{R}^{m\times m}$ is *not* a group under multiplication.

Exercise 2.26: Let $m \in \mathbb{N}^+$. Explain why $\mathrm{GL}_m(\mathbb{R})$ satisfies the identity and inverse properties of a group.

Exercise 2.27: Let $m \in \mathbb{N}^+$ and $G = \mathrm{GL}_m(\mathbb{R})$.
(a) Show that there exist $a, b \in G$ such that $(ab)^{-1} \neq a^{-1}b^{-1}$.
(b) Show that for any $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Exercise 2.28: Let $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$, and $\times$ the ordinary multiplication of real numbers. Show that $\mathbb{R}^+$ is a multiplicative group by explaining why $(\mathbb{R}^+, \times)$ satisfies the properties of a group.

Exercise 2.29: Define $\mathbb{Q}^*$ to be the set of non-zero rational numbers; that is,

$$\mathbb{Q}^* = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \text{ where } a \neq 0 \text{ and } b \neq 0 \right\}.$$

Show that $\mathbb{Q}^*$ is a multiplicative group.

Exercise 2.30: Show that every group of order 3 has the same structure.

Exercise 2.31: *Not* every group of order 4 has the same structure, because there are two Cayley tables with different structures. One of these groups is the **Klein four-group**, where each element is its own inverse; the other is called a **cyclic group** of order 4, where not every element is its own inverse. Determine addition tables for each group.

Exercise 2.32: Let G be a group, and $x, y \in G$. Show that $xy^{-1} \in G$.

Exercise 2.33: Suppose that H is an arbitrary group. Explain why we cannot assume that for every $a, b \in H$, $(ab)^{-1} = a^{-1}b^{-1}$, but we can assume that $(ab)^{-1} = b^{-1}a^{-1}$.

Exercise 2.34: Let $\circ$ denote the ordinary composition of functions, and consider the following functions that map any point $P = (x, y) \in \mathbb{R}^2$ to another point in $\mathbb{R}^2$:

$$\begin{aligned} I(P) &= P, \\ F(P) &= (y, x), \\ X(P) &= (-x, y), \\ Y(P) &= (x, -y). \end{aligned}$$

(a) Let $P = (2,3)$. Label the points P, $I(P)$, $F(P)$, $X(P)$, $Y(P)$, $(F \circ X)(P)$, $(X \circ Y)(P)$, and $(F \circ F)(P)$ on an x-y axis. (Some of these may result in the same point; if so, label the point twice.)
(b) Show that $F \circ F = X \circ X = Y \circ Y = I$.
(c) Show that $G = \{I, F, X, Y\}$ is *not* a group.

(d) Find the smallest group $\overline{G}$ such that $G \subset \overline{G}$. While you're at it, construct the Cayley table for $\overline{G}$.
(e) Is $\overline{G}$ abelian?

Exercise 2.35: Let i be a number such that $i^2 = -1$, and let Q_8 be the set of **quaternions**, defined by the matrices $\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ where

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

(a) Show that $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$.
(b) Show that $\mathbf{ij} = \mathbf{k}$, $\mathbf{jk} = \mathbf{i}$, and $\mathbf{ik} = -\mathbf{j}$.
(c) Use (a) and (b) to build the Cayley table of Q_8. (In this case, the Cayley table is the multiplication table.)
(c) Show that Q_8 is a group under matrix multiplication.
(d) Explain why Q_8 is not an abelian group.

Exercise 2.36: Let G be any group. For all $x, y \in G$, define the **commutator** of x and y to be $x^{-1}y^{-1}xy$. We write $[x,y]$ for the commutator of x and y.
(a) Explain why $[x,y] = e$ iff x and y commute.
(b) Show that $[x,y]^{-1} = [y,x]$; that is, the inverse of $[x,y]$ is $[y,x]$.
(c) Let $z \in G$. Denote the **conjugation of any $g \in G$ by z** as $g^z = zgz^{-1}$. Show that $[x,y]^z = [x^z, y^z]$.

2.2: The symmetries of a triangle

In this section, we show that the symmetries of an equilateral triangle form a group. We call this group D_3. This group *is not abelian.* You already know that groups of order 2, 3, and 4 are abelian; in Section 3.3 you will learn why a group of order 5 must also be abelian. Thus, D_3 is the smallest non-abelian group.

To describe D_3, we start with an equilateral triangle in $\mathbb{R}^2$, with its center at the origin. We want to look at its group of symmetries, where a *symmetry* of the triangle is a distance-preserving function on $\mathbb{R}^2$ that maps points on the triangle back onto itself.

Example 2.37: Two obvious symmetries of an equilateral triangle are a 120° rotation through the origin, and a flip through the y-axis. See Figure 2.1. ◿

What functions are symmetries of the triangle? To answer this question, we divide it into two parts.

1. What are the distance-preserving functions that map $\mathbb{R}^2$ to itself? Here, distance is measured by the usual metric,

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

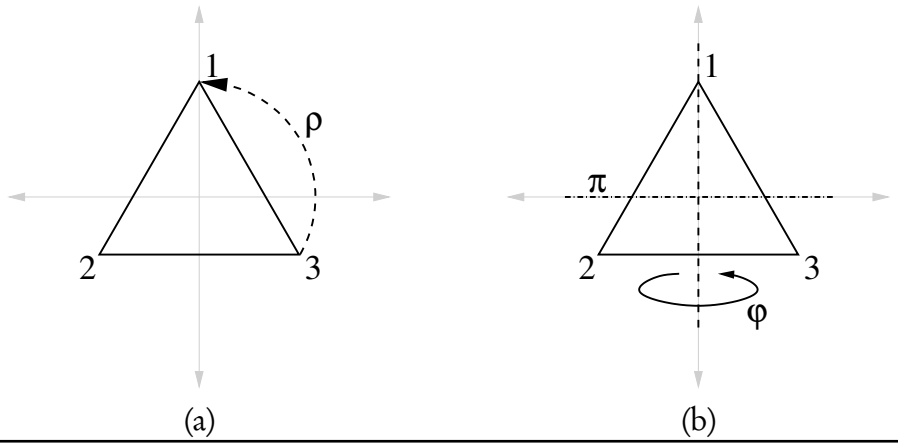


Figure 2.1. Rotation and reflection of the triangle

2. Not all of the functions identitifed by question (1) map points on the triangle back onto the triangle; for example a 45° degree rotation does not. Which ones do?

Lemma 2.38 answers the first question.

Lemma 2.38: *Let $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$. If*

- *α does not move the origin; that is, $\alpha(0,0) = (0,0)$, and*
- *the distance between $\alpha(P)$ and $\alpha(R)$ is the same as the distance between P and R for every $P, R \in \mathbb{R}^2$,*

then α has one of the following two forms:

$$\rho = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \quad \exists t \in \mathbb{R}$$

or

$$\varphi = \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix} \quad \exists t \in \mathbb{R}.$$

The two values of t may be different.

(You might wonder why we assume that the origin doesn't move. Basically, this makes life easier. If it bothers you, try to see if you can prove that the origin *must* remain in the same place under the action of a function α that preserves both distance and a figure centered at the origin. Then see if you can prove it when the figure is not centered at the origin.)

PROOF: Assume that $\alpha(0,0) = (0,0)$ and for every $P, R \in \mathbb{R}^2$ the distance between $\alpha(P)$ and $\alpha(R)$ is the same as the distance between P and R. We can determine α precisely merely from how it acts on two points in the plane!

First, let $P = (1,0)$. Write $\alpha(P) = Q = (q_1, q_2)$; this is the point where α moves Q. The distance between P and the origin is 1. Since $\alpha(0,0) = (0,0)$, the distance between Q and the

origin is $\sqrt{q_1^2+q_2^2}$. Because α preserves distance,

$$1=\sqrt{q_1^2+q_2^2},$$

or

$$q_1^2+q_2^2=1.$$

The only values for Q that satisfy this equation are those points that lie on the circle whose center is the origin. Any point on this circle can be parametrized as

$$(\cos t,\sin t)$$

where $t\in\mathbb{R}$ represents an angle. Hence, $\alpha(P)=(\cos t,\sin t)$.

Let $R=(0,1)$. Write $\alpha(R)=S=(s_1,s_2)$. An argument similar to the one above shows that S also lies on the circle whose center is the origin. Moreover, the distance between P and R is $\sqrt{2}$, so the distance between Q and S is also $\sqrt{2}$. That is,

$$\sqrt{(\cos t-s_1)^2+(\sin t-s_2)^2}=\sqrt{2},$$

or

$$(\cos t-s_1)^2+(\sin t-s_2)^2=2. \tag{1}$$

We can simplify (1) to obtain

$$-2(s_1\cos t+s_2\sin t)+\left(s_1^2+s_2^2\right)=1. \tag{2}$$

To solve this, recall that the distance from S to the origin must be the same as the distance from R to the origin, which is 1. Hence

$$\begin{aligned}\sqrt{s_1^2+s_2^2}&=1\\ s_1^2+s_2^2&=1.\end{aligned}$$

Substituting this into (2), we find that

$$\begin{aligned}-2(s_1\cos t+s_2\sin t)+s_1^2+s_2^2&=1\\ -2(s_1\cos t+s_2\sin t)+1&=1\\ -2(s_1\cos t+s_2\sin t)&=0\\ s_1\cos t&=-s_2\sin t. \end{aligned}\tag{3}$$

At this point we can see that $s_1=\sin t$ and $s_2=-\cos t$ would solve the problem; so would $s_1=-\sin t$ and $s_2=\cos t$. Are there any other solutions?

Recall that $s_1^2+s_2^2=1$, so $s_2=\pm\sqrt{1-s_1^2}$. Likewise $\sin t=\pm\sqrt{1-\cos^2 t}$. Substituting

into equation (3) and squaring (so as to remove the radicals), we find that

$$\begin{aligned} s_1 \cos t &= -\sqrt{1-s_1^2} \cdot \sqrt{1-\cos^2 t} \\ s_1^2 \cos^2 t &= \left(1-s_1^2\right)\left(1-\cos^2 t\right) \\ s_1^2 \cos^2 t &= 1-\cos^2 t - s_1^2 + s_1^2 \cos^2 t \\ s_1^2 &= 1-\cos^2 t \\ s_1^2 &= \sin^2 t \\ \therefore s_1 &= \pm \sin t . \end{aligned}$$

Along with equation (3), this implies that $s_2 = \mp \cos t$. Thus there are *two* possible values of s_1 and s_2.

It can be shown (see Exercise 2.45) that α is a linear transformation on the vector space $\mathbb{R}^2$ with the basis $\left\{\vec{P}, \vec{R}\right\} = \{(1,0),(0,1)\}$. Linear algebra tells us that we can describe any linear transformation as a matrix. If $s = (\sin t, -\cos t)$ then

$$\alpha = \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix};$$

otherwise

$$\alpha = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}.$$

The lemma names the first of these forms φ and the second ρ. □

Before answering the second question, let's consider an example of what the two basic forms of α do to the points in the plane.

Example 2.39: Consider the set of points $\mathcal{S} = \{(0,2),(\pm 2,1),(\pm 1,-2)\}$; these form the vertices of a (non-regular) pentagon in the plane. Let $t = \pi/4$; then

$$\rho = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \quad \text{and} \quad \varphi = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix}.$$

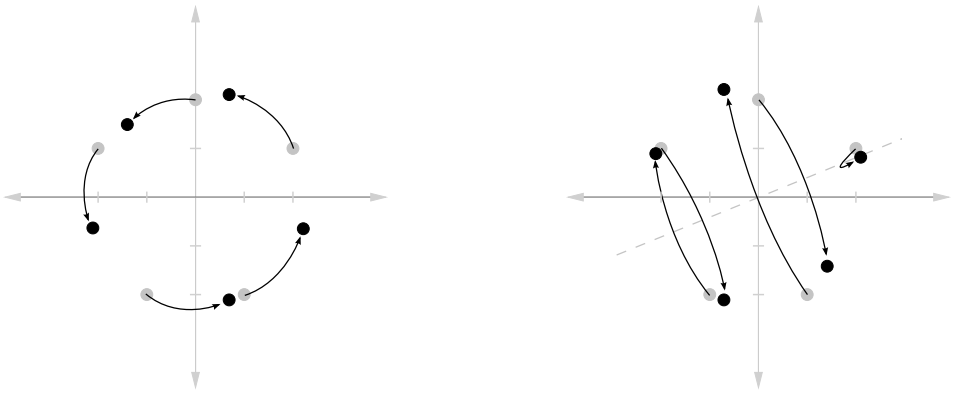


Figure 2.2. Actions of ρ and φ on a pentagon, with $t = \pi/4$

If we apply ρ to every point in the plane, then the points of $\mathcal{S}$ move to

$$\begin{aligned}
\rho(\mathcal{S}) &= \{\rho(0,2), \rho(-2,1), \rho(2,1), \rho(-1,-2), \rho(1,-2)\} \\
&= \left\{ \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} -2 \\ 1 \end{pmatrix}, \right. \\
&\qquad \left. \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} -1 \\ -2 \end{pmatrix}, \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right\} \\
&= \left\{ \left(-\sqrt{2}, \sqrt{2}\right), \left(-\sqrt{2} - \frac{\sqrt{2}}{2}, -\sqrt{2} + \frac{\sqrt{2}}{2}\right), \right. \\
&\qquad \left. \left(\sqrt{2} - \frac{\sqrt{2}}{2}, \sqrt{2} + \frac{\sqrt{2}}{2}\right), \left(-\frac{\sqrt{2}}{2} + \sqrt{2}, -\frac{\sqrt{2}}{2} - \sqrt{2}\right), \left(\frac{\sqrt{2}}{2} + \sqrt{2}, \frac{\sqrt{2}}{2} - \sqrt{2}\right) \right\} \\
&\approx \{(-1.4, 1.4), (-2.1, -0.7), (0.7, 2.1), (0.7, -2.1), (2.1, -0.7)\}.
\end{aligned}$$

This is a 45° ($\pi/4$) counterclockwise rotation in the plane.

If we apply φ to every point in the plane, then the points of $\mathcal{S}$ move to

$$\begin{aligned}
\varphi(\mathcal{S}) &= \{\varphi(0,2), \varphi(-2,1), \varphi(2,1), \varphi(-1,-2), \varphi(1,-2)\} \\
&\approx \{(1.4, -1.4), (-0.7, -2.1), (2.1, 0.7), (-2.1, 0.7), (-0.7, 2.1)\}.
\end{aligned}$$

This is shown in Figure 2.2 . The line of reflection for φ has slope $\left(1 - \cos\frac{\pi}{4}\right) / \sin\frac{\pi}{4}$. (You will show this in Exercise 2.47) ◿

The second questions asks which of the matrices described by Lemma 2.38 also preserve the triangle.

- The first solution (ρ) corresponds to a rotation of degree t of the plane. To preserve the triangle, we can only have $t = 0, 2\pi/3, 4\pi/3$ (0°, 120°, 240°). (See Figure 2.1(a).) Let ι

correspond to $t = 0$, the identity rotation; notice that

$$\iota = \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which is what we would expect for the identity. We can let ρ correspond to a counter-clockwise rotation of 120°, so

$$\rho = \begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

A rotation of 240° is the same as rotating 120° twice. We can write that as $\rho \circ \rho$ or ρ^2; matrix multiplication gives us

$$\rho^2 = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

- The second solution (φ) corresponds to a flip along the line whose slope is

$$m = (1 - \cos t) \,/\, \sin t.$$

One way to do this would be to flip across the y-axis (see Figure 2.1(b)). For this we need the slope to be undefined, so the denominator needs to be zero and the numerator needs to be non-zero. One possibility for t is $t = \pi$ (but not $t = 0$). So

$$\varphi = \begin{pmatrix} \cos\pi & \sin\pi \\ \sin\pi & -\cos\pi \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

There are two other flips, but we can actually ignore them, because they are combinations of φ and ρ. (Why? See Exercise 2.44.)

Let $D_3 = \{\iota, \varphi, \rho, \rho^2, \rho\varphi, \rho^2\varphi\}$. In the exercises, you will explain why D_3 is a group. To do that, it is helpful to observe two important properties.

Corollary 2.40: *In D_3, $\varphi\rho = \rho^2\varphi$.*

PROOF: Compare

$$\varphi\rho = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

and

$$\begin{aligned}\rho^2\varphi &= \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}\begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.\end{aligned}$$

□

Did you notice something interesting about Corollary 2.40? It implies that multiplication in D_3 is non-commutative! We have $\varphi\rho = \rho^2\varphi$, and a little logic (or an explicit computation) shows that $\rho^2\varphi \neq \rho\varphi$: thus $\varphi\rho \neq \rho\varphi$.

Corollary 2.41: *In D_3, $\rho^3 = \varphi^2 = \iota$.*

PROOF: You do it! See Exercise 2.42. □

Exercises.

Exercise 2.42: Show explicitly (by matrix multiplication) that in D_3, $\rho^3 = \varphi^2 = \iota$.

Exercise 2.43: The multiplication table for D_3 has at least this structure:

$\circ$	ι	φ	ρ	ρ^2	$\rho\varphi$	$\rho^2\varphi$
ι	ι	φ	ρ	ρ^2	$\rho\varphi$	$\rho^2\varphi$
φ	φ		$\rho^2\varphi$			
ρ	ρ	$\rho\varphi$				
ρ^2	ρ^2					
$\rho\varphi$	$\rho\varphi$					
$\rho^2\varphi$	$\rho^2\varphi$					

Complete the multiplication table, writing every element in the form $\rho^m\varphi^n$, never with φ before ρ. Explain how D_3 satisfies the properties of a group. Rather than using matrix multiplication, use the result of Exercise 2.42.

Exercise 2.44: Two other values of t allow us to define flips. Find these values of t, and explain why their matrices are equivalent to the matrices $\rho\varphi$ and $\rho^2\varphi$.

Exercise 2.45: Show that any function α satisfying the requirements of Theorem 2.38 is a linear transformation; that is, for all $P, Q \in \mathbb{R}^2$ and for all $a, b \in \mathbb{R}$, $\alpha(aP + bQ) = a\alpha(P) + b\alpha(Q)$. Use the following steps.

(a) Prove that $\alpha(P)\cdot\alpha(Q) = P\cdot Q$, where $\cdot$ denotes the usual dot product (or inner product) on $\mathbb{R}^2$.
(b) Show that $\alpha(1,0)\cdot\alpha(0,1) = 0$.
(c) Show that $\alpha((a,0)+(0,b)) = a\alpha(1,0)+b\alpha(0,1)$.
(d) Show that $\alpha(aP) = a\alpha(P)$.
(e) Show that $\alpha(P+Q) = \alpha(P)+\alpha(Q)$.

Exercise 2.46: Show that the only point in $\mathbb{R}^2$ left stationary by ρ is the origin. That is, if $\rho(P) = P$, then $P = (0,0)$.

Exercise 2.47: Show that the only points in $\mathbb{R}^2$ left stationary by φ lie along the line whose slope is $(1-\cos t)/\sin t$.

2.3: Cyclic groups and order

Here we re-introduce the familiar notation of exponents, in a manner consistent with what you learned of exponents for real numbers. We use this to describe an important class of groups that are recur frequently, at least indirectly.

Notation 2.48: Let G be a group, and $g \in G$. If we want to perform the operation on g ten times, we could write

$$\prod_{i=1}^{10} g = g\cdot g\cdot g\cdot g\cdot g\cdot g\cdot g\cdot g\cdot g\cdot g$$

but this grows tiresome. Instead we will adapt notation from high-school algebra and write

$$g^{10}.$$

We likewise define g^{-10} to represent

$$\prod_{i=1}^{10} g^{-1} = g^{-1}\cdot g^{-1}\cdot g^{-1}\cdot g^{-1}\cdot g^{-1}\cdot g^{-1}\cdot g^{-1}\cdot g^{-1}\cdot g^{-1}\cdot g^{-1}.$$

Indeed, for any $n \in \mathbb{N}^+$ and any $g \in G$ we adopt the following convention:

- g^n means to perform the operation on n copies of g, so $g^n = \prod_{i=1}^{n} g$;
- g^{-n} means to perform the operation on n copies of g^{-1}, so $g^{-n} = \prod_{i=1}^{n} g^{-1} = (g^{-1})^n$;
- $g^0 = e$, and if I want to be annoying I can write $g^0 = \prod_{i=1}^{0} g$.

In additive groups we write instead $ng = \sum_{i=1}^{n} g$, $(-n)g = \sum_{i=1}^{n}(-g)$, and $0g = 0$.

Notice that this definition assume n is *positive*.

Definition 2.49: Let G be a group. If there exists $g \in G$ such that every element $x \in G$ has the form $x = g^n$ for some $n \in \mathbb{Z}$, then G is a **cyclic group** and we write $G = \langle g\rangle$. We call g a **generator** of G.

The idea of a cyclic group is that it has the form $\{\ldots, g^{-2}, g^{-1}, e, g^1, g^2, \ldots\}$. If the group is additive, we would of course write $\{\ldots, -2g, -g, 0, g, 2g, \ldots\}$.

Example 2.50: $\mathbb{Z}$ is cyclic, since any $n \in \mathbb{Z}$ has the form $n \cdot 1$. Thus $\mathbb{Z} = \langle 1 \rangle$. In addition, n has the form $(-n) \cdot (-1)$, so $\mathbb{Z} = \langle -1 \rangle$ as well. Both 1 and -1 are generators of $\mathbb{Z}$.

You will show in the exercises that $\mathbb{Q}$ is not cyclic. ◿

In Definition 2.49 we referred to g as *a* generator of G, not as *the* generator. There could in fact be more than one generator; we see this in Example 2.50 from the fact that $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Here is another example.

Example 2.51: Let

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \subsetneq \mathrm{GL}_m(\mathbb{R}).$$

It turns out that G is a group; both the second and third matrices generate it. For example,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \text{◿}$$

An important question arises here. Given a group G and an element $g \in G$, define

$$\langle g \rangle = \left\{ \ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots \right\}.$$

We know that every cyclic group has the form $\langle g \rangle$ for some $g \in G$. Is the converse also true that $\langle g \rangle$ is a group for any $g \in G$? As a matter of fact, yes!

Theorem 2.52: *For every group G and for every $g \in G$, $\langle g \rangle$ is an abelian group.*

To prove Theorem 2.52, we need to make sure we can perform the usual arithmetic on exponents.

Lemma 2.53: *Let G be a group, $g \in G$, and $m, n \in \mathbb{Z}$. Each of the following holds:*
(A) $g^m g^{-m} = e$; *that is,* $g^{-m} = (g^m)^{-1}$.
(B) $(g^m)^n = g^{mn}$.
(C) $g^m g^n = g^{m+n}$.

The proof will justify this argument by applying the notation described at the beginning of this chapter. We have to be careful with this approach, because in the lemma we have $m, n \in \mathbb{Z}$, but

the notation was given under the assumption that $n \in \mathbb{N}^+$. To make this work, we'll have to consider the cases where m and n are positive or negative separately. We call this a *case analysis*.

PROOF: Each claim follows by case analysis.

(A) If $m = 0$, then $g^{-m} = g^0 = e = e^{-1} = (g^0)^{-1} = (g^m)^{-1}$.
Otherwise, $m \neq 0$. First assume that $m \in \mathbb{N}^+$. By notation, $g^{-m} = \prod_{i=1}^{m} g^{-1}$. Hence

$$\begin{aligned} g^m g^{-m} &\underset{\text{def.}}{=} \left(\prod_{i=1}^{m} g\right)\left(\prod_{i=1}^{m} g^{-1}\right) \\ &\underset{\text{ass.}}{=} \left(\prod_{i=1}^{m-1} g\right)\left(g \cdot g^{-1}\right)\left(\prod_{i=1}^{m-1} g^{-1}\right) \\ &\underset{\text{id.}}{=} \left(\prod_{i=1}^{m-1} g\right) e \left(\prod_{i=1}^{m-1} g^{-1}\right) \\ &\underset{\text{inv.}}{=} \left(\prod_{i=1}^{m-1} g\right)\left(\prod_{i=1}^{m-1} g^{-1}\right) \\ &\;\;\vdots \\ &= e. \end{aligned}$$

Since the inverse of an element is unique, $g^{-m} = (g^m)^{-1}$.
Now assume that $m \in \mathbb{Z}\backslash\mathbb{N}$. Since m is negative, we cannot express the product using m; the notation discussed on page 40 requires a *positive* exponent. Consider instead $\widehat{m} = |m| \in \mathbb{N}^+$. Since the oppositve of a negative number is positive, we can write $-m = \widehat{m}$ and $-\widehat{m} = m$. Since $\widehat{m}$ is positive, we can apply the notation to it directly; $g^{-m} = g^{\widehat{m}} = \prod_{i=1}^{\widehat{m}} g$, while $g^m = g^{-\widehat{m}} = \prod_{i=1}^{\widehat{m}} g^{-1}$. (To see this in a more concrete example, try it with an actual number. If $m = -5$, then $\widehat{m} = |-5| = 5 = -(-5)$, so $g^m = g^{-5} = g^{-\widehat{m}}$ and $g^{-m} = g^5 = g^{\widehat{m}}$.) As above, we have

$$g^m g^{-m} \underset{\text{subs.}}{=} g^{-\widehat{m}} g^{\widehat{m}} \underset{\text{not.}}{=} \left(\prod_{i=1}^{\widehat{m}} g^{-1}\right)\left(\prod_{i=1}^{\widehat{m}} g\right) = e.$$

Hence $g^{-m} = (g^m)^{-1}$.

(B) If $n = 0$, then $(g^m)^n = (g^m)^0 = e$ because *anything* to the zero power is e. Assume first that $n \in \mathbb{N}^+$. By notation, $(g^m)^n = \prod_{i=1}^{n} g^m$. We split this into two subcases.

(B1) If $m \in \mathbb{N}$, we have

$$(g^m)^n \underset{\text{not.}}{=} \prod_{i=1}^{n}\left(\prod_{i=1}^{m} g\right) \underset{\text{ass.}}{=} \prod_{i=1}^{mn} g \underset{\text{not.}}{=} g^{mn}.$$

(B2) Otherwise, let $\widehat{m} = |m| \in \mathbb{N}^+$ and we have

$$(g^m)^n \underset{\text{subs.}}{=} \left(g^{-\widehat{m}}\right)^n \underset{\text{not.}}{=} \prod_{i=1}^{n} \left(\prod_{i=1}^{\widehat{m}} g^{-1} \right) \underset{\text{ass.}}{=} \prod_{i=1}^{\widehat{m}n} g^{-1} \underset{\text{not.}}{=} \left(g^{-1}\right)^{\widehat{m}n} \underset{\text{not.}}{=} g^{-\widehat{m}n} \underset{\text{subs.}}{=} g^{mn}.$$

What if n is negative? Let $\widehat{n} = -n$; by notation, $(g^m)^n = (g^m)^{-\widehat{n}} = \prod_{i=1}^{\widehat{n}} (g^m)^{-1}$. By (A), this becomes $\prod_{i=1}^{\widehat{n}} g^{-m}$. By notation, we can rewrite this as $\left(g^{-m}\right)^{\widehat{n}}$. Since $\widehat{n} \in \mathbb{N}^+$, we can apply case (B1) or (B2) as appropriate, so

$$(g^m)^n = \left(g^{-m}\right)^{\widehat{n}} \underset{\text{(B1) or (B2)}}{=} g^{(-m)\widehat{n}} \underset{\text{integers!}}{=} g^{m(-\widehat{n})} \underset{\text{subst}}{=} g^{mn}.$$

(C) We consider three cases.
If $m = 0$ or $n = 0$, then $g^0 = e$, so $g^{-0} = g^0 = e$.
If m, n have the same sign (that is, $m, n \in \mathbb{N}^+$ or $m, n \in \mathbb{Z}\backslash\mathbb{N}$), then write $\widehat{m} = |m|$, $\widehat{n} = |n|$, $g_m = g^{\frac{\widehat{m}}{m}}$, and $g_n = g^{\frac{\widehat{n}}{n}}$. This effects a really nice trick: if $m \in \mathbb{N}^+$, then $g_m = g$, whereas if m is negative, $g_m = g^{-1}$. This notational trick allows us to write $g^m = \prod_{i=1}^{\widehat{m}} g_m$ and $g^n = \prod_{i=1}^{\widehat{n}} g_n$, where $g_m = g_n$ and $\widehat{m}$ and $\widehat{n}$ are both positive integers. Then

$$g^m g^n = \prod_{i=1}^{\widehat{m}} g_m \prod_{i=1}^{\widehat{n}} g_n = \prod_{i=1}^{\widehat{m}} g_m \prod_{i=1}^{\widehat{n}} g_m = \prod_{i=1}^{\widehat{m}+\widehat{n}} g_m = (g_m)^{\widehat{m}+\widehat{n}} = g^{m+n}.$$

Since g and n were arbitrary, the induction implies that $g^n g^{-n} = e$ for all $g \in G$, $n \in \mathbb{N}^+$.
Now consider the case where m and n have different signs. In the first case, suppose m is negative and $n \in \mathbb{N}^+$. As in (A), let $\widehat{m} = |m| \in \mathbb{N}^+$; then

$$g^m g^n = \left(g^{-1}\right)^{-m} g^n = \left(\prod_{i=1}^{\widehat{m}} g^{-1} \right) \left(\prod_{i=1}^{n} g \right).$$

If $\widehat{m} \geq n$, we have more copies of g^{-1} than g, so after cancellation,

$$g^m g^n = \prod_{i=1}^{\widehat{m}-n} g^{-1} = g^{-(\widehat{m}-n)} = g^{m+n}.$$

Otherwise, $\widehat{m} < n$, and we have more copies of g than of g^{-1}. After cancellation,

$$g^m g^n = \prod_{i=1}^{n-\widehat{m}} g = g^{n-\widehat{m}} = g^{n+m} = g^{m+n}.$$

The remaining case ($m \in \mathbb{N}^+$, $n \in \mathbb{Z}\backslash\mathbb{N}$) is similar, and you will prove it for homework.

□

These properties of exponent arithmetic allow us to show that $\langle g \rangle$ is a group.

PROOF OF THEOREM 2.52: We show that $\langle g \rangle$ satisfies the properties of an abelian group. Let $x, y, z \in \langle g \rangle$. By definition of $\langle g \rangle$, there exist $a, b, c \in \mathbb{Z}$ such that $x = g^a$, $y = g^b$, and $z = g^c$.

- By substitution, $xy = g^a g^b$. By Lemma 2.53, $xy = g^a g^b = g^{a+b} \in \langle g \rangle$. So $\langle g \rangle$ is closed.
- By substitution, $x(yz) = g^a \left(g^b g^c\right)$. These are elements of G by inclusion (that is, $\langle g \rangle \subseteq G$ so $x, y, z \in G$), so the associative property *in* G gives us

$$x(yz) = g^a \left(g^b g^c\right) = \left(g^a g^b\right) g^c = (xy) z.$$

- By definition, $e = g^0 \in \langle g \rangle$.
- By definition, $g^{-a} \in \langle g \rangle$, and by Lemma 2.53 $x \cdot g^{-a} = g^a g^{-a} = e$. Hence $x^{-1} = g^{-a} \in \langle g \rangle$.
- Using Lemma 2.53 with the fact that $\mathbb{Z}$ is commutative under addition,

$$xy = g^a g^b = g^{a+b} = g^{b+a} = g^b g^a = yx.$$

□

Given an element and an operation, Theorem 2.52 links them to a group. It makes sense, therefore, to link an element to the order of the group that it generates.

Definition 2.54: Let G be a group, and $g \in G$. We say that the **order** of g is $\text{ord}(g) = |\langle g \rangle|$. If $\text{ord}(g) = \infty$, we say that g has **infinite order**.

If the order of a group is finite, then we can write an element in different ways.

Example 2.55: Recall Example 2.51; we can write

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^8 = \cdots.$$

Since multiples of 4 give the identity, let's take any power of the matrix, and divide it by 4. The Division Theorem allows us to write any power of the matrix as $4q + r$, where $0 \leq r < 4$. Since there are only four possible remainders, and multiples of 4 give the identity, positive powers of

this matrix can generate only four possible matrices:

$$\begin{aligned}
\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{4q} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{4q+1} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\
\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{4q+2} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \\
\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{4q+3} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.
\end{aligned}$$

We can do the same with negative powers; the Division Theorem still gives us only four possible remainders. Let's write

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Thus

$$\langle g \rangle = \left\{ I_2, g, g^2, g^3 \right\}. \triangle$$

The example suggests that if the order of an element G is $n \in \mathbb{N}$, then we can write

$$\langle g \rangle = \left\{ e, g, g^2, \ldots, g^{n-1} \right\}.$$

This explains why we call $\langle g \rangle$ a *cyclic* group: once they reach $\text{ord}(g)$, the powers of g "cycle".To prove this in general, we have to show that for a generic cyclic group $\langle g \rangle$ with $\text{ord}(g) = n$,

- n is the smallest positive power that gives us the identity; that is, $g^n = e$, and
- for any two integers between 0 and n, the powers of g are different; that is, if $0 \leq a < b < n$, then $g^a \neq g^b$.

Theorem 2.56 accomplishes that, and a bit more as well.

Theorem 2.56: *Let G be a group, $g \in G$, and $\text{ord}(g) = n$. Then*
(A) for all $a, b \in \mathbb{N}$ such that $0 \leq a < b < n$, we have $g^a \neq g^b$.
In addition, if $n < \infty$, each of the following holds:
(B) $g^n = e$;
(C) n is the smallest positive integer d such that $g^d = e$; and
(D) if $a, b \in \mathbb{Z}$ and $n \mid (a - b)$, then $g^a = g^b$.

PROOF: The fundamental assertion of the theorem is (A). The remaining assertions turn out to be corollaries.

(A) By way of contradiction, suppose that there exist $a, b \in \mathbb{N}$ such that $0 \leq a < b < n$ and $g^a = g^b$; then $e = (g^a)^{-1} g^b$. By Exercise 2.59, we can write

$$e = g^{-a} g^b = g^{-a+b} = g^{b-a}.$$

Let $S = \{m \in \mathbb{N}^+ : g^m = e\}$. By the well-ordering property of $\mathbb{N}$, there exists a smallest element of S; call it d. Recall that $a < b$, so $b - a \in \mathbb{N}^+$, so $g^{b-a} \in S$. By the choice of d, we know that $d \leq b - a$. By Exercise 1.25, $d \leq b - a < b$, so $0 < d < b < n$.
We can now list d distinct elements of $\langle g \rangle$:

$$g, g^2, g^3, \ldots, g^d = e. \tag{4}$$

Since $d < n$, this list omits $n - d$ elements of $\langle g \rangle$. (If $\operatorname{ord}(g) = \infty$, then it omits infinitely many elements of $\langle g \rangle$.) Let x be one such element. By definition of $\langle g \rangle$, we can write $x = g^c$ for some $c \in \mathbb{Z}$. Choose q, r that satisfy the Division Theorem for division of c by d; that is,

$$c = qd + r \quad \text{such that} \quad q, d \in \mathbb{Z} \text{ and } 0 \leq r < d.$$

We have $g^c = g^{qd+r}$. By Lemma 2.53,

$$g^c = \left(g^d\right)^q \cdot g^r = e^q \cdot g^r = e \cdot g^r = g^r.$$

Recall that $0 \leq r < d$, so we listed g^r above when we listed the powers of g less than d. Since $g^r = g^c$, we have already listed g^c. This contradicts the assumption that $g^c = g^r$ was not listed. Hence if $0 \leq a < b < n$, then $g^a \neq g^b$.

For the remainder of the proof, we assume that $n < \infty$.

(B) Let $S = \{m \in \mathbb{N}^+ : g^m = e\}$. Is S non-empty? Since $\langle g \rangle < \infty$, there must exist $a, b \in \mathbb{N}^+$ such that $a < b$ and $g^a = g^b$. Using the inverse property and substitution, $g^0 = e = g^b (g^a)^{-1}$. By Lemma 2.53, $g^0 = g^{b-a}$. By definition, $b - a \in \mathbb{N}^+$. Hence S is non-empty.

By the well-ordering property of $\mathbb{N}$, there exists a smallest element of S; call it d. Since $\langle g \rangle$ contains n elements, $1 < d \leq n$. If $d < n$, that would contradict assertion (A) of this theorem (with $a = 0$ and $b = d$). Hence $d = n$, and $g^n = e$, and we have shown (A).

(C) In (B), S is the set of all positive integers m such that $g^m = e$; we let the smallest element be d, and we found that $d = n$.

(D) Let $a, b \in \mathbb{Z}$. Assume that $n \mid (a - b)$. Let $q \in \mathbb{Z}$ such that $nq = a - b$. Then

$$g^b = g^b \cdot e = g^b \cdot e^q = g^b \cdot \left(g^d\right)^q = g^b \cdot g^{dq} = g^b \cdot g^{a-b} = g^{b+(a-b)} = g^a.$$

□

We conclude therefore that, at least when they are finite, cyclic groups are aptly named: increasing powers of g generate new elements until the power reaches n, in which case $g^n = e$ and we "cycle around".

Exercises.

Exercise 2.57: Recall from Example 2.51 the matrix

$$A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

Express A as a power of the other non-identity matrices of the group.

Exercise 2.58: In Exercise 2.35 you showed that the quaternions form a group under matrix multiplication. Verify that $H = \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}\}$ is a cyclic group. What elements generate H?

Exercise 2.59: Complete the proof of Lemma 2.53(C).

Exercise 2.60: Let G be a group, and $g \in G$. Let $d, n \in \mathbb{Z}$ and assume $\text{ord}(g) = d$. Show that $g^n = e$ if and only if $d \mid n$.

Exercise 2.61: Show that any group of 3 elements is cyclic.

Exercise 2.62: Is the Klein 4-group (Exercise 2.31 on page 32) cyclic? What about the cyclic group of order 4?

Exercise 2.63: Show that Q_8 is not cyclic.

Exercise 2.64: Show that $\mathbb{Q}$ is not cyclic.

Exercise 2.65: Use a fact from linear algebra to explain why $\text{GL}_m(\mathbb{R})$ is not cyclic.

2.4: The roots of unity

One of the major motivations in the development of group theory was to give a structure that would help study the roots of polynomials. A polynomial, of course, has the form

$$ax + b, \quad ax^2 + bx + c, \quad ax^3 + bx^2 + cx + d, \quad \ldots$$

A **root** of a polynomial $f(x)$ is any a such that $f(a) = 0$. For example, if $f(x) = x^4 - 1$, then 1, -1, i, and $-i$ are all roots of f. In fact, they are the *only* roots of f! Every root a corresponds to a factor $x - a$ of f; that is, $f(x) = (x+1)(x-1)(x+i)(x-i)$, so we cannot have any other roots; otherwise f would have to have a degree higher than 4. This fact is usually discussed in precalculus algebra; if you have not seen it, take it on faith for now; we explain why in some detail in Section 7.3.

Any root of the polynomial $f(x) = x^n - 1$ is called a **root of unity**. These are very important in the study of polynomial roots; we are interested in the fact that the set of roots of unity forms a group. To see why, we need to describe them first.

Theorem 2.66: *Let $n \in \mathbb{N}^+$. The complex number*

$$\alpha = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right).$$

is a root of $f(x) = x^n - 1$.

To prove this, we need a different property of α.

Lemma 2.67: *If α is defined as in Theorem 2.66, then*

$$\alpha^m = \cos\left(\frac{2\pi m}{n}\right) + i\sin\left(\frac{2\pi m}{n}\right)$$

for every $m \in \mathbb{N}^+$.

PROOF: We proceed by induction on m. For the *inductive base*, it is clear by definition of α that α^1 has the desired form. For the *inductive hypothesis*, assume that α^m has the desired form; in the *inductive step*, we need to show that

$$\alpha^{m+1} = \cos\left(\frac{2\pi(m+1)}{n}\right) + i\sin\left(\frac{2\pi(m+1)}{n}\right).$$

To see why this is true, use the trigonometric sum identities $\cos(A+B) = \cos A\cos B - \sin A\sin B$ and $\sin(A+B) = \sin A\cos B + \sin B\cos A$ to rewrite α^{m+1}, like so:

$$\begin{aligned}
\alpha^{m+1} &= \alpha^m \cdot \alpha \\
&\underset{\text{hyp.}}{\underset{\text{ind.}}{=}} \left[\cos\left(\frac{2\pi m}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right]\left[\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right] \\
&= \cos\left(\frac{2\pi m}{n}\right)\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\cos\left(\frac{2\pi m}{n}\right) \\
&\quad + i\sin\left(\frac{2\pi m}{n}\right)\cos\left(\frac{2\pi}{n}\right) - \sin\left(\frac{2\pi m}{n}\right)\sin\left(\frac{2\pi}{n}\right) \\
&= \left[\cos\left(\frac{2\pi m}{n}\right)\cos\left(\frac{2\pi}{n}\right) - \sin\left(\frac{2\pi m}{n}\right)\sin\left(\frac{2\pi}{n}\right)\right] \\
&\quad + i\left[\sin\left(\frac{2\pi}{n}\right)\cos\left(\frac{2\pi m}{n}\right) + \sin\left(\frac{2\pi m}{n}\right)\cos\left(\frac{2\pi}{n}\right)\right] \\
&= \cos\left(\frac{2\pi(m+1)}{n}\right) + i\sin\left(\frac{2\pi(m+1)}{n}\right).
\end{aligned}$$

□

Once we have Lemma 2.67, proving Theorem 2.66 is spectacularly easy.

PROOF OF THEOREM ??: Substitution and the lemma give us

$$\alpha^n - 1 = \left[\cos\left(\frac{2\pi n}{n}\right) + i\sin\left(\frac{2\pi n}{n}\right)\right] - 1 = (1 + i\cdot 0) - 1 = 0,$$

so α is indeed a root of $x^n - 1$. □

Theorem 2.68: *The nth roots of unity are* $\Omega_n = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, *where* α *is defined as in Theorem 2.66. They form a cyclic group of order n under multiplication.*

PROOF: For $m \in \mathbb{N}^+$, we use the fact that the complex numbers are commutative under multiplication:

$$(\alpha^m)^n - 1 = \alpha^{mn} - 1 = \alpha^{nm} - 1 = (\alpha^n)^m - 1 = 1^m - 1 = 0.$$

Hence α^m is a root of unity for any $m \in \mathbb{N}^+$; they are distinct for $m = 0, \ldots, n-1$ because the real and imaginary parts do not agree (think of a circle, and see Figure). Since there can be only n distinct roots, Ω_n is a complete list of nth roots of unity.

We only sketch the proof that Ω_n is a cyclic group.

(closure) Let $x, y \in \Omega_n$; you will show in Exercise 2.70 that $xy \in \Omega_n$.

(associativity) The complex numbers are associative under multiplication; since $\Omega_n \subsetneq \mathbb{C}$, the elements of Ω_n are also associative under multiplication.

(identity) The multiplicative identity $1 \in \Omega_n$ since $1^n = 1$ for all $n \in \mathbb{N}^+$.

(inverses) Let $x \in \Omega_n$; you will show in Exercise 2.71 that $x^{-1} \in \Omega_n$.

(cyclic) Theorem 2.66 tells us that $\alpha \in \Omega_n$; the remaining elements are powers of α. Hence $\Omega_n = \langle \alpha \rangle$.

□

You might be wondering whether α is the only generator of Ω_n; in fact, it is not. We are not yet ready to give a precise criterion that signals which elements generate Ω_n, but they do have a special name.

Definition 2.69: We call any generator of Ω_n a **primitive nth root of unity**.

Exercises.

Exercise 2.70: Suppose that a and b are both nth roots of unity. Show that ab is also an nth root of unity.

Exercise 2.71: Let a be an nth root of unity. Find a number b such that $ab = 1$, and show that b is also an nth root of unity.

Exercise 2.72: Suppose β is a root of $x^n - b$. Show that $\alpha\beta$ is also a root of $x^n - b$, where α is an nth root of unity.

Exercise 2.73: Find the primitive square roots of unity, the primitive cube roots of unity, and the primitive fourth roots of unity.

Exercise 2.74: Plot the eighth roots of unity on an x-y plane, with the root $a+ib$ corresponding to the point (a,b) on the plane. Do you notice anything geometric about these points? If not, try plotting the nth roots of unity for other values of n.

2.5: Elliptic Curves

An excellent example of how groups can appear in places that you might not expect is in *elliptic curves*. These functions have many applications, partly due to an elegant group structure.

Definition 2.75: Let $a,b \in \mathbb{R}$ such that $-4a^3 \neq 27b^2$. We say that $E \subseteq \mathbb{R}^2$ is an **elliptic curve** if

$$E = \left\{(x,y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\right\} \cup \{P_\infty\},$$

where P_∞ denotes a **point at infinity**.

What is meant by a point at infinity? If different branches of a curve extend toward infinity, we imagine that they meet at a point, called the point at infinity.

There are different ways of visualizing a point at infinity. One is to imagine the real plane as if it were wrapped onto a sphere. The scale on the axes changes at a rate inversely proportional to one's distance from the origin; in this way, no finite number of steps bring one to the point on the sphere that lies opposite to the origin. On the other hand, this point would be a limit as x or y approaches $\pm\infty$. Think of the line $y = x$. If you start at the origin, you can travel either northeast or southwest on the line. Any finite distance in either direction takes you short of the point opposite the origin, but the limit of both directions meets at the point opposite the origin. This point is the point at infinity.

Example 2.76: Let

$$E = \left\{(x,y) \in \mathbb{R}^2 : y^2 = x^3 - x\right\} \cup \{P_\infty\}.$$

Here $a = -1$ and $b = 0$. Figure 2.3 gives a diagram of E.

It turns out that E is an additive group. Given $P, Q \in E$, we can define addition by:

- If $P = P_\infty$, then define $P + Q = Q$.
- If $Q = P_\infty$, then define $P + Q = P$.
- If $P, Q \neq P_\infty$, then:
  - If $P = (p_1, p_2)$ and $Q = (p_1, -p_2)$, then define $P + Q = P_\infty$.
  - If $P = Q$, then construct the tangent line ℓ at P. It turns out that ℓ intersects E at another point $S = (s_1, s_2)$ in $\mathbb{R}^2$. Define $P + Q = (s_1, -s_2)$.
  - Otherwise, construct the line ℓ determined by P and Q. It turns out that ℓ intersects E at another point $S = (s_1, s_2)$ in $\mathbb{R}^2$. Define $P + Q = (s_1, -s_2)$.

The last two statements require us to ensure that, given two distinct and finite points $P, Q \in E$, a line connecting them intersects E at a third point S. Figure 2.4 shows the addition of

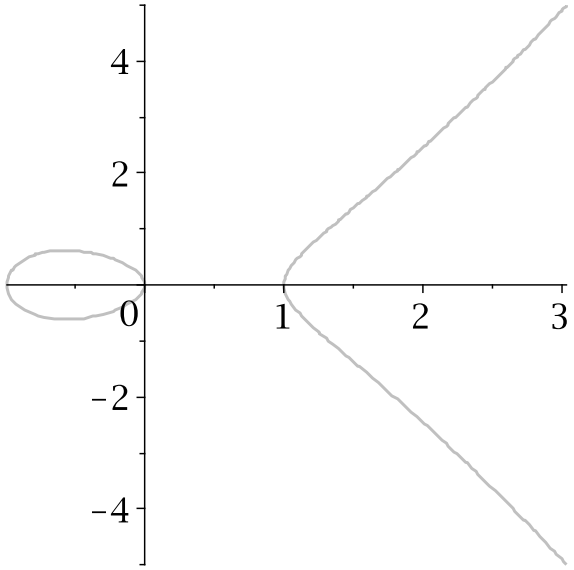


Figure 2.3. A plot of the elliptic curve $y^2 = x^3 - x$.

$P = \left(2, -\sqrt{6}\right)$ and $Q = (0,0)$; the line intersects E at $S = \left(-1/2, \sqrt{6}/4\right)$, so $P + Q = \left(-1/2, -\sqrt{6}/4\right)$. ◿

Exercises

Exercise 2.77: Let E be an arbitrary elliptic curve, defined as the roots of a function $f(x,y) = y^2 - x^3 - ax - b$. Show that $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) \neq (0,0)$ for any point on E.

This shows that E is "smooth", and that tangent lines exist at each point in $\mathbb{R}^2$. (This includes vertical lines, where $\frac{\partial f}{\partial x} = 0$ and $\frac{\partial f}{\partial y} \neq 0$.)

Exercise 2.78: Show that E is an additive group under the addition defined above, with

- P_∞ as the zero element; *and*
- for any $P = (p_1, p_2) \in E$, then $-P = (p_1, -p_2) \in E$.

Exercise 2.79: Choose different values for a and b to generate another elliptic curve. Graph it, and illustrate each kind of addition.

Exercise 2.80: Recall from Section 2.5 the elliptic curve E determined by the equation $y^2 = x^3 - x$.

(a) Compute the cyclic group generated by $(0,0)$ in E.

(b) Verify that $\left(\sqrt{2}+1, \sqrt{2}+2\right)$ is a point on E.

(c) Compute the cyclic group generated by $\left(\sqrt{2}+1, \sqrt{2}+2\right)$ in E.

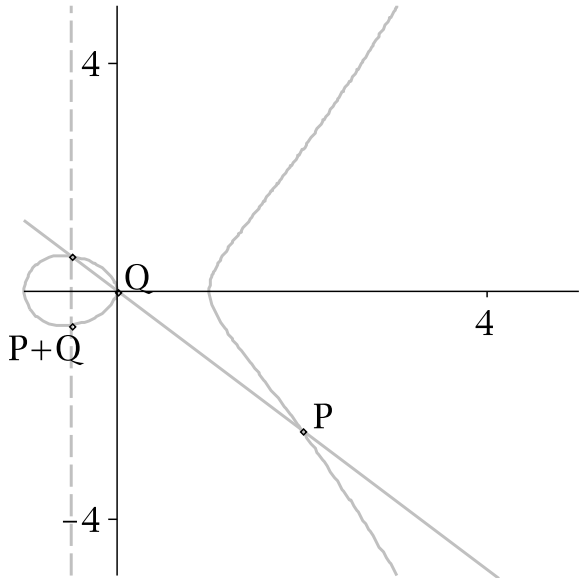


Figure 2.4. Addition on an elliptic curve

Appendix: Basic elliptic curves with Sage

Sage computes elliptic curves of the form

$$y^2 + a_{1,1}xy + a_{0,1}y = x^3 + a_{2,0}x^2 + a_{1,0}x + a_{0,0} \tag{5}$$

using the command

`E = EllipticCurve(AA,[`$a_{1,1}$`,` $a_{2,0}$`,` $a_{0,1}$`,` $a_{1,0}$`,` $a_{0,0}$`]).`[16]

From then on, the symbol `E` represents the elliptic curve. You can refer to points on `E` using the command

`P = E(`a`,` b`,` c`)`

where

- if $c = 0$, then you must have both $a = 0$ and $b = 1$, in which case `P` represents P_∞; but
- if $c = 1$, then substituting $x = a$ and $y = b$ *must* satisfy equation 5.

By this reasoning, you can build the origin using `E(0,0,1)` and the point at infinity using `E(0,1,0)`. You can illustrate the addition shown in Figure 2.4 using the following commands.

```
sage:  E = EllipticCurve(AA,[0,0,0,-1,0])
sage:  P = E(2,-sqrt(6),1)
sage:  Q = E(0,0,1)
sage:  P + Q
(-1/2 :  -0.6123724356957945?  :  1)
```

[16] Here `AA` represents the field $\mathbb{A}$ of algebraic real numbers, which is a fancy way of referring to all real roots of all polynomials with rational coefficients.

This point corresponds to $P + Q$ as shown in Figure 2.4. To see this visually, create the plot using the following sequence of commands.

```
# Create a plot of the curve
sage:  plotE = plot(E, -2, 3)
# Create graphical points for P and Q
sage:  plotP = point((P[0],P[1]))
sage:  plotQ = point((Q[0],Q[1]))
# Create the point R, then a graphical point for R.
sage:  R = P+Q
sage:  plotR = point((R[0],R[1]))
# Compute the slope of the line from P to Q
# and round it to 5 decimal places.
sage:  m = round( (P[1] - Q[1]) / (P[0] - Q[0]) , 5)
# Plot line PQ.
sage:  plotPQ = plot(m*x, -2, 3, rgbcolor=(0.7,0.7,0.7))
# Plot the vertical line from where line PQ intersects E
# to the opposite point, R.
sage:  lineR = line(((R[0],R[1]),(R[0],-R[1])),
                    rgbcolor=(0.7,0.7,0.7))
# Display the entire affair.
sage:  plotE + plotP + plotQ + plotR + plotPQ
```

Chapter 3:
Subgroups

A subset of a group is not necessarily a group; for example, $\{2,4\} \subset \mathbb{Z}$, but $\{2,4\}$ doesn't satisfy any properties of an additive group unless we change the definition of addition. Some subsets of groups are instantly groups, and one of the keys to algebra consists in understanding the relationship between subgroups and groups.

We start this chapter by describing the properties that guarantee that a subset is a "subgroup" of a group (Section 3.1). We then explore how subgroups create *cosets*, equivalence classes within the group that perform a role similar to division of integers (Section 3.2). It turns out that in finite groups, we can count the number of these equivalence classes quite easily (Section 3.3).

Cosets open the door to a special class of groups called *quotient groups*, (Sections 3.4), one of which is a very natural, very useful tool (Section 3.5) that will eventually allow us to devise some "easy" solutions for problems in Number Theory (Chapter 6).

3.1: Subgroups

Definition 3.1: Let G be a group and $H \subseteq G$ be nonempty. If H is also a group under the same operation as G, then H is a **subgroup** of G. If $\{e\} \subsetneq H \subsetneq G$ then H is a **proper subgroup** of G.

Notation 3.2: If H is a subgroup of G, then we write $H < G$.

Example 3.3: Check that the following statements are true by verifying that the properties of a group are satisfied.

(a) $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$.

(b) Let $4\mathbb{Z} := \{4m : m \in \mathbb{Z}\} = \{\ldots, -4, 0, 4, 8, \ldots\}$. Then $4\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

(c) Let $d \in \mathbb{Z}$ and $d\mathbb{Z} := \{dm : m \in \mathbb{Z}\}$. Then $d\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

(d) $\langle \mathbf{i} \rangle$ is a subgroup of Q_8. ◿

Checking all four properties of a group is cumbersome. It would be convenient to verify that a set is a subgroup by checking fewer properties. It also makes sense that if a group is abelian, then its subgroups would be abelian, so we shouldn't have to check the abelian property. So which properties *must* we check to decide whether a subset is a subgroup?

To start with, we can eliminate the associative and abelian properties from consideration. In fact, the operation remains associative and commutative for any subgroup.

Lemma 3.4: *Let G be a group and $H \subseteq G$. Then H satisfies the associative property of a group. In addition, if G is abelian, then H satisfies the commutative property of an abelian group. So, we only need to check the closure, identity, and inverse properties to ensure that G is a group.*

Be careful: Lemma 3.4 neither assumes nor concludes that H is a subgroup. The other three properties may not be satisfied: H may not be closed; it may lack an identity; or some element

may lack an inverse. The lemma merely states that any subset automatically satisfies two important properties of a group.

PROOF: If $H = \emptyset$ then the lemma is true trivially.

Otherwise $H \neq \emptyset$. Let $a, b, c \in H$. Since $H \subseteq G$, we have $a, b, c \in G$. Since the operation is associative in G, $a(bc) = (ab)c$. If G is abelian, then $ab = ba$. □

Lemma 3.4 has reduced the number of requirements for a subgroup from four to three. Amazingly, we can simplify this further, to *only one criterion*.

Theorem 3.5 (The Subgroup Theorem): *Let $H \subseteq G$ be nonempty. The following are equivalent:*
(A) $H < G$;
(B) for every $x, y \in H$, we have $xy^{-1} \in H$.

Notation 3.6: Observe that if G were an additive group, we would write $x - y$ instead of xy^{-1}.

PROOF: By Exercise 2.32 on page 32, (A) implies (B).

Conversely, assume (B). By Lemma 3.4, we need to show only that H satisfies the closure, identity, and inverse properties. We do this slightly out of order:

identity: Let $x \in H$. By (B), $e = x \cdot x^{-1} \in H$.[17]

inverse: Let $x \in H$. Since H satisfies the identity property, $e \in H$. By (B), $x^{-1} = e \cdot x^{-1} \in H$.

closure: Let $x, y \in H$. Since H satisfies the inverse property, $y^{-1} \in H$. By (B), $xy = x \cdot \left(y^{-1}\right)^{-1} \in H$.

Since H satisfies the closure, identity, and inverse properties, $H < G$. □

The Subgroup Theorem makes it much easier to decide whether a subset of a group is a subgroup, because we need to consider only the one criterion given.

Example 3.7: Let $d \in \mathbb{Z}$. We claim that $d\mathbb{Z} < \mathbb{Z}$. (Here $d\mathbb{Z}$ is the set defined in Example 3.3.) *Why?* Let's use the Subgroup Theorem.

Let $x, y \in d\mathbb{Z}$. By definition, $x = dm$ and $y = dn$ for some $m, n \in \mathbb{Z}$. Note that $-y = -(dn) = d(-n)$. Then

$$x - y = x + (-y) = dm + d(-n) = d(m + (-n)) = d(m - n).$$

Now $m - n \in \mathbb{Z}$, so $x - y = d(m - n) \in d\mathbb{Z}$. By the Subgroup Theorem, $d\mathbb{Z} < \mathbb{Z}$. ◿

The following geometric example gives a visual image of what a subgroup "looks" like.

Example 3.8: Let G be the set of points in the x-y plane. Define an addition for elements of G in the following way. For $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, define

$$P_1 + P_2 = (x_1 + x_2, y_1 + y_2).$$

[17] Notice that here we are replacing the y in (B) with x. This is fine, since nothing in (B) requires x and y to be distinct.

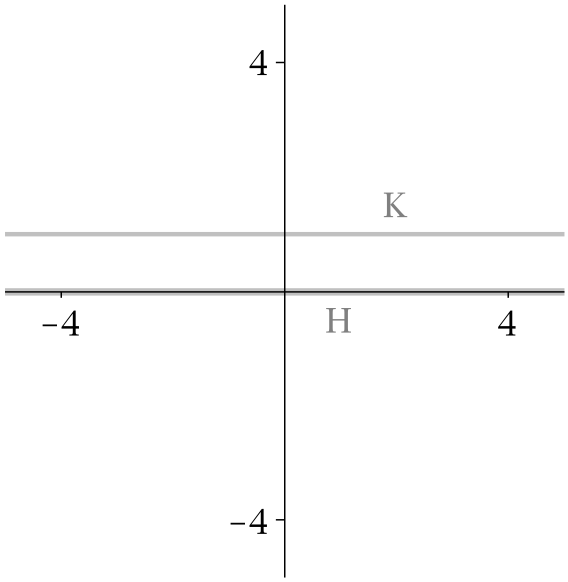


Figure 3.1. H and K from Example 3.8

You showed in Exercise 2.23 that this makes G a group. (Actually you proved it for $G \times H$ where G and H were groups. Here $G = H = \mathbb{R}$.)

Let $H = \{x \in G : x = (a, 0)\ \exists a \in \mathbb{R}\}$. We claim that $H < G$. *Why?* Use the subgroup theorem: Let $P, Q \in H$. By the definition of H, we can write $P = (p, 0)$ and $Q = (q, 0)$ where $p, q \in \mathbb{R}$. Then

$$P - Q = P + (-Q) = (p, 0) + (-q, 0) = (p - q, 0).$$

Membership in H requires the second ordinate to be zero. The second ordinate of $P - Q$ is in fact zero, so $P - Q \in H$. The Subgroup Theorem implies that $H < G$.

Let $K = \{x \in G : x = (a, 1)\ \exists a \in \mathbb{R}\}$. We claim that $K \not< G$. *Why not?* Again, use the Subgroup Theorem: Let $P, Q \in K$. By the definition of K, we can write $P = (p, 1)$ and $Q = (q, 1)$ where $p, q \in \mathbb{R}$. Then

$$P - Q = P + (-Q) = (p, 1) + (-q, -1) = (p - q, 0).$$

Membership in K requires the second ordinate to be one, but the second ordinate of $P - Q$ is zero, not one. Since $P - Q \notin K$, the Subgroup Theorem tells us that K is not a subgroup of G.

Figure 3.1 gives a visualization of H and K. You will diagram another subgroup of G in Exercise 3.15. ◿

Examples 3.7 and 3.8 give us examples of how the Subgroup Theorem verifies subgroups of *abelian* groups. Two interesting examples of nonabelian subgroups appear in D_3.

Example 3.9: Recall D_3 from Section 2.2. Both $H = \{\iota, \varphi\}$ and $K = \{\iota, \rho, \rho^2\}$ are subgroups of D_3. *Why?* Certainly $H, K \subsetneq G$, and Theorem 2.52 on page 41 tells us that H and K are groups. ◿

If a group satisfies a given property, a natural question to ask is whether its subgroups also satisfy this property. Cyclic groups are a good example: is every subgroup of a cyclic group also cyclic? The answer relies on the Division Theorem (Theorem 1.19 on page 9).

Theorem 3.10: *Subgroups of cyclic groups are also cyclic.*

PROOF: Let G be a cyclic group, and $H < G$. From the fact that G is cyclic, choose $g \in G$ such that $G = \langle g \rangle$.

First we must find a candidate generator of H. If $H = \{e\}$, then $H = \langle e \rangle = \langle g^0 \rangle$, and we are done. So assume there exists $h \in H$ such that $h \neq e$. By inclusion, every element $x \in H$ can be written in the form $x = g^i$ for some $i \in \mathbb{Z}$, so $h = g^n$ for some $n \in \mathbb{Z}$. Without loss of generality, we may assume that $n \in \mathbb{N}^+$; after all, we just showed that we can choose $h \neq e$, so $n \neq 0$, and if $n \notin \mathbb{N}$, then closure of H implies that $h^{-1} = g^{-n} \in H$, so choose h^{-1} instead.

A good candidate for the generator would be the smallest positive power of g in H, if it exists. Let S be the set of positive natural numbers i such that $g^i \in H$; in other words, $S = \left\{ i \in \mathbb{N}^+ : g^i \in H \right\}$. From the well-ordering of $\mathbb{N}$, there exists a smallest element of S; call it d, and assign $h = g^d$.

We claim that $H = \langle h \rangle$. Let $x \in H$; then $x \in G$. By hypothesis, G is cyclic, so $x = g^a$ for some $a \in \mathbb{Z}$. By the Division Theorem, we know that there exist unique $q, r \in \mathbb{Z}$ such that

- $a = qd + r$, and
- $0 \leq r < d$.

Let $y = g^r$; by Exercise 2.59, we can rewrite this as

$$y = g^r = g^{a-qd} = g^a g^{-(qd)} = x \cdot \left(g^d\right)^{-q} = x \cdot h^{-q}.$$

Now, $x \in H$ by definition, and $h^{-q} \in H$ by closure and the existence of inverses, so by closure $y = x \cdot h^{-q} \in H$ as well. We chose d as the smallest positive power of g in H, and we just showed that $g^r \in H$. Recall that $0 \leq r < d$. If $0 < r$; then $g^r \in H$, so $r \in S$. But $r < d$, which contradicts the choice of d as the smallest element of S. Hence r cannot be positive; instead, $r = 0$ and $x = g^a = g^{qd} = h^q \in \langle h \rangle$.

Since x was arbitrary in H, every element of H is in $\langle h \rangle$; that is, $H \subseteq \langle h \rangle$. Since $h \in H$ and H is a group, closure implies that $H \supseteq \langle h \rangle$, so $H = \langle h \rangle$. In other words, H is cyclic. □

We again look to $\mathbb{Z}$ for an example.

Example 3.11: Recall from Example 2.50 on page 41 that $\mathbb{Z}$ is cyclic; in fact $\mathbb{Z} = \langle 1 \rangle$. By Theorem 3.10, $d\mathbb{Z}$ is cyclic. In fact, $d\mathbb{Z} = \langle d \rangle$. Can you find another generator of $d\mathbb{Z}$? ◿

Exercises.

Exercise 3.12: Recall that Ω_n, the nth roots of unity, form a cyclic group of order n under multiplication.

(a) The elements of Ω_4 are listed at the beginning of Section 2.4. Explain why $\Omega_2 < \Omega_4$.

(b) Compute Ω_8, and explain why both $\Omega_2 < \Omega_8$ and $\Omega_4 < \Omega_8$.

(b) Explain why, if $d \mid n$, then $\Omega_d < \Omega_n$.

Exercise 3.13: Show that even though the Klein 4-group is not cyclic, each of its proper subgroups is cyclic (see Exercises 2.31 on page 32 and 2.62 on page 47).

Exercise 3.14:

(a) Let $D_n(\mathbb{R}) = \{aI_n : a \in \mathbb{R}\} \subseteq \mathbb{R}^{n\times n}$; that is, $D_n(\mathbb{R})$ is the set of all diagonal matrices whose values along the diagonal is constant. Show that $D_n(\mathbb{R}) < \mathbb{R}^{n\times n}$. (In case you've forgotten Exercise 2.25, the operation here is addition.)

(b) Let $D_n^*(\mathbb{R}) = \{aI_n : a \in \mathbb{R}\setminus\{0\}\} \subseteq \mathrm{GL}_n(\mathbb{R})$; that is, $D_n^*(\mathbb{R})$ is the set of all non-zero diagonal matrices whose values along the diagonal is constant. Show that $D_n^*(\mathbb{R}) < \mathrm{GL}_n(\mathbb{R})$. (In case you've forgotten Definition 2.4, the operation here is multiplication.)

Exercise 3.15: Let $G = \mathbb{R}^2 := \mathbb{R}\times\mathbb{R}$, with addition defined as in Exercise 2.23 and Example 3.8. Let $L = \{x \in G : x = (a,a)\ \exists a \in \mathbb{R}\}$.

(a) Describe L geometrically.

(b) Show that $L < G$.

(c) Suppose $\ell \subseteq G$ is any line. Identify as general a criterion as possible that decides whether $\ell < G$. Justify your answer.

Exercise 3.16: Let G be any group and $g \in G$. Show that $\langle g\rangle < G$.

Exercise 3.17: Let G be an abelian group. Let H, K be subgroups of G. Let

$$H + K = \{x + y : x \in H, y \in K\}.$$

Show that $H + K < G$.

Exercise 3.18: Let $H = \{\iota, \varphi\} < D_3$.

(a) Find a different subgroup K of D_3 with only two elements.

(b) Let $HK = \{xy : x \in H, y \in K\}$. Show that $HK \not< D_3$.

(c) Why does the result of (b) not contradict the result of Exercise 3.17?

Exercise 3.19: Explain why $\mathbb{R}$ cannot be cyclic.

Exercise 3.20: Let G be a group and $A_1, A_2, \ldots, A_m$ subgroups of G. Let

$$B = A_1 \cap A_2 \cap \cdots \cap A_m.$$

Show that $B < G$.

Exercise 3.21: Let G be a group and H, K two subgroups of G. Let $A = H \cup K$. Show that A *need not* be a subgroup of G.

3.2: Cosets

Recall the Division Theorem (Theorem 1.19 on page 9). Normally, we think of division of n by d as dividing n into q parts, each containing d elements, with r elements left over. For example, $n = 23$ apples divided among $d = 6$ bags gives $q = 3$ apples per bag and $r = 5$ apples left over.

Another way to look at division by d is that it divides $\mathbb{Z}$ into d sets of integers. Each integer falls into a set according to its remainder after division. An illustration using $n = 4$:

$\mathbb{Z}$:	…	-2	-1	0	1	2	3	4	5	6	7	8	…
		↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
division by 4:	…	2	3	0	1	2	3	0	1	2	3	0	…

Here $\mathbb{Z}$ is divided into four sets

$$\begin{aligned} A &= \{\ldots, -4, 0, 4, 8, \ldots\} \\ B &= \{\ldots, -3, 1, 5, 9, \ldots\} \\ C &= \{\ldots, -2, 2, 6, 10, \ldots\} \\ D &= \{\ldots, -1, 3, 7, 11, \ldots\}. \end{aligned} \tag{6}$$

Observe two important facts:

- the sets A, B, C, and D *cover* $\mathbb{Z}$; that is,

$$\mathbb{Z} = A \cup B \cup C \cup D;$$

  and
- the sets A, B, C, and D are *disjoint;* that is,

$$A \cap B = A \cap C = A \cap D = B \cap C = B \cap D = C \cap D = \emptyset.$$

We can diagram this:

$$\mathbb{Z} = \begin{array}{|c|}\hline A \\ \hline B \\ \hline C \\ \hline D \\ \hline \end{array}$$

This phenomenon, where a set is the union of smaller, disjoint sets, is important enough to highlight with a definition.

Definition 3.22: Suppose that A is a set and $\mathcal{B} = \{B_\lambda\}$ a family of subsets of A, called **classes**. We say that $\mathcal{B}$ is a **partition** of A if

- the classes **cover** A: that is, $A = \bigcup B_\lambda$; and
- distinct classes are disjoint: that is, if $B_1, B_2 \in \mathcal{B}$ are distinct ($B_1 \neq B_2$), then $B_1 \cap B_2 = \emptyset$.

Example 3.23: Let $\mathcal{B} = \{A, B, C, D\}$ where A, B, C, and D are defined as in (3.23). Then $\mathcal{B}$ is a partition of $\mathbb{Z}$. ◿

Two aspects of division allow us to use it to partition $\mathbb{Z}$ into sets:

- *existence of a remainder,* which implies that every integer belongs to at least one class, which in turn implies that the union of the classes covers $\mathbb{Z}$; and
- *uniqueness of the remainder,* which implies that every integer ends up in only one set, so that the classes are disjoint.

Using the vocabulary of groups, recall that $A = 4\mathbb{Z} < \mathbb{Z}$ (page 54). All the elements of B have the form $1+x$ for some $x \in A$. For example, $-3 = 1+(-4)$. Likewise, all the elements of C have the form $2+x$ for some $x \in A$, and all the elements of D have the form $3+x$ for some $x \in A$. So if we define

$$1+A := \{1+x : x \in A\},$$

then

$$\begin{aligned} 1+A &= \{\ldots, 1+(-4), 1+0, 1+4, 1+8, \ldots\} \\ &= \{\ldots, -3, 1, 5, 9, \ldots\} \\ &= B. \end{aligned}$$

Likewise, we can write $A = 0+A$ and $C = 2+A$, $D = 3+A$.

Pursuing this further, you can check that

$$\cdots = -3+A = 1+A = 5+A = 9+A = \cdots$$

and so forth. Interestingly, all the sets in the previous line are the same as B! In addition, $B = 1+A$, $B = 5+A$, and $1-5 = -4 \in A$. The same holds for C: $C = 2+A$, $C = 10+A$, and $2-10 = -8 \in A$. This relationship will prove important at the end of the section.

So the partition by remainders of division by four is related to the subgroup A of multiples of 4. This will become very important in Chapter 6.

How can we generalize this phenomen to subgroups that don't necessarily involve numbers?

Definition 3.24: Let G be a group and $A < G$. Let $g \in G$. We define the **left coset of A with g** as

$$gA = \{ga : a \in A\}$$

and the **right coset of A with g** as

$$Ag = \{ag : a \in A\}.$$

If A is an additive subgroup, we write the coset of A with g as

$$g+A := \{g+a : a \in A\}.$$

In general, left cosets and right cosets are not equal, partly because the operation might not commute. If we speak of "cosets" without specifying "left" or "right", we means "left cosets".

Example 3.25: Recall the group D_3 from Section 2.2 and the subgroup $H = \{\iota, \varphi\}$ from Example 3.9. In this case,

$$\rho H = \{\rho, \rho\varphi\} \text{ and } H\rho = \{\rho, \varphi\rho\}.$$

Since $\varphi\rho = \rho^2\varphi \neq \rho\varphi$, we see that $\rho H \neq H\rho$. ◿

Sometimes, the left coset and the right coset *are* equal. This is always true in abelian groups, as illustrated by Example 3.26.

Example 3.26: Consider the subgroup $H = \{(a, 0) : a \in \mathbb{R}\}$ of $\mathbb{R}^2$ from Exercise 3.15. Let $p = (3, -1) \in \mathbb{R}^2$. The coset of H with p is

$$\begin{aligned} p + H &= \{(3,-1) + q : q \in H\} \\ &= \{(3,-1) + (a, 0) : a \in \mathbb{R}\} \\ &= \{(3 + a, -1) : a \in \mathbb{R}\}. \end{aligned}$$

Sketch some of the points in $p + H$, and compare them to your sketch of H in Exercise 3.15. How does the coset compare to the subgroup?

Generalizing this further, every coset of H has the form $p + H$ where $p \in \mathbb{R}^2$. Elements of $\mathbb{R}^2$ are points, so $p = (x, y)$ for some $x, y \in \mathbb{R}$. The coset of H with p is

$$p + H = \{(x + a, y) : a \in \mathbb{R}\}.$$

Sketch several more cosets. How would you describe the set of *all* cosets of H in $\mathbb{R}^2$? ◿

The group does not *have* to be abelian in order to have the left and right cosets equal. When deciding if $gA = Ag$, we are not deciding *whether elements of G commute*, but *whether subsets of G are equal*. Returning to D_3, we can find a subgroup whose left and right cosets are equal even though the group is not abelian and the operation is not commutative.

Example 3.27: Let $K = \{\iota, \rho, \rho^2\}$; certainly $K < D_3$, after all, $K = \langle\rho\rangle$. In this case, $\alpha K = K\alpha$ for all $\alpha \in D_3$:

α	αK	$K\alpha$
ι	K	K
φ	$\{\varphi, \varphi\rho, \varphi\rho^2\} = \{\varphi, \rho\varphi, \rho^2\varphi\}$	$\{\varphi, \rho\varphi, \rho^2\varphi\}$
ρ	K	K
ρ^2	K	K
$\rho\varphi$	$\{\rho\varphi, (\rho\varphi)\rho, (\rho\varphi)\rho^2\} = \{\rho\varphi, \varphi, \rho^2\varphi\}$	$\{\rho\varphi, \varphi, \rho^2\varphi\}$
$\rho^2\varphi$	$\{\rho^2\varphi, (\rho^2\varphi)\rho, (\rho^2\varphi)\rho^2\} = \{\rho^2\varphi, \rho\varphi, \varphi\}$	$\{\rho^2\varphi, \rho\varphi, \varphi\}$

In each case, the sets φK and $K\varphi$ are equal, even though φ does not commute with ρ. (You should verify these computations by hand.) ◿

We can now explain the observation we made previously:

Theorem 3.28: *The cosets of a subgroup partition the group.*

PROOF: Let G be a group, and $A < G$. We have to show two things:

(CP1) the cosets of A cover G, and
(CP2) distinct cosets of A are disjoint.

We show (CP1) first. Let $g \in G$. The definition of a group tells us that $g = ge$. Since $e \in A$ by definition of subgroup, $g = ge \in gA$. Since g was arbitrary, every element of G is in some coset of A. Hence the union of all the cosets is G.

For (CP2), let $x, y \in G$. We proceed by showing the contrapositive: if two cosets are not disjoint, then they are not distinct. Assume that the cosets xA and yA are not disjoint; that is, $(xA) \cap (yA) \neq \emptyset$. We want to show that they are not distinct; that is, $xA = yA$. Since xA and yA are sets, we must show that two sets are equal. To do that, we show that $xA \subseteq yA$ and then $xA \supseteq yA$.

To show that $xA \subseteq yA$, let $g \in xA$. By assumption, $(xA) \cap (yA) \neq \emptyset$, so choose $h \in (xA) \cap (yA)$ as well. By definition of the sets, there exist $a_1, a_2, a_3 \in A$ such that $g = xa_1$, and $h = xa_2 = ya_3$. Since $xa_2 = ya_3$, the properties of a group imply that $x = y\left(a_3 a_2^{-1}\right)$. Thus

$$g = xa_1 = \left(y\left(a_3 a_2^{-1}\right)\right) a_1 = y\left(\left(a_3 a_2^{-1}\right) a_1\right) \in yA.$$

Since g was arbitrary in xA, we have shown $xA \subseteq yA$.

A similar argument shows that $xA \supseteq yA$. Thus $xA = yA$.

We have shown that if xA and yA are not disjoint, then they are not distinct. The contrapositive of this statement is precisely (CP2). Having shown (CP2) and (CP1), we have shown that the cosets of A partition G. □

We conclude this section with three facts that allow us to decide when cosets are equal.

Lemma 3.29 (Equality of cosets): *Let G be a group and $H < G$. All of the following hold:*
(CE1) $eH = H$.
(CE2) *For all $a \in G$, $a \in H$ iff $aH = H$.*
(CE3) *For all $a, b \in G$, $aH = bH$ if and only if $a^{-1}b \in H$.*

As usual, you should keep in mind that in additive groups these conditions translate to
(CE1) $0 + H = H$.
(CE2) For all $a \in G$, if $a \in H$ then $a + H = H$.
(CE3) For all $a, b \in G$, $a + H = b + H$ if and only if $a - b \in H$.

PROOF: We only sketch the proof here. You will fill in the details in Exercise 3.37. Remember that part of this problem involves proving that two sets are equal, and to prove that, you should prove that each is a subset of the other.

(CE1) is "obvious" (but fill in the details anyway).

Since (CE2) is an equivalence ("iff"), we have to prove two directions. Let $a \in G$. First, assume that $aH = H$; it is "obvious" that $a \in H$ (but fill in the details anyway). Conversely, assume that $a \in H$; it is "obvious" that $aH \subseteq H$. For the other direction, let $h \in H$; then find an element $x \in H$ such that $ax = h$. It's not so hard to find x from that equation, but you must also explain how we know that $x \in H$ and how subsequently $ax \in aH$; otherwise, we don't know that $h \in aH$.

Since (CE3) is also an equivalence, we have to prove two directions. Let $a, b \in G$. First, assume that $aH = bH$. Let $x \in aH$; then $x = ah$ for some $h \in H$. Since $aH = bH$, we know that $x \in bH$, so $x = b\widehat{h}$ for some $\widehat{h} \in H$ as well. By substitution, $ah = b\widehat{h}$. It is "obvious" from here that $a^{-1}b \in H$ (but fill in the details anyway).

Conversely, assume that $a^{-1}b \in H$. We must show that $aH = bH$, which requires us to show that $aH \subseteq bH$ and $aH \supseteq bH$. Since $a^{-1}b \in H$, we have

$$b = a\left(a^{-1}b\right) \in aH.$$

We can thus write $b = ah$ for some $h \in H$. Let $y \in bH$; then $y = b\widehat{h}$ for some $\widehat{h} \in H$, and we have $y = (ah)\,\widehat{h} \in H$. Since y was arbitrary in bH, we now have $aH \supseteq bH$.

Although we could build a similar argument to show that $aH \subseteq bH$, instead we point out that $aH \supseteq bH$ implies that $aH \cap bH \neq \emptyset$. The cosets are not disjoint, so by Theorem 3.28, they are not distinct: $aH = bH$. □

Exercises.

Exercise 3.30: Show explicitly why left and right cosets are equal in abelian groups.

Exercise 3.31: In Exercise 3.12, you showed that $\Omega_2 < \Omega_8$. Compute the left and right cosets of Ω_2 in Ω_8.

Exercise 3.32: Let $\{e, a, b, a+b\}$ be the Klein 4-group. (See Exercises 2.31 on page 32, 2.62 on page 47, and 3.13 on page 58.) Compute the cosets of $\langle a \rangle$.

Exercise 3.33: In Exercise 3.18 on page 58, you found another subgroup K of order 2 in D_3. Does K satisfy the property $\alpha K = K\alpha$ for all $\alpha \in D_3$?

Exercise 3.34: Recall the subgroup L of $\mathbb{R}^2$ from Exercise 3.15 on page 58.

(a) Give a geometric interpretation of the coset $(3,-1)+L$.
(b) Give an algebraic expression that describes $p+L$, for arbitrary $p \in \mathbb{R}^2$.
(c) Give a geometric interpretation of the cosets of L in $\mathbb{R}^2$.
(d) Use your geometric interpretation of the cosets of L in $\mathbb{R}^2$ to explain why the cosets of L partition $\mathbb{R}^2$.

Exercise 3.35: Recall $D_n(\mathbb{R})$ from Exercise 3.14 on page 58. Give a description in set notation for

$$\begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix} + D_2(\mathbb{R}).$$

List some elements of the coset.

Exercise 3.36: In the proof of Theorem 3.28 on page 61, we stated that "A similar argument shows that $xA \supseteq yA$." Give this argument.

Exercise 3.37: Prove Lemma 3.29(A).

Exercise 3.38: It turns out that membership in a coset is an equivalence relation. That is, if we define a relation $\sim$ on $x, y \in G$ by

$$x \sim y \quad \iff \quad x \text{ and } y \text{ are in the same coset of a subgroup } A \text{ of } G,$$

then this relation is reflexive, symmetric, and transitive. Prove this.

3.3: Lagrange's Theorem

This section introduces an important result describing the number of cosets a subgroup can have. This leads to some properties regarding the order of a group and any of its elements.

Notation 3.39: Let G be a group, and $A < G$. We write G/A for the set of all left cosets of A. That is,

$$G/A = \{gA : g \in G\}.$$

We also write $A\backslash G$ for the set of all right cosets of A:

$$A\backslash G = \{Ag : g \in G\}.$$

Example 3.40: Let $G = \mathbb{Z}$ and $A = 4\mathbb{Z}$. We saw in Example 3.23 that

$$G/A = \mathbb{Z}/4\mathbb{Z} = \{A, 1+A, 2+A, 3+A\}.$$

We actually "waved our hands" in Example 3.23. That means that we did not provide a very detailed argument, so let's show the details here. Recall that $4\mathbb{Z}$ is the set of multiples of $\mathbb{Z}$, so $x \in A$ iff x is a multiple of 4. What about the remaining elements of $\mathbb{Z}$?

Let $x \in \mathbb{Z}$; then

$$x + A = \{x + z : z \in A\} = \{x + 4n : n \in \mathbb{Z}\}.$$

Use the Division Theorem to write

$$x = 4q + r$$

for unique $q, r \in \mathbb{Z}$, where $0 \leq r < 4$. Then

$$x + A = \{(4q + r) + 4n : n \in \mathbb{Z}\} = \{r + 4(q + n) : n \in \mathbb{Z}\}.$$

By closure, $q + n \in \mathbb{Z}$. If we write m in place of $4(q + n)$, then $m \in 4\mathbb{Z}$. So

$$x + A = \{r + m : m \in 4\mathbb{Z}\} = r + 4\mathbb{Z}.$$

The distinct cosets of A are thus determined by the distinct remainders from division by 4. Since the remainders from division by 4 are 0, 1, 2, and 3, we conclude that

$$\mathbb{Z}/A = \{A, 1+A, 2+A, 3+A\}$$

as claimed above. ◿

Example 3.41: Let $G = D_3$ and $K = \{\iota, \rho, \rho^2\}$ as in Example 3.27, then

$$G/K = D_3/\langle\rho\rangle = \{K, \varphi K\}.$$

◿

Example 3.42: Let $H < \mathbb{R}^2$ be as in Example 3.8 on page 55; that is,

$$H = \left\{(a, 0) \in \mathbb{R}^2 : a \in \mathbb{R}\right\}.$$

Then

$$\mathbb{R}^2/H = \left\{r + H : r \in \mathbb{R}^2\right\}.$$

It is not possible to list all the elements of G/A, but some examples would be

$$(1,1)+H,\ (4,-2)+H.$$

Speaking *geometrically*, what do the elements of G/A look like? ◿

It is important to keep in mind that G/A is a set whose elements are also sets. As a result, showing equality of two elements of G/A requires one to show that two sets are equal.

When G is finite, a simple formula gives us the size of G/A.

Theorem 3.43 (Lagrange's Theorem): *Let G be a group of finite order, and $A < G$. Then*

$$|G/A| = \frac{|G|}{|A|}.$$

The notation of cosets is somewhat suggestive of the relationship we illustrated at the begining of Section 3.2 between cosets and division of the integers. Nevertheless, Lagrange's Theorem is *not* as obvious as the notation might imply: we can't "divide" the sets G and A. Rather, we are dividing group G by its subgroup A into cosets, obtaining the set of cosets G/A. Lagrange's Theorem states that the number of elements in G/A is the same as the quotient of the order of G by the order of A. Since G/A is not a number, we are not moving the absolute value bars "inside" the fraction.

PROOF: From Theorem 3.28 we know that the cosets of A partition G. There are $|G/A|$ cosets of A. Each of them has the same size, $|A|$. The number of elements of G is thus the product of

the number of elements in each coset and the number of cosets. That is, $|G/A| \cdot |A| = |G|$. This implies the theorem. □

The next-to-last sentence of the proof contains the statement $|G/A| \cdot |A| = |G|$. Since $|A|$ is the order of the group A, and $|G/A|$ is an integer, we conclude that:

Corollary 3.44: *The order of a subgroup divides the order of a group.*

Example 3.45: Let G be the Klein 4-group (see Exercises 2.31 on page 32, 2.62 on page 47, and 3.13 on page 58). Every subgroup of the Klein 4-group is cyclic, and has order 1, 2, or 4. As predicted by Corollary 3.44, the orders of the subgroups divide the order of the group.

Likewise, the order of $\{\iota, \varphi\}$ divides the order of D_3.

By contrast, the subset HK of D_3 that you computed in Exercise 3.18 on page 58 has four elements. Since $4 \nmid 6$, the contrapositive of Lagrange's Theorem implies that HK *cannot* be a subgroup of D_3. ◿

From the fact that every element g generates a cyclic subgroup $\langle g \rangle < G$, Lagrange's Theorem also implies an important consequence about the order of any element of any finite group.

Corollary 3.46: *In a finite group G, the order of any element divides the order of a group.*

PROOF: You do it! See Exercise 3.48. □

Exercises.

Exercise 3.47: Recall from Exercise 3.12 that if $d \mid n$, then $\Omega_d < \Omega_n$. How many cosets of Ω_d are there in Ω_n?

Exercise 3.48: Prove Corollary 3.46.

Exercise 3.49: Suppose that a group G has order 8, but is not cyclic. Show that $g^4 = e$ for all $g \in G$.

Exercise 3.50: Suppose that a group has five elements. Will it be cyclic?

Exercise 3.51: Find a sufficient (but not necessary) condition on the order of a group of order at least two that guarantees that the group is cyclic.

3.4: Quotient Groups

Let $A < G$. Is there a natural generalization of the operation of G that makes G/A a group? By a "natural" generalization, we mean something like

$$(gA)(hA) = (gh)A.$$

The first order of business it to make sure that the operation even makes sense. The technical word for this is that the operation is **well-defined**. *What does that mean?* A coset can have different representations. The operation defined above would not be an operation if two different representations of gA gave us two different answers. Example 3.52 shows how it can go wrong.

Example 3.52: Recall $A = \langle\varphi\rangle < D_3$ from Example 3.41. By the definition of the operation, we have

$$(\rho A)\left(\rho^2 A\right) = \left(\rho \circ \rho^2\right) A = \rho^3 A = \iota A = A.$$

Another representation of $\rho A = \{\rho\varphi, \rho\varphi^2\}$ is $(\rho\varphi)A$. If the operation were well-defined, then we should have $((\rho\varphi)A)\left(\rho^2 A\right) = (\rho A)\left(\rho^2 A\right) = A$. That is *not* the case:

$$((\rho\varphi)A)\left(\rho^2 A\right) = \left((\rho\varphi)\rho^2\right)A = \left(\rho\left(\varphi\rho^2\right)\right)A = (\rho(\rho\varphi))A = \left(\rho^2\varphi\right)A \neq A.$$

◿

On the other hand, sometimes the operation *is* well-defined.

Example 3.53: Recall the subgroup $A = 4\mathbb{Z}$ of $\mathbb{Z}$. Let $B, C, D \in \mathbb{Z}/A$, so $B = b + 4\mathbb{Z}$, $C = c + 4\mathbb{Z}$, and $D = d + 4\mathbb{Z}$ for some $b, c, d \in \mathbb{Z}$.

The problem is that we could have $B = D$ but $B + C \neq D + C$. For example, if $B = 1 + 4\mathbb{Z}$ and $D = 5 + 4\mathbb{Z}$, $B = D$. Does it follow that $B + C = D + C$?

From Lemma 3.29, we know that $B = D$ iff $b - d \in A = 4\mathbb{Z}$. That is, $b - d = 4m$ for some $m \in \mathbb{Z}$. Let $x \in B + C$; then $x = (b + c) + 4n$ for some $n \in \mathbb{Z}$; we have $x = ((d + 4m) + c) + 4n = (d + c) + 4(m + n) \in D + C$. Since x was arbitrary in $B + C$, we have $B + C \subseteq D + C$. A similar argument shows that $B + C \supseteq D + C$, so $B + C = D + C$. ◿

So the operation was well-defined here. What made for the difference? When we rewrote

$$((d + 4m) + c) + 4n = (d + c) + 4(m + n)$$

we relied on the fact that *addition commutes in an abelian group*. Without that fact, we could not have swapped c and $4m$. Can we identify a condition on a subgroup that would guarantee that the procedure results in an operation? If cosets are to act as a group, does the group have to be abelian?

The key in Example 3.53 was not really that $\mathbb{Z}$ is abelian. Rather, the key was that we could swap $4m$ and c in the expression $((d + 4m) + c) + 4m$. In a general group setting where $A < G$, for every $c \in G$ and for every $a \in A$ we would need to find $a' \in A$ to replace ca with $a'c$. The abelian property makes it easy to do that, but we don't *need* G to be abelian; we need A to satisfy this property. Let's emphasize that:

The operation defined above is well-defined
iff
for every $c \in G$ and for every $a \in A$
there exists $a' \in A$ such that $ca = a'c$.

Think about this in terms of sets: for every $c \in G$ and for *every* $a \in A$, there exists $a' \in A$ such that $ca = a'c$. Here $ca \in cA$ is arbitrary, so $cA \subseteq Ac$. The other direction must also be true, so $cA \supseteq Ac$. In other words,

The operation defined above is well-defined
iff $cA = Ac$ *for all* $c \in G$.

This property merits a definition.

Definition 3.54: Let $A < G$. If

$$gA = Ag$$

for every $g \in G$, then A is a **normal subgroup** of G.

Notation 3.55: We write $A \triangleleft G$ to indicate that A is a normal subgroup of G.

Although we have outlined the argument above, we should show explicitly that if A is a normal subgroup, then the operation proposed for G/A is indeed well-defined.

Lemma 3.56: *Let $A < G$. Then (CO1) implies (CO2).*
(CO1) $A \triangleleft G$.
(CO2) *Let $X, Y \in G/A$ and $x, y \in G$ such that $X = xA$ and $Y = yA$. The operation $\cdot$ on G/A defined by*

$$XY = (xy)A$$

is well-defined for all $x, y \in G$.

PROOF: Let $W, X, Y, Z \in G/A$ and choose $w, x, y, z \in G$ such that $W = wA$, $X = xA$, $Y = yA$, and $Z = zA$. To show that the operation is well-defined, we must show that if $W = X$ and $Y = Z$, then $WY = XZ$ regardless of the values of w, x, y, or z. Assume therefore that $W = X$ and $Y = Z$. By substitution, $wA = xA$ and $yA = zA$. By Lemma 3.29(CE3), $w^{-1}x \in A$ and $y^{-1}z \in A$.

Since WY and XZ are sets, showing that they are equal requires us to show that each is a subset of the other. First we show that $WY \subseteq XZ$. To do this, let $t \in WY = (wy)A$. By definition of a coset, $t = (wy)a$ for some $a \in A$. What we will do now is rewrite t by

- using the fact that A is normal to move some element of a left, then right, through the representation of t; and
- using the fact that $W = X$ and $Y = Z$ to rewrite products of the form $w\breve{\alpha}$ as $x\widehat{\alpha}$ and $y\dot{\alpha}$ as $z\ddot{\alpha}$, where $\breve{\alpha}, \widehat{\alpha}, \dot{\alpha}, \ddot{\alpha} \in A$.

How, precisely? By the associative property, $t = w(ya)$. By definition of a coset, $ya \in yA$. By hypothesis, A is normal, so $yA = Ay$; thus, $ya \in Ay$. By definition of a coset, there exists $\breve{a} \in A$ such that $ya = \breve{a}y$. By substitution, $t = w(\breve{a}y)$. By the associative property, $t = (w\breve{a})y$. By definition of a coset, $w\breve{a} \in wA$. By hypothesis, A is normal, so $wA = Aw$. Thus $w\breve{a} \in Aw$. By hypothesis, $W = X$; that is, $wA = xA$. Thus $w\breve{a} \in xA$, and by definition of a coset, $w\breve{a} = x\hat{a}$

for some $\hat{a} \in A$. By substitution, $t = (x\hat{a})\,y$. The associative property again gives us $t = x\,(\hat{a}y)$; since A is normal we can write $\hat{a}y = y\dot{a}$ for some $\dot{a} \in A$. Hence $t = x\,(y\dot{a})$. Now,

$$y\dot{a} \in yA = Y = Z = zA,$$

so we can write $y\dot{a} = z\ddot{a}$ for some $\ddot{a} \in A$. By substitution and the definition of coset arithmetic,

$$t = x\,(z\ddot{a}) = (xz)\,\ddot{a} \in (xz)A = (xA)\,(zA) = XZ.$$

Since t was arbitrary in WY, we have shown that $WY \subseteq XZ$. A similar argument shows that $WY \supseteq XZ$; thus $WY = XZ$ and the operation is well-defined. □

An easy generalization of the argument of Example 3.53 shows the following Theorem.

Theorem 3.57: *Let G be an abelian group, and $H < G$. Then $H \triangleleft G$.*

PROOF: You do it! See Exercise 3.66. □

As we pointed out before, we don't need an abelian group to have a normal subgroup.

Example 3.58: Let

$$A_3 = \left\{\iota, \rho, \rho^2\right\} < D_3.$$

We call A_3 the **alternating group** on three elements. We claim that $A_3 \triangleleft D_3$. Indeed,

σ	σA_3	$A_3\sigma$
ι	A_3	A_3
ρ	A_3	A_3
ρ^2	A_3	A_3
φ	$\varphi A_3 = \{\varphi, \varphi\rho, \varphi\rho^2\} = \{\varphi, \rho^2\varphi, \rho\varphi\} = A_3\varphi$	$A_3\varphi = \varphi A_3$
$\rho\varphi$	$\{\rho\varphi, (\rho\varphi)\,\rho, (\rho\varphi)\,\rho^2\} = \{\rho\varphi, \varphi, \rho^2\varphi\} = \varphi A_3$	φA_3
$\rho^2\varphi$	$\{\rho^2\varphi, (\rho^2\varphi)\,\rho, (\rho^2\varphi)\,\rho^2\} = \{\rho^2\varphi, \rho\varphi, \varphi\} = \varphi A_3$	φA_3

(We have left out some details. You should check the computation carefully, using extensively the fact that $\varphi\rho = \rho^2\varphi$.) ◿

As we wanted, normal subgroups allow us to turn the set of cosets into a group G/A.

Theorem 3.59: *Let G be a group. If $A \triangleleft G$, then G/A is a group.*

PROOF: Assume $A \triangleleft G$. By Lemma 3.56, the operation is well-defined, so it remains to show that G/A satisfies the properties of a group.

(closure) Closure follows from the fact that multiplication of cosets is well-defined when $A \triangleleft G$, as shown in Lemma 3.56: Let $X, Y \in G/A$, and choose $g_1, g_2 \in G$ such that $X = g_1A$ and $Y = g_2A$. By definition of coset multiplication, $XY = (g_1A)\,(g_2A) = (g_1g_2)A \in G/A$. Since X, Y were arbitrary in G/A, coset multiplication is closed.

(associativity) The associative property of G/A follows from the associative property of G. Let $X, Y, Z \in G/A$; choose $g_1, g_2, g_3 \in G$ such that $X = g_1A$, $Y = g_2A$, and $Z = g_3A$. Then

$$(XY)\,Z = [(g_1A)\,(g_2A)]\,(g_3A)\,.$$

By definition of coset multiplication,

$$(XY)\,Z = ((g_1g_2)A)\,(g_3A)\,.$$

By the definition of coset multiplication,

$$(XY)\,Z = ((g_1g_2)\,g_3)\,A.$$

(Note the parentheses grouping g_1g_2.) Now apply the associative property of G and reverse the previous steps to obtain

$$\begin{aligned}(XY)\,Z &= (g_1\,(g_2g_3))\,A\\ &= (g_1A)\,((g_2g_3)A)\\ &= (g_1A)\,[(g_2A)\,(g_3A)]\\ &= X\,(YZ)\,.\end{aligned}$$

Since $(XY)\,Z = X\,(YZ)$ and X, Y, Z were arbitrary in G/A, coset multiplication is associative.

(identity) We claim that the identity of G/A is A itself. Let $X \in G/A$, and choose $g \in G$ such that $X = gA$. Since $e \in A$, Lemma 3.29 on page 62 implies that $A = eA$, so

$$XA = (gA)\,(eA) = (ge)\,A = gA = X.$$

Since X was arbitrary in G/A and $XA = X$, A is the identity of G/A.

(inverse) Let $X \in G/A$. Choose $g \in G$ such that $X = gA$, and let $Y = g^{-1}A$. We claim that $Y = X^{-1}$. By applying substitution and the operation on cosets,

$$XY = (gA)\left(g^{-1}A\right) = \left(g\,g^{-1}\right)A = eA = A.$$

Hence X has an inverse in G/A. Since X was arbitrary in G/A, every element of G/A has an inverse.

We have shown that G/A satisfies the properties of a group. □

We need a definition for this new kind of group.

Definition 3.60: Let G be a group, and $A \triangleleft G$. Then G/A is **the quotient group of G with respect to A**, also called G **mod** A.

Normally we simply say "the quotient group" rather than "the quotient group of G with respect to A." We meet a very interesting and important quotient group in Section 3.5.

Example 3.61: Since A_3 is a normal subgroup of D_3, D_3/A_3 is a group. By Lagrange's Theorem, it has $6/3 = 2$ elements. The composition table is

$\circ$	A_3	φA_3
A_3	A_3	φA_3
φA_3	φA_3	A_3

◿

Exercises.

Exercise 3.62: Show that for any group G, $\{e\} \triangleleft G$ and $G \triangleleft G$.

Exercise 3.63: Recall from Exercise 3.12 that if $d \mid n$, then $\Omega_d < \Omega_n$.
(a) Explain how we know that, in fact, $\Omega_d \triangleleft \Omega_n$.
(b) Compute the Cayley table of the quotient group Ω_8/Ω_2. Does it have the same structure as the Klein 4-group, or as the Cyclic group of order 4?

Exercise 3.64: Let $H = \langle \mathbf{i} \rangle < Q_8$.
(a) Show that $H \triangleleft Q_8$ by computing all the cosets of H.
(b) Compute the multiplication table of Q_8/H.

Exercise 3.65: Let $H = \langle -1 \rangle < Q_8$.
(a) Show that $H \triangleleft Q_8$ by computing all the cosets of H.
(b) Compute the multiplication table of Q_8/H.
(c) With which well-known group does Q_8/H have the same structure?

Exercise 3.66: Let G be an abelian group. Explain why for any $H < G$ we know that $H \triangleleft G$.

Exercise 3.67: Let G be a group, $g \in G$, and $H < G$. Define the **conjugation** of H by g as

$$gHg^{-1} = \{h^g : h \in H\}.$$

(The notation h^g is the definition of conjugation from Exercise 2.36 on page 33; that is, $h^g = ghg^{-1}$.) Show that $H \triangleleft G$ if and only if $H = gHg^{-1}$ for all $g \in G$.[18]

Exercise 3.68: Recall the subgroup L of $\mathbb{R}^2$ from Exercises 3.15 on page 58 and 3.34 on page 63.
(a) Explain how we know that $L \triangleleft \mathbb{R}^2$ *without* checking that $p + L = L + p$ for any $p \in \mathbb{R}^2$.
(b) Sketch two elements of $\mathbb{R}^2/L$ and show their addition.

Exercise 3.69: Explain why every subgroup of $D_m(\mathbb{R})$ is normal.

Exercise 3.70: Show that Q_8 is not a normal subgroup of $\mathrm{GL}_m(\mathbb{C})$.

[18] Certain texts define a normal subgroup this way; that is, a subgroup H is normal if every conjugate of H is precisely H. They then prove that in this case, any left coset equals the corresponding right coset.

Exercise 3.71: Let G be a group. Define the **centralizer** of G as

$$Z(G) = \{g \in G : \ xg = gx \ \forall x \in G\}.$$

Show that $Z(G) \triangleleft G$.

Exercise 3.72: Let G be a group, and $H < G$. Define the **normalizer** of H as

$$N_G(H) = \{g \in G : \ gH = Hg\}.$$

Show that $H \triangleleft N_G(H)$.

Exercise 3.73: Let G be a group, and $A < G$. Suppose that $|G/A| = 2$; that is, the subgroup A partitions G into precisely two left cosets. Show that:

- $A \triangleleft G$; and
- G/A is abelian.

Exercise 3.74: Recall from Exercise 2.36 on page 33 the commutator of two elements of a group. Let $[G,G]$ denote the intersection of all subgroups of G that contain $[x,y]$ for all $x,y \in G$.

(a) Compute $[D_3, D_3]$.

(b) Compute $[Q_8, Q_8]$.

(c) Show that $[G,G] \triangleleft G$; that is, $[G,G]$ is a normal subgroup of G. *Note:* We call $[G,G]$ the **commutator subgroup** of G. See Section 3.6.

3.5: “Clockwork” groups

By Theorem 3.57, every subgroup H of $\mathbb{Z}$ is normal. Let $n \in \mathbb{Z}$; since $n\mathbb{Z} < \mathbb{Z}$, it follows that $n\mathbb{Z} \triangleleft \mathbb{Z}$. Thus $\mathbb{Z}/n\mathbb{Z}$ is a quotient group.

We used $n\mathbb{Z}$ in many examples of subgroups. One reason is that you are accustomed to working with $\mathbb{Z}$, so it should be conceptually easy. Another reason is that the quotient group $\mathbb{Z}/n\mathbb{Z}$ has a vast array of applications in number theory and computer science. You will see some of these in Chapter 6. Because this group is so important, we give it several special names.

Definition 3.75: Let $n \in \mathbb{Z}$. We call the quotient group $\mathbb{Z}/n\mathbb{Z}$

- $\mathbb{Z}$ mod $n\mathbb{Z}$, or
- $\mathbb{Z}$ **mod** n, or
- the **linear residues modulo** n.

Notation 3.76: It is common to write $\mathbb{Z}_n$ instead of $\mathbb{Z}/n\mathbb{Z}$.

Example 3.77: You already saw a bit of $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$ at the beginning of Section 3.2 and again in Example 3.53. Recall that $\mathbb{Z}_4 = \{4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$. Addition in this group will always give us one of those four representations of the cosets:

$$(2+4\mathbb{Z}) + (1+4\mathbb{Z}) = 3+4\mathbb{Z};$$
$$(1+4\mathbb{Z}) + (3+4\mathbb{Z}) = 4+4\mathbb{Z} = 4\mathbb{Z};$$
$$(2+4\mathbb{Z}) + (3+4\mathbb{Z}) = 5+4\mathbb{Z} = 1+4\mathbb{Z};$$

and so forth.

Reasoning similar to that used at the beginning of Section 3.2 would show that

$$\mathbb{Z}_{31} = \mathbb{Z}/31\mathbb{Z} = \{31\mathbb{Z}, 1+31\mathbb{Z}, \ldots, 30+31\mathbb{Z}\}.$$

We show this explicitly in Theorem 3.81. ◿

Before looking at some properties of $\mathbb{Z}_n$, let's look for an easier way to talk about its elements. It is burdensome to write $a+n\mathbb{Z}$ whenever we want to discuss an element of $\mathbb{Z}_n$, so we adopt the following convention.

Notation 3.78: Let $A \in \mathbb{Z}_n$ and choose $r \in \mathbb{Z}$ such that $A = r+n\mathbb{Z}$.

- If it is clear from context that A is an element of $\mathbb{Z}_n$, then we simply write r instead of $r+n\mathbb{Z}$.
- If we want to emphasize that A is an element of $\mathbb{Z}_n$ (perhaps there are a lot of integers hanging about) then we write $[r]_n$ instead of $r+n\mathbb{Z}$.
- If the value of n is obvious from context, we simply write $[r]$.

To help you grow accustomed to the notation $[r]_n$, we use it for the rest of this chapter, even when n is mind-bogglingly obvious.

The first property is that, for most values of n, $\mathbb{Z}_n$ has finitely many elements. To show that there are finitely many elements of $\mathbb{Z}_n$, we rely on the following fact, which is important enough to highlight as a separate result.

Lemma 3.79: *Let $n \in \mathbb{Z}\setminus\{0\}$ and $[a]_n \in \mathbb{Z}_n$. Use the Division Theorem to choose $q, r \in \mathbb{Z}$ such that $a = qn+r$ and $0 \le r < n$. Then $[a]_n = [r]_n$.*

It should not surprise you that the proof of Lemma 3.79relies on the Division Theorem, since we said that the elements of $\mathbb{Z}_n$ correspond to the remainders from division by n. It is similar to the discussion in Example 3.40 on page 64, so you might want to reread that.

PROOF: We give two different proofs.

(1) By definition and substitution,

$$\begin{aligned}
[a]_n &= a+n\mathbb{Z} \\
&= (qn+r)+n\mathbb{Z} \\
&= \{(qn+r)+nd : d \in \mathbb{Z}\} \\
&= \{r+n(q+d) : d \in \mathbb{Z}\} \\
&= \{r+nm : m \in \mathbb{Z}\} \\
&= r+n\mathbb{Z} \\
&= [r]_n.
\end{aligned}$$

(2) Rewrite $a = qn+r$ as $a-r = qn$. By definition, $a-r \in n\mathbb{Z}$. The immensely useful Lemma 3.29 shows that $a+n\mathbb{Z} = r+n\mathbb{Z}$, and the notation implies that $[a]_n = [r]_n$. □

Definition 3.80: We call $[r]_n$ in Lemma 3.79 the **canonical representation** of $[a]_n$. That is, the canonical representation of an element of $\mathbb{Z}_n$ is the representation whose value is between 0 and $n-1$, inclusive.

Theorem 3.81: *$\mathbb{Z}_n$ is finite for every nonzero $n \in \mathbb{Z}$. In fact, if $n \neq 0$ then $\mathbb{Z}_n$ has $|n|$ elements corresponding to the remainders from division by n: 0, 1, 2, …, $n-1$.*

PROOF: Lemma 3.79 on the preceding page states that every element of such $\mathbb{Z}_n$ can be represented by $[r]_n$ for some $r \in \mathbb{Z}$ where $0 \leq r < |n|$. But there are only $|n|$ possible choices for such a remainder. □

Let's look at how we can perform arithmetic in $\mathbb{Z}_n$.

Lemma 3.82: *Let $d, n \in \mathbb{Z}$ and $[a]_n, [b]_n \in \mathbb{Z}_n$. Then*

$$[a]_n + [b]_n = [a+b]_n \qquad \text{and} \qquad d\,[a]_n = [da]_n .$$

For example, $[3]_7 + [9]_7 = [3+9]_7 = [12]_7 = [5]_7$ and $-4\,[3]_5 = [-4 \cdot 3]_5 = [-12]_5 = [3]_5$.

PROOF: Applying the definitions of the notation, of coset addition, and of $n\mathbb{Z}$, we see that

$$\begin{aligned} [a]_n + [b]_n &= (a + n\mathbb{Z}) + (b + n\mathbb{Z}) \\ &= (a+b) + n\mathbb{Z} \\ &= [a+b]_n . \end{aligned}$$

For $d\,[a]_n$, we consider two cases. If d is positive, then the expression $d\,[a]_n$ is the sum of d copies of $[a]_n$, which the Lemma's first claim (now proved) implies to be

$$\underbrace{[a]_n + [a]_n + \cdots + [a]_n}_{d \text{ times}} = [2a]_n + \underbrace{[a]_n + \cdots + [a]_n}_{d-2 \text{ times}} = \cdots = [da]_n .$$

If d is negative, then the expression $d\,[a]_n$ is the sum of $|d|$ copies of $-[a]_n$ (this notation is defined at the beginning of Chapter 2, Section 2.3). Again using the first claim, $[a]_n + [-a]_n = [a + (-a)]_n = [0]_n$, so $-[a]_n = [-a]_n$. By substitution,

$$d\,[a]_n = |d|\,(-[a_n]) = |d|\,[-a]_n = [|d| \cdot (-a)]_n = [-d \cdot (-a)]_n = [da]_n .$$

□

Lemmas 3.79 and 3.82 imply that each $\mathbb{Z}_n$ acts as a **"clockwork" group**. Why?

- To add $[a]_n$ and $[b]_n$, let $c = a + b$.
- If $0 \leq c < n$, then you are done. After all, division of c by n gives $q = 0$ and $r = c$.

- Otherwise, $c < 0$ or $c \geq n$, so we divide c by n, obtaining q and r where $0 \leq r < n$. The sum is $[r]_n$.

We call this "clockwork" because it counts like a clock: if you wait ten hours starting at 5 o'clock, you arrive not at 15 o'clock, but at $15 - 12 = 3$ o'clock.

It should be clear from Example 2.8 on page 27 as well as Exercise 2.30 on page 32 that $\mathbb{Z}_2$ and $\mathbb{Z}_3$ have precisely the same structure as the groups of order 2 and 3.

On the other hand, we saw in Exercise 2.31 on page 32 that there are two possible structures for a group of order 4: the Klein 4-group, and a cyclic group. Which structure does $\mathbb{Z}_4$ have?

Example 3.83: Use Lemma 3.82 on the preceding page to observe that

$$\left\langle [1]_4 \right\rangle = \left\{ [0]_4, [1]_4, [2]_4, [3]_4 \right\}$$

since $[2]_4 = [1]_4 + [1]_4$, $[3]_4 = [2]_4 + [1]_4$, and $[0]_4 = 0 \cdot [1]_4$ (or $[0]_4 = [3]_4 + [1]_4$). ◿

The fact that $\mathbb{Z}_4$ was cyclic makes one wonder: is $\mathbb{Z}_n$ always cyclic? Yes!

Theorem 3.84: *$\mathbb{Z}_n$ is cyclic for every $n \in \mathbb{Z}$.*

PROOF: Let $n \in \mathbb{Z}$. We have

$$[a]_n = [a \cdot 1]_n = a\,[1]_n \in \left\langle [1]_n \right\rangle.$$

So $\mathbb{Z}_n \subseteq \left\langle [1]_n \right\rangle$. It is clear that $\mathbb{Z}_n \supseteq \left\langle [1]_n \right\rangle$, so in fact $\mathbb{Z}_n = \left\langle [1]_n \right\rangle$, and $\mathbb{Z}_n$ is therefore cyclic. □

We saw in Example 3.83 that not *every* non-zero element necessarily generates $\mathbb{Z}_n$. A natural and interesting followup question to ask is, which non-zero elements *do* generate $\mathbb{Z}_n$? You need a bit more background in number theory before you can answer that question, but in the exercises you will build some more addition tables and use them to formulate a hypothesis.

The following important lemma gives an "easy" test for whether two integers are in the same coset of $\mathbb{Z}_n$.

Lemma 3.85: *Let $a, b, n \in \mathbb{Z}$ and assume that n. The following are equivalent.*
(A) $a + n\mathbb{Z} = b + n\mathbb{Z}$.
(B) $[a]_n = [b]_n$.
(C) $n \mid (a - b)$.

PROOF: You do it! See Exercise 3.92. □

Exercises.

Exercise 3.86: We showed that $\mathbb{Z}_n$ is finite for $n \neq 0$. What if $n = 0$? How many elements would it have? Illustrate a few additions and subtractions, and indicate whether you think that $\mathbb{Z}_0$ is an interesting or useful group.

Exercise 3.87: We don't actually talk about $\mathbb{Z}_n$ for $n < 0$. Show that this is because $\mathbb{Z}_n = \mathbb{Z}_{|n|}$.

Exercise 3.88: As discussed in the notes, we know already that $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are not very interesting, because their addition tables are predetermined. Since their addition tables should be easy to determine, go ahead and write out the addition tables for these groups.

Exercise 3.89: Write down the addition table for $\mathbb{Z}_5$. Which elements generate $\mathbb{Z}_5$?

Exercise 3.90: Write down the addition table for $\mathbb{Z}_6$. Which elements generate $\mathbb{Z}_6$?

Exercise 3.91: Compare the results of Example 3.83 and Exercises 3.88, 3.89, and 3.90. Formulate a conjecture as to which elements generate $\mathbb{Z}_n$. Do not try to prove your example.

Exercise 3.92: Prove Lemma 3.85.

3.6: "Solvable" groups

One of the major motivations of group theory was the question of whether a polynomial can be solved by radicals. For example, if we have a quadratic equation $ax^2 + bx + c = 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

(This works unless $a \neq 0$, in which case we wouldn't consider the equation quadratic.) Since the solution contains nothing more than addition, multiplication, and radicals, we say that a quadratic equation is *solvable by radicals*.

Similar formulas can be found for cubic and quartic equations. When mathematicians turned their attention to quintic equations, however, they hit a wall: they weren't able to use previous techniques to find a "quintic formula". Eventually, it was shown that this is because some quintic equations are not solvable by radicals. The method they used to show this is related to the following concept.

Definition 3.93: If a group G contains subgroups $G_0, G_1, \ldots, G_n$ such that

- $G_0 = \{e\}$;
- $G_n = G$;
- $G_{i-1} \triangleleft G_i$; and
- G_i / G_{i-1} is abelian,

then G is a **solvable group**. The chain of subgroups $G_0, \ldots, G_n$ is called a **normal series**.

Example 3.94: Any finite abelian group G is solvable: let $G_0 = \{e\}$ and $G_1 = G$. Subgroups of an abelian group are always normal, so $G_0 \triangleleft G_1$. In addition, $X, Y \in G_1/G_0$ implies that $X = x\{e\}$ and $Y = y\{e\}$ for some $x, y \in G_1 = G$. Since G is abelian,

$$XY = (xy)\{e\} = (yx)\{e\} = YX.$$

◿

Example 3.95: The group D_3 is solvable. To see this, let $n = 2$ and $G_1 = \langle \rho \rangle$:

- By Exercise 3.62 on page 71, $\{e\} \triangleleft G_1$. To see that $G_1/\{e\}$ is abelian, note that for any $X, Y \in G_1/\{e\}$, we can write $X = x\{e\}$ and $Y = y\{e\}$ for some $x, y \in G_1$. By definition of G_1, we can write $x = \rho^a$ and $y = \rho^b$ for some $a, b \in \mathbb{Z}$. We can then fall back on the commutative property of addition in $\mathbb{Z}$ to show that

$$XY = (xy)\{e\} = \rho^{a+b}\{e\} = \rho^{b+a}\{e\} = (yx)\{e\} = YX.$$

- By Exercise 3.73 on page 72 and the fact that $|G_1| = 3$ and $|G_2| = 6$, we know that $G_1 \triangleleft G_2$. The same exercise tells us that G_2/G_1 is abelian. ◿

The following properties of solvable subgroups are very useful in a branch of algebra called *Galois Theory*.

Theorem 3.96: *Every quotient group of a solvable group is solvable.*

PROOF: Let G be a group and $A \triangleleft G$. We need to show that G/A is solvable. Since G is solvable, choose a normal series $G_0, \ldots, G_n$. Let

$$A_i = \{gA : g \in G_i\}.$$

We claim that the chain $A_0, A_1, \ldots, A_n$ likewise satisfies the definition of a solvable group.

First, we show that $A_{i-1} \triangleleft A_i$ for each $i = 1, \ldots, n$. Let $X \in A_i$; by definition, $X = xA$ for some $x \in G_i$. We have to show that $XA_{i-1} = A_{i-1}X$. Let $Y \in A_{i-1}$; by definition, $Y = yA$ for some $y \in G_{i-1}$. Recall that $G_{i-1} \triangleleft G_i$, so there exists $\widehat{y} \in G_{i-1}$ such that $xy = \widehat{y}x$. Let $\widehat{Y} = \widehat{y}A$; since $\widehat{y} \in G_{i-1}$, $\widehat{Y} \in A_{i-1}$. Using substitution and the definition of coset arithmetic, we have

$$XY = (xy)A = (\widehat{y}x)A = \widehat{Y}X \in A_{i-1}X.$$

Since Y was arbitrary in A_{i-1}, $XA_{i-1} \subseteq A_{i-1}X$. A similar argument shows that $XA_{i-1} \supseteq A_{i-1}X$, so the two are equal. Since X is an arbitrary coset of A_{i-1} in A_i, we conclude that $A_{i-1} \triangleleft A_i$.

Second, we show that A_i/A_{i-1} is abelian. Let $X, Y \in A_i/A_{i-1}$. By definition, we can write $X = SA_{i-1}$ and $Y = TA_{i-1}$ for some $S, T \in A_i$. Again by definition, there exist $s, t \in G_i$ such that $S = sA$ and $T = tA$. Let $U \in A_{i-1}$; we can likewise write $U = uA$ for some $u \in G_{i-1}$.

Since G_i/G_{i-1} is abelian, $(st)\,G_{i-1} = (ts)\,G_{i-1}$; thus, $(st)\,u = (ts)\,v$ for some $v \in G_{i-1}$. By definition, $vA \in A_{i-1}$. By substitution and the definition of coset arithmetic, we have

$$\begin{aligned} XY &= (ST)\,A_{i-1} \\ &= ((st)\,A)\,A_{i-1} \\ &= [(st)\,A]\,(uA) \\ &= ((st)\,u)\,A \\ &= ((ts)\,v)\,A \\ &= [(ts)\,A]\,(vA) \\ &= ((ts)\,A)\,A_{i-1} \\ &= (TS)\,A_{i-1} \\ &= YX. \end{aligned}$$

Since X and Y were arbitrary in the quotient group A_i/A_{i-1}, we conclude that it is abelian.

We have constructed a normal series in G/A; it follows that G/A is solvable. □

The following result is also true:

Theorem 3.97: *Every subgroup of a solvable group is solvable.*

Proving it, however, is a little more difficult. We need the definition of the commutator from Exercises 2.36 on page 33 and 3.74 on page 72.

Definition 3.98: Let G be a group. The **commutator subgroup** G' of G is the intersection of all subgroups of G that contain $[x,y]$ for all $x,y \in G$.

Notice that $G' < G$ by Exercise 3.20.

Notation 3.99: We wrote G' as $[G,G]$ in Exercise 3.74.

Lemma 3.100: *For any group G, $G' \triangleleft G$. In addition, G/G' is abelian.*

PROOF: You showed that $G' \triangleleft G$ in Exercise 3.74 on page 72. To show that G/G' is abelian, let $X, Y \in G/G'$. Write $X = xG'$ and $Y = yG'$ for appropriate $x,y \in G$. By definition, $XY = (xy)\,G'$. Let $g' \in G'$; by definition, $g' = [a,b]$ for some $a,b \in G$. Since G' is a group, it is closed under the operation, so $[x,y]\,[a,b] \in G'$. Let $z \in G'$ such that $[x,y]\,[a,b] = z$. Rewrite this expression as

$$\left(x^{-1}y^{-1}xy\right)[a,b] = z \quad \Longrightarrow \quad (xy)\,[a,b] = (yx)\,z.$$

(Multiply both sides of the equation on the left by yx.) Hence

$$(xy)\,g = (xy)\,[a,b] = (yx)\,z \in (yx)\,G'.$$

Since g' was arbitrary, $(xy)G' \subseteq (yx)G'$. A similar argument shows that $(xy)G' \supseteq (yx)G'$. Thus

$$XY = (xy)G' = (yx)G' = YX,$$

and G/G' is abelian. □

Lemma 3.101: *If $H \subseteq G$, then $H' \subseteq G'$.*

PROOF: You do it! See Exercise 3.105. □

Notation 3.102: Define $G^{(0)} = G$ and $G^{(i)} = \left(G^{(i-1)}\right)'$; that is, $G^{(i)}$ is the commutator subgroup of $G^{(i-1)}$.

Lemma 3.103: *A group is solvable if and only if $G^{(n)} = \{e\}$ for some $n \in \mathbb{N}$.*

PROOF: ($\Longrightarrow$) Suppose that G is solvable. Let $G_0, \ldots, G_n$ be a normal series for G. We claim that $G^{(n-i)} \subseteq G_i$. If this claim were true, then $G^{(n-0)} \subseteq G_0 = \{e\}$, and we would be done. We proceed by induction on $n - i \in \mathbb{N}$.

Inductive base: If $n - i = 0$, then $G^{(n-i)} = G = G_n$.

Inductive hypothesis: Assume that the assertion holds for $n - i$.

Inductive step: By definition, $G^{(n-i+1)} = \left(G^{(n-i)}\right)'$. By the inductive hypothesis, $G^{(n-i)} \subseteq G_i$; by Lemma 3.101, $\left(G^{(n-i)}\right)' \subseteq G_i'$. Hence

$$G^{(n-i+1)} \subseteq G_i'. \tag{7}$$

Recall from the properties of a normal series that G_i/G_{i-1} is abelian; for any $x, y \in G_i$, we have

$$(xy)G_{i-1} = \left(xG_{i-1}\right)\left(yG_{i-1}\right) = \left(yG_{i-1}\right)\left(xG_{i-1}\right) = (yx)G_{i-1}.$$

By Lemma 3.29 on page 62, $(yx)^{-1}(xy) \in G_{i-1}$; in other words, $[x,y] = x^{-1}y^{-1}xy \in G_{i-1}$. Since x and y were arbitrary in G_i, we have $G_i' \subseteq G_{i-1}$. Along with (7), this implies that $G^{(n-(i-1))} = G^{(n-i+1)} \subseteq G_{i-1}$.

We have shown the claim; thus, $G^{(n)} = \{e\}$ for some $n \in \mathbb{N}$.

($\Longleftarrow$) Suppose that $G^{(n)} = \{e\}$ for some $n \in \mathbb{N}$. We have

$$\{e\} = G^{(n)} < G^{(n-1)} < \cdots < G^{(0)} = G.$$

By Lemma 3.100, the subgroups form a normal series; that is,

$$\{e\} = G^{(n)} \triangleleft G^{(n-1)} \triangleleft \cdots \triangleleft G^{(0)} = G$$

and G_i/G_{i-1} is abelian for each $i = 1, \ldots, n$. □

We can now prove Theorem 3.97.

PROOF OF THEOREM 3.97: Let $H < G$. Assume G is solvable; by Lemma 3.103, $G^{(n)} = \{e\}$. By Lemma (3.101), $H^{(i)} \subseteq G^{(i)}$ for all $n \in \mathbb{N}$, so $H^{(n)} \subseteq \{e\}$. By the definition of a group, $H^{(n)} \supseteq \{e\}$, so the two are equal. By the same lemma, H is solvable. □

Exercises.

Exercise 3.104: Explain why Ω_n is solvable for any $n \in \mathbb{N}^+$.

Exercise 3.105: Show that if $H \subseteq G$, then $H' \subseteq G'$.

Exercise 3.106: Show that D_n is solvable for all $n \geq 3$.

Exercise 3.107: Show that Q_8 is solvable.

Exercise 3.108: In the textbook *God Created the Integers...* the theoretical physicist Stephen Hawking reprints, with commentary, some of the greatest mathematical results in history. One excerpt is from Evariste Galois' *Memoirs* on the solvability of polynomials by radicals. Hawking sums it up this way.

> To be brief, Galois demonstrated that the general polynomial of degree n could be solved by radicals if and only if every subgroup N of the group of permutations S_n is a normal subgroup. Then he demonstrated that every subgroup of S_n is normal for all $n \leq 4$ but not for any $n > 5$.
>
> —p. 105

Unfortunately, Hawking's explanation is completely wrong, and this exercise leads you towards an explanation as to why.[19] You have not yet studied the groups of permutations S_n, but you will learn in Section 5.1 that the group S_3 is really the same as D_3.[20] (To be precise, Exercise 5.31 asks you to show that $S_3 \cong D_3$.) So we will look at D_3, instead.

(a) Find all six subgroups of D_3.
(b) It is known that the general polynomial of degree 3 can be solved by radicals. According to the quote above, what must be true about all the subgroups of D_3?
(c) Why is Hawking's explanation of Galois' result "obviously" wrong?

[19] Perhaps Hawking was trying to simplify what Galois actually showed, and went too far. (I've done much worse in my lifetime.) In fact, Galois showed that a polynomial of degree n could be solved by radicals if and only if a corresponding group, now called its **Galois group,** was a solvable group. He then showed that the Galois group of $x^5 + 2x + 5$ was not a solvable group.

[20] To resurrect a term we used with monoids, S_3 is isomorphic to D_3. We will talk about group isomorphisms in the very next chapter.

Chapter 4:
Isomorphisms

We have on occasion observed that different groups have the same Cayley table. We have also talked about different groups having the same structure: regardless of whether a group of order two is additive or multiplicative, its elements behave in exactly the same fashion. The groups may look superficially different because of their elements and operations, but the "group behavior" is identical.

As we saw in Chapter 1, algebraists describe such a relationship between two monoids as *isomorphic*. Isomorphism for groups has the same intuitive meaning as isomorphism for monoids:

If two groups G and H have identical group structure,
we say that G and H are *isomorphic*.[21]

However, striking differences exist in the details. We want to study isomorphism of groups in quite a bit of detail, so to define isomorphism precisely, we start by reconsidering another topic that you studied in the past, functions. There we will also introduce the related notion of *homomorphism*.[22] This is the focus of Section 4.1. Section 4.2 lists some results that should help convince you that the existence of an isomorphism does, in fact, show that two groups have an identical group structure. Section 4.3 describes how we can create new isomorphisms from a homomorphism's *kernel*, a special subgroup defined by a homomorphism. Section 4.4 introduces a class of isomorphism that is important for later applications, an *automorphism*.

4.1: Homomorphisms

It turns out that we don't need quite so much to obtain an isomorphism with groups. It will take us a little bit to work into it; the key idea is that the operation is preserved. Although we worked this into the definition of a monoid isomorphism, here we will put it in the spotlight.

Definition 4.1: Let G, H be groups and $f : G \to H$ a function. We say that f is a **group homomorphism** from G to H if it satisfies the property that $f(x)f(y) = f(xy)$ for every $x, y \in G$.

Notation 4.2: As with monoids, you have to be careful with the fact that different groups have different operations. Depending on the context, the proper way to describe the homomorphism property may be

- $f(xy) = f(x) + f(y)$;
- $f(x + y) = f(x)f(y)$;

[21] The word comes Greek words that mean *identical shape*.

[22] The word comes Greek words that mean *common shape*. Here the *shape* that remains *common* is the effect of the operation on the elements of the group. The function shows that the group operation behaves the same way on elements of the range as on elements of the domain.

- $f(x \circ y) = f(x) \odot f(y)$;
- etc.

Example 4.3: A trivial example of a homomorphism, but an important one, is the identity function $\iota : G \to G$ by $\iota(g) = g$ for all $g \in G$. It should be clear that this is a homomorphism, since for all $g, h \in G$ we have

$$\iota(gh) = gh = \iota(g)\iota(h).$$

For a non-trivial homomorphism, let $f : \mathbb{Z} \to 2\mathbb{Z}$ by $f(x) = 4x$. Then f is a group homomorphism, since for any $x \in \mathbb{Z}$ we have

$$f(x) + f(y) = 4x + 4y = 4(x+y) = f(x+y). \triangle$$

The homomorphism property should remind you of certain special functions and operations that you have studied in Linear Algebra or Calculus. Recall from Exercise 2.28 that $\mathbb{R}^+$, the set of all positive real numbers, is a multiplicative group.

Example 4.4: Let $f : (GL_m(\mathbb{R}), \times) \to (\mathbb{R}^+, \times)$ by $f(A) = |\det A|$. An important fact from Linear Algebra tells us that for any two square matrices A and B, $\det A \cdot \det B = \det(AB)$. Thus

$$f(A) \cdot f(B) = |\det A| \cdot |\det B| = |\det A \cdot \det B| = |\det(AB)| = f(AB),$$

implying that f is a homomorphism of groups. $\triangle$

Let's look at a clockwork group that we studied in the previous section.

Example 4.5: Let $n \in \mathbb{Z}$ such that $n > 1$, and let $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ by the assignment $f(x) = [x]_n$. We claim that f is a homomorphism. *Why?* From Lemma 3.82, we know that for any $x, y \in \mathbb{Z}_n$, $f(x+y) = [x+y]_n = [x]_n + [y]_n = f(x) + f(y)$. $\triangle$

Preserving the operation guarantees that a homomorphism tells us an enormous amount of information about a group. If there is a homomorphism f from G to H, then elements of the **image of** G,

$$f(G) = \{h \in H : \exists g \in G \text{ such that } f(g) = h\}$$

act the same way as their preimages in G.

This does *not* imply that the *group structure* is the same. In Example 4.5, for example, f is a homomorphism from an infinite group to a finite group; even if the group operations behave in a similar way, the groups themselves are inherently different. If we can show that the groups have the same "size" in addition to a similar operation, then the groups are, for all intents and purposes, identical.

How do we decide that two groups have the same size? For finite groups, this is "easy": count the elements. We can't do that for infinite groups, so we need something a little more general.[23]

[23] The standard method in set theory of showing that two sets are the same "size" is to show that there exists a one-to-one, onto function between the sets. For example, one can use this definition to show that $\mathbb{Z}$ and $\mathbb{Q}$ are the same size, but $\mathbb{Z}$ and $\mathbb{R}$ are not. So an isomorphism is a homomorphism that also shows that two sets are the same size.

Definition 4.6: Let $f : G \to H$ be a homomorphism of groups. If f is one-to-one and onto, then f is an **isomorphism** and the groups G and H are **isomorphic**. ◿

Notation 4.7: If the groups G and H are isomorphic, we write $G \cong H$.

Example 4.8: Recall the homomorphisms of Example 4.3,

$$\iota : G \to G \quad \text{by} \quad \iota(g) = g \qquad \text{and} \qquad f : \mathbb{Z} \to 2\mathbb{Z} \quad \text{by} \quad f(x) = 4x.$$

First we show that ι is an isomorphism. We already know it's a homomorphism, so we need only show that it's one-to-one and onto.

one-to-one: Let $g, h \in G$. Assume that $\iota(g) = \iota(h)$. By definition of ι, $g = h$. Since g and h were arbitrary in G, ι is one-to-one.

onto: Let $g \in G$. We need to find $x \in G$ such that $\iota(x) = g$. Using the definition of ι, $x = g$ does the job. Since g was arbitrary in G, ι is onto.

Now we show that f is one-to-one, but not onto.

one-to-one: Let $a, b \in \mathbb{Z}$. Assume that $f(a) = f(b)$. By definition of f, $4a = 4b$. Then $4(a-b) = 0$; by the zero product property of the integers, $4 = 0$ or $a - b = 0$. Since $4 \neq 0$, we must have $a - b = 0$, or $a = b$. We assumed $f(a) = f(b)$ and showed that $a = b$. Since a and b were arbitrary, f is one-to-one.

***not** onto:* There is no element $a \in \mathbb{Z}$ such that $f(a) = 2$. If there were, $4a = 2$. The only possible solution to this equation is $a = 1/2 \notin \mathbb{Z}$. ◿

Example 4.9: Recall the homomorphism of Example 4.4,

$$f : \mathrm{GL}_m(\mathbb{R}) \to \mathbb{R}^+ \quad \text{by} \quad f(A) = |\det A|.$$

We claim that f is onto, but not one-to-one.

That f is not one-to-one: Observe that f maps both of the following two diagonal matrices to 2, even though the matrices are unequal:

$$A = \begin{pmatrix} 2 & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & & & & \\ & 2 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & \ddots \end{pmatrix}.$$

(Unmarked entries are zeroes.)

That f is onto: Let $x \in \mathbb{R}^+$; then $f(A) = x$ where A is the diagonal matrix

$$A = \begin{pmatrix} x & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots \end{pmatrix}.$$

(Again, unmarked entries are zeroes.) ◿

We *cannot* conclude from these examples that $\mathbb{Z} \ncong 2\mathbb{Z}$ and that $\mathbb{R}^+ \ncong \mathbb{R}^{m\times n}$. *Why not?* In each case, we were considering only one of the (possibly many) homomorphisms. It is quite possible that a different homomorphism would show that $\mathbb{Z} \cong 2\mathbb{Z}$ and that $\mathbb{R}^+ \cong \mathbb{R}^{m\times n}$. You will show in the exercises that the first assertion is in fact true, while the second is not.

We conclude this chapter with three important properties of homomorphisms. This result lays the groundwork for important results in later sections, and is generally useful.

Theorem 4.10: *Let $f : G \to H$ be a homomorphism of groups. Denote the identity of G by e_G, and the identity of H by e_H. Then f*
preserves identities: $f(e_G) = e_H$; *and*
preserves inverses: *for every $x \in G$, $f\left(x^{-1}\right) = f(x)^{-1}$.*

Theorem 4.10 applies of course to isomorphisms as well. It might not seem interesting that, if the operation's behavior is preserved, the identity is mapped to the identity, and inverses are mapped to inverses. However, this is *not* true for monoids, which is why the definition of a monoid isomorphism required that the identity be preserved (page 18). You should think carefully about the proof below, and identify precisely why this theorem holds for groups, but not for monoids.

PROOF: *That f preserves identities:* Let $x \in G$, and $y = f(x)$. By the property of homomorphisms,

$$e_H y = y = f(x) = f(e_G x) = f(e_G) f(x) = f(e_G) y.$$

By the transitive property of equality,

$$e_H y = f(e_G) y.$$

Multiply both sides of the equation *on the right* by y^{-1} to obtain

$$e_H = f(e_G).$$

That f preserves inverses: Let $x \in G$. By the property of homomorphisms and by the fact that f preserves identity,

$$e_H = f(e_G) = f\left(x \cdot x^{-1}\right) = f(x) \cdot f\left(x^{-1}\right).$$

Thus

$$e_H = f(x) \cdot f\left(x^{-1}\right).$$

Pay careful attention to what this equation says! Since the product of $f(x)$ and $f\left(x^{-1}\right)$ is the identity, those two elements must be inverses! Hence $f\left(x^{-1}\right)$ is the inverse of $f(x)$, which we write as

$$f\left(x^{-1}\right) = f(x)^{-1}.$$

□

Corollary 4.11: *Let $f : G \to H$ be a homomorphism of groups. Then $f\left(x^{-1}\right)^{-1} = f(x)$ for every $x \in G$.*

PROOF: You do it! See Exercise 4.25. □

It will probably not surprise you that homomorphisms preserve powers of an element.

Theorem 4.12: *Let $f : G \to H$ be a homomorphism of groups. Then f preserves powers of elements of G. That is, if $f(g) = h$, then $f(g^n) = f(g)^n = h^n$.*

PROOF: You do it! See Exercise 4.28. □

Naturally, if homomorphisms preserve powers of an element, they must also preserve cyclic groups.

Corollary 4.13: *Let $f : G \to H$ be a homomorphism of groups. If $G = \langle g \rangle$ is a cyclic group, then $f(g)$ determines f completely. In other words, the image $f(G)$ is a cyclic group, and $f(G) = \langle f(g) \rangle$.*

PROOF: We have to show that two sets are equal. Recall that, since G is cyclic, for any $x \in G$ there exists $n \in \mathbb{Z}$ such that $x = g^n$.

First we show that $f(G) \subseteq \langle f(g) \rangle$. Let $y \in f(G)$ and choose $x \in G$ such that $y = f(x)$. Choose $n \in \mathbb{Z}$ such that $x = g^n$. By substitution and Theorem 4.12, $y = f(x) = f(g^n) = f(g)^n$. Hence $y \in \langle f(g) \rangle$. Since y was arbitrary in $f(G)$, $f(G) \subseteq \langle f(g) \rangle$.

Now we show that $f(G) \supseteq \langle f(g) \rangle$. Let $y \in \langle f(g) \rangle$, and choose $n \in \mathbb{Z}$ such that $y = f(g)^n$. By Theorem 4.12, $y = f(g^n)$. Since $g^n \in G$, $f(g^n) \in f(G)$, so $y \in f(G)$. Since y was arbitrary in $\langle f(g) \rangle$, $f(G) \supseteq \langle f(g) \rangle$.

We have shown that $f(G) \subseteq \langle f(g) \rangle$ and $f(G) \supseteq \langle f(g) \rangle$. By equality of sets, $f(G) = \langle f(g) \rangle$. □

We need one last definition, related to something you should have seen in linear algebra. It will prove important in subsequent sections and chapters.

Definition 4.14: Let G and H be groups, and $f : G \to H$ a homomorphism. Let

$$Z = \{g \in G : f(g) = e_H\};$$

that is, Z is the set of all elements of G that f maps to the identity of H. We call Z the **kernel** of f, written $\ker f$.

Theorem 4.15: *Let $f : G \to H$ be a homomorphism of groups. Then $\ker f \triangleleft G$.*

PROOF: You do it! See Exercise 4.32. □

Exercises.

Example 4.16: Suppose f is an isomorphism. What is $\ker f$?

Exercise 4.17:
(a) Show that $f : \mathbb{Z} \to 2\mathbb{Z}$ by $f(x) = 2x$ is an isomorphism. Hence $\mathbb{Z} \cong 2\mathbb{Z}$.
(b) Show that $\mathbb{Z} \cong n\mathbb{Z}$ for every nonzero integer n.

Exercise 4.18: Let $n \geq 1$ and $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ by $f(a) = [a]_n$.
(a) Show that f is a homomorphism.
(b) Explain why f cannot possibly be an isomorphism.
(c) Determine $\ker f$. (It might help to use a specific value of n first.)
(d) Indicate how we know that $\mathbb{Z}/\ker f \cong \mathbb{Z}_n$. (Eventually, we will show that $G/\ker f \cong H$ for *any* homomorphism $f : G \longrightarrow H$ that is onto.)

Exercise 4.19: Show that $\mathbb{Z}_2$ is isomorphic to the group of order two from Example 2.8 on page 27. *Caution!* Notice that the first group is usually written using addition, but the second group is multiplicative. Your proof should observe these distinctions.

Exercise 4.20: Show that $\mathbb{Z}_2$ is isomorphic to the Boolean xor group of Exercise 2.19 on page 30. *Caution!* Remember to denote the operation in the Boolean xor group correctly.

Exercise 4.21: Show that $\mathbb{Z}_n \cong \Omega_n$ for $n \in \mathbb{N}^+$.

Exercise 4.22: Suppose we try to define $f : Q_8 \longrightarrow \Omega_4$ by $f(\mathbf{i}) = f(\mathbf{j}) = f(\mathbf{k}) = i$, and $f(\mathbf{xy}) = f(\mathbf{x})f(\mathbf{y})$ for all other $\mathbf{x}, \mathbf{y} \in Q_8$. Show that f is *not* a homomorphism.

Exercise 4.23: Show that $\mathbb{Z}$ is isomorphic to $\mathbb{Z}_0$. (Because of this, people generally don't pay attention to $\mathbb{Z}_0$.)

Exercise 4.24: Recall the subgroup L of $\mathbb{R}^2$ from Exercises 3.15 on page 58, 3.34 on page 63, and 3.68 on page 71. Show that $L \cong \mathbb{R}$.

Exercise 4.25: Prove Corollary 4.11.

Exercise 4.26: Let φ be a homomorphism from a finite group G to a group H. Recall from Exercise 4.32 that $\ker\varphi \triangleleft G$. Explain why $|\ker\varphi| \cdot |\varphi(G)| = |G|$. (This is sometimes called **the Homomorphism Theorem**.)

Exercise 4.27: Let $f : G \to H$ be an isomorphism. Isomorphisms are by definition one-to-one functions, so f has an inverse function f^{-1}. Show that $f^{-1} : H \to G$ is also an isomorphism.

Exercise 4.28: Prove Theorem 4.12.

Exercise 4.29: Let $f : G \to H$ be a homomorphism of groups. Assume that G is abelian.
(a) Show that $f(G)$ is abelian.
(b) Is H abelian? Explain why or why not.

Exercise 4.30: Let $f : G \to H$ be a homomorphism of groups. Let $A < G$. Show that $f(A) < H$.

Exercise 4.31: Let $f : G \to H$ be a homomorphism of groups. Let $A \triangleleft G$.
(a) Show that $f(A) \triangleleft f(G)$.
(b) Do you think that $f(A) \triangleleft H$? Justify your answer.

Exercise 4.32: Prove Theorem 4.15.

Exercise 4.33: Show that if G is a group, then $G/\{e\} \cong G$ and $G/G \cong \{e\}$.

Exercise 4.34: In Chapter 1, the definition of an isomorphism for *monoids* required that the function map the identity to the identity (Definition 1.56 on page 18). By contrast, Theorem 4.10 shows that the preservation of the operation guarantees that a group homomorphism maps the identity to the identity, so we don't need to require this in the definition of an isomorphism for *groups* (Definition 4.6).

The difference between a group and a monoid is the existence of an inverse. Use this to show that, in a monoid, you *can* have a function that preserves the operation, but not the identity. In other words, show that Theorem 4.10 is false for monoids.

4.2: Consequences of isomorphism

Throughout this section, G and H are groups.

The purpose of this section is to show why we use the name *isomorphism:* if two groups are isomorphic, then they are indistinguishable *as groups*. The elements of the sets are different, and the operation may be defined differently, but as groups the two are identical. Suppose that two groups G and H are isomorphic. We will show that

- isomorphism is an equivalence relation;
- G is abelian iff H is abelian;
- G is cyclic iff H is cyclic;
- every subgroup A of G corresponds to a unique subgroup A' of H (in particular, if A is of order n, so is A');
- every normal subgroup N of G corresponds to a unique normal subgroup N' of H;
- the quotient group G/N corresponds to a quotient group H/N'.

All of these depend on the existence of an isomorphism $f : G \to H$. In particular, uniqueness is guaranteed only for any one isomorphism; if two different isomorphisms f, f' exist between G and H, then a subgroup A of G may well correspond to two distinct subgroups B and B' of H.

The fact that isomorphism is an equivalence relation will prove helpful with the equivalence properties; for example, "G is cyclic iff H is cyclic." So, we start with that one first.

Theorem 4.35: *Isomorphism is an equivalence relation. That is, $\cong$ satisfies the reflexive, symmetric, and transitive properties.*

PROOF: First we show that $\cong$ is reflexive. Let G be any group, and let ι be the identity homomorphism from Example 4.3. We showed in Example 4.8 that ι is an isomorphism. Since $\iota : G \to G$, $G \cong G$. Since G was an arbitrary group, $\cong$ is reflexive.

Next, we show that $\cong$ is symmetric. Let G, H be groups and assume that $G \cong H$. By definition, there exists an isomorphism $f : G \to H$. By Exercise 4.27, f^{-1} is also a isomorphism. Hence $H \cong G$.

Finally, we show that $\cong$ is transitive. Let G, H, K be groups and assume that $G \cong H$ and $H \cong K$. By definition, there exist isomorphisms $f : G \to H$ and $g : H \to K$. Define $h : G \to K$ by

$$h(x) = g(f(x)).$$

We claim that h is an isomorphism. We show each requirement in turn:

That h is a homomorphism, let $x, y \in G$. By definition of h, $h(x \cdot y) = g(f(x \cdot y))$. Applying the fact that g and f are both homomorphisms,

$$h(x \cdot y) = g(f(x \cdot y)) = g(f(x) \cdot f(y)) = g(f(x)) \cdot g(f(y)) = h(x) \cdot h(y).$$

Thus h is a homomorphism.

That h is one-to-one, let $x, y \in G$ and assume that $h(x) = h(y)$. By definition of h,

$$g(f(x)) = g(f(y)).$$

Now f is an isomorphism, so by definition it is one-to-one, and by definition of one-to-one

$$g(x) = g(y).$$

Similarly g is an isomorphism, so $x = y$. Since x and y were arbitrary in G, h is one-to-one.

That h is onto, let $z \in K$. We claim that there exists $x \in G$ such that $h(x) = z$. Since g is an isomorphims, it is by definition onto, so there exists $y \in H$ such that $g(y) = z$. Since f is an isomorphism, there exists $x \in G$ such that $f(x) = y$. Putting this together with the definition of h, we see that

$$z = g(y) = g(f(x)) = h(x).$$

Since z was arbitrary in K, h is onto.

We have shown that h is a one-to-one, onto homorphism. Thus h is an isomorphism, and $G \cong K$. □

Theorem 4.36: *Suppose that $G \cong H$. Then G is abelian iff H is abelian.*

PROOF: Let $f : G \to H$ be an isomorphism. Assume that G is abelian. We must show that H is abelian. By Exercise 4.29, $f(G)$ is abelian. Since f is an isomorphism, and therefore onto, $f(G) = H$. Hence H is abelian.

Since isomorphism is symmetric, $H \cong G$. Along with the above argument, this implies that if H is abelian, then G is, too.

Hence, G is abelian iff H is abelian. □

Theorem 4.37: *Suppose $G \cong H$. Then G is cyclic iff H is cyclic.*

PROOF: Let $f : G \to H$ be an isomorphism. Assume that G is cyclic. We must show that H is cyclic; that is, we must show that every element of H is generated by a fixed element of H.

Since G is cyclic, by definition $G = \langle g \rangle$ for some $g \in G$. Let $h = f(g)$; then $h \in H$. We claim that $H = \langle h \rangle$.

Let $x \in H$. Since f is an isomorphism, it is onto, so there exists $a \in G$ such that $f(a) = x$. Since G is cyclic, there exists $n \in \mathbb{Z}$ such that $a = g^n$. By Theorem 4.12,

$$x = f(a) = f(g^n) = f(g)^n = h^n.$$

Since x was an arbitrary element of H and x is generated by h, all elements of H are generated by h. Hence $H = \langle h \rangle$ is cyclic.

Since isomorphism is symmetric, $H \cong G$. Along with the above argument, this implies that if H is cyclic, then G is, too.

Hence, G is cyclic iff H is cyclic. □

Theorem 4.38: *Suppose $G \cong H$. Every subgroup A of G is isomorphic to a subgroup B of H. Moreover, each of the following holds. :*
(A) A is of finite order n iff B is of finite order n.
(B) A is normal iff B is normal.

PROOF: Let $f : G \to H$ be an isomorphism. Let A be a subgroup of G. By Exercise 4.30, $f(A) < H$.

First we show that $f(A)$ is a subgroup of H. Let $x, y \in f(A)$; by definition, $x = f(a)$ and $y = f(b)$ for some $a, b \in A$. Applying properties of homomorphisms (the definition of a homomorphism, and Theorem 4.10), we see that

$$xy^{-1} = f(a) f(b)^{-1} = f\left(ab^{-1}\right).$$

By closure, $ab^{-1} \in A$. So $xy^{-1} \in f(A)$, and the Subgroup Theorem implies that $f(A) < H$.

Now we claim that f is one-to-one and onto from A to $f(A)$. Onto is immediate from the definition of $f(A)$. The one-to-one property holds because f is one-to-one in G and $A \subseteq G$.

We have shown that $f(A) < H$ and that f is one-to-one and onto from A to $f(A)$. Hence $A \cong f(A)$.

Claim (A) follows from the fact that f is one-to-one and onto.

For claim (B), assume $A \triangleleft G$. We want to show that $B \triangleleft H$; that is, $xB = Bx$ for every $x \in H$. So let $x \in H$ and $y \in B$; since f is an isomorphism, it is onto, so $f(g) = x$ and $f(a) = y$ for some $g \in G$ and some $a \in A$. Then

$$xy = f(g) f(a) = f(ga).$$

Since $A \triangleleft G$, $gA = Ag$, so there exists $a' \in A$ such that $ga = a'g$. Let $y' = f(a')$. Thus

$$xy = f(a'g) = f(a') f(g) = y'x.$$

Notice that $y' \in f(A) = B$, so $xy = y'x \in Bx$.

We have shown that for arbitrary $x \in H$ and arbitrary $y \in B$, there exists $y' \in B$ such that $xy = y'x$. Hence $xB \subseteq Bx$. A similar argument shows that $xB \supseteq Bx$, so $xB = Bx$. This is the definition of a normal subgroup, so $B \triangleleft H$.

Since isomorphism is symmetric, $B \cong A$. Along with the above argument, this implies that if $B \triangleleft H$, then $A \triangleleft G$, as well.

Hence, A is normal iff B is normal. □

Theorem 4.39: *Suppose $G \cong H$ as groups. Every quotient group of G is isomorphic to a quotient group of H.*

We use Lemma 3.29(CE3) on page 62 on coset equality heavily in this proof; you may want to go back and review it.

PROOF: Let $f : G \to H$ be an isomorphism. Consider an arbitrary quotient group of G defined, by G/A, where $A \triangleleft G$. Let $B = f(A)$; by Theorem 4.38 $B \triangleleft H$, so H/B is a quotient group. We want to show that $G/A \cong H/B$.

Let $f_A : G/A \to H/B$ by

$$f_A(X) = f(g)B \qquad \text{where} \qquad X = gA \in G/A.$$

You might suspect that we only have to show that f_A is a one-to-one, onto homomorphism, but this is not true. We have to show first that f_A is well-defined. What does this mean?

Let X be any coset in G/A. It is usually the case that X can have more than one representation; that is, we can find $g \neq \widehat{g}$ where $X = gA = \widehat{g}A$. (For example, in D_3 we know that $\varphi A_3 = (\rho\varphi)A_3$ even though $\varphi \neq \rho\varphi$; see Example 3.58 on page 69.) If $f(g) \neq f(\widehat{g})$, then $f_A(X)$ would have more than one possible value, since

$$f_A(X) = f_A(gA) = f(g) \neq f(\widehat{g}) = f_A(\widehat{g}A) = f(X).$$

In other words, f_A would not be a function, since at least one element of the domain (X) would correspond to at least two elements of the range ($f(g)$ and $f(\widehat{g})$). See Figure 4.1. A homomorphism must first be a function, so if f_A is not even a function, then it is not well-defined.

That f_A is well-defined: Let $X \in G/A$ and consider two representations g_1A and g_2A of X. Then

$$f_A(g_1A) = f(g_1)B \quad \text{and} \quad f_A(g_2A) = f(g_2)B.$$

We must show that the cosets $f_A(g_1)B$ and $f_A(g_2)B$ are equal in H/B. By hypothesis, $g_1A = g_2A$. Lemma 3.29(CE3) implies that $g_2^{-1}g_1 \in A$. Recall that $f(A) = B$; this implies that

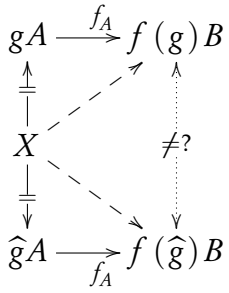


Figure 4.1. Mappings whose domains are quotient groups might not be functions: how do we know that $f(g) = f(\widehat{g})$? If not, then $f_A(X)$ could have two different values.

$f\left(g_2^{-1}g_1\right) \in B$. The homomorphism property implies that

$$f(g_2)^{-1} f(g_1) = f\left(g_2^{-1}\right) f(g_1) = f\left(g_2^{-1}g_1\right) \in B.$$

Lemma 3.29(CE3) again implies that $f(g_1)B = f(g_2)B$. In other words,

$$f_A(X) = f(g_1)B = f(g_2)B$$

so there is no ambiguity in the definition of f_A as to the image of X in H/B; the function is well-defined.

That f_A is a homomorphism: Let $X, Y \in G/A$ and write $X = g_1A$ and $Y = g_2A$ for appropriate $g_1, g_2 \in G$. Now

$$\begin{aligned} f_A(XY) &= f_A((g_1A)\cdot(g_2A)) \\ &= f_A(g_1g_2\cdot A) \\ &= f(g_1g_2)B \\ &= (f(g_1)f(g_2))\cdot B \\ &= f(g_1)A'\cdot f(g_2)B \\ &= f_A(g_1A)\cdot f_A(g_2A) \\ &= f_A(X)\cdot f_A(Y) \end{aligned}$$

where each equality is justified by (respectively) the definitions of X and Y; the definition of coset multiplication in G/A; the definition of f_A; the homomorphism property of f; the definition of coset multiplication in H/B; the definition of f_A; and the definitions of X and Y. The chain of equalities shows clearly that f_A is a homomorphism.

That f_A is one-to-one: Let $X, Y \in G/A$ and assume that $f_A(X) = f_A(Y)$. Let $g_1, g_2 \in G$

such that $X = g_1A$ and $Y = g_2A$. The definition of f_A implies that

$$f(g_1)B = f_A(X) = f_A(Y) = f(g_2)B,$$

so by Lemma 3.29(CE3) $f(g_2)^{-1} f(g_1) \in B$. Recall that $B = f(A)$, so there exists $a \in A$ such that $f(a) = f(g_2)^{-1} f(g_1)$. The homomorphism property implies that

$$f(a) = f\left(g_2^{-1}\right) f(g_1) = f\left(g_2^{-1} g_1\right).$$

Recall that f is an isomorphism, hence one-to-one. The definition of one-to-one implies that

$$g_2^{-1} g_1 = a \in A.$$

Applying Lemma 3.29(CE3) again gives us $g_1A = g_2A$, and

$$X = g_1A = g_2A = Y.$$

We took arbitrary $X, Y \in G/A$ and showed that if $f_A(X) = f_A(Y)$, then $X = Y$. It follows that f_A is one-to-one.

That f_A is onto: You do it! See Exercise 4.40. □

Exercises.

Exercise 4.40: Show that the function f_A defined in the proof of Theorem 4.39 is onto.

Exercise 4.41: Recall from Exercise 2.58 on page 47 that $\langle \mathbf{i} \rangle$ is a cyclic group of Q_8.

(a) Show that $\langle \mathbf{i} \rangle \cong \mathbb{Z}_4$ by giving an explicit isomorphism.

(b) Let A be a proper subgroup of $\langle \mathbf{i} \rangle$. Find the corresponding subgroup of $\mathbb{Z}_4$.

(c) Use the proof of Theorem 4.39 to determine the quotient group of $\mathbb{Z}_4$ to which $\langle \mathbf{i} \rangle / A$ is isomorphic.

Exercise 4.42: Recall from Exercise 4.24 on page 86 that the set

$$L = \left\{ x \in \mathbb{R}^2 : \; x = (a, a) \; \exists a \in \mathbb{R} \right\}$$

defined in Exercise 3.15 on page 58 is isomorphic to $\mathbb{R}$.

(a) Show that $\mathbb{Z} \triangleleft \mathbb{R}$.

(b) Give the precise definition of $\mathbb{R}/\mathbb{Z}$.

(c) Explain why we can think of $\mathbb{R}/\mathbb{Z}$ as the set of classes $[a]$ such that $a \in [0, 1)$. Choose one such $[a]$ and describe the elements of this class.

(d) Find the subgroup H of L that corresponds to $\mathbb{Z} < \mathbb{R}$. What do this section's theorems imply that you can conclude about H and L/H?

(e) Use the homomorphism f_A defined in the proof of Theorem 4.39 to find the images $f_{\mathbb{Z}}(\mathbb{Z})$ and $f_{\mathbb{Z}}(\pi + \mathbb{Z})$.

(f) Use the answer to (c) to describe L/H intuitively. Choose an element of L/H and describe the elements of this class.

4.3: The Isomorphism Theorem

In this section, we identify an important relationship between a subgroup $A < G$ that has a special relationship to a homomorphism, and the image of the quotient group $f(G/A)$. First, an example.

Example 4.43: Recall $A_3 = \{\iota, \rho, \rho^2\} \triangleleft D_3$ from Example 3.58. We saw that D_3/A_3 has only two elements, so it must be isomorphic to the group of two elements. First we show this explicitly: Let $\mu : D_3/A_3 \to \mathbb{Z}_2$ by

$$\mu(X) = \begin{cases} 0, & X = A_3; \\ 1, & \text{otherwise.} \end{cases}$$

Is μ a homomorphism? Recall that A_3 is the identity element of D_3/A_3, so for any $X \in D_3/A_3$

$$\mu(X \cdot A_3) = \mu(X) = \mu(X) + 0 = \mu(X) + \mu(A_3).$$

This verifies the homomorphism property for all products in the Cayley table of D_3/A_3 except $(\varphi A_3) \cdot (\varphi A_3)$, which is easy to check:

$$\mu((\varphi A_3) \cdot (\varphi A_3)) = \mu(A_3) = 0 = 1 + 1 = \mu(\varphi A_3) + \mu(\varphi A_3).$$

Hence μ is a homomorphism. The property of isomorphism follows from the facts that

- $\mu(A_3) \neq \mu(\varphi A_3)$, so μ is one-to-one, and
- both 0 and 1 have preimages, so μ is onto.

Notice further that $\ker \mu = A_3$.

Something subtle is at work here. Let $f : D_3 \to \mathbb{Z}_2$ by

$$f(x) = \begin{cases} 0, & x \in A_3; \\ 1, & \text{otherwise.} \end{cases}$$

Is f a homomorphism? The elements of A_3 are ι, ρ, and ρ^2; f maps these elements to zero, and the other three elements of D_3 to 1. Let $x, y \in D_3$ and consider the various cases:

Case 1. $x, y \in A_3$.

Since A_3 is a group, closure implies that $xy \in A_3$. Thus

$$f(xy) = 0 = 0 + 0 = f(x) + f(y).$$

Case 1. $x \in A_3$ and $y \notin A_3$.

Since A_3 is a group, closure implies that $xy \notin A_3$. (Otherwise $xy = z$ for some $z \in A_3$, and multiplication by the inverse implies that $y = x^{-1}z \in A_3$, a contradiction.) Thus

$$f(xy) = 1 = 0 + 1 = f(x) + f(y).$$

Case 1. $x \notin A_3$ and $y \in A_3$.

An argument similar to the case above shows that $f(xy) = f(x) + f(y)$.

Case 1. $x, y \notin A_3$.

Inspection of the Cayley table of D_3 (Exercise 2.43 on page 39) shows that $xy \in A_3$. Hence

$$f(xy) = 0 = 1 + 1 = f(x) + f(y).$$

We have shown that f is a homomorphism from D_3 to $\mathbb{Z}_2$. Again, $\ker f = A_3$.

In addition, consider the function $\eta : D_3 \to D_3/A_3$ by

$$\eta(x) = \begin{cases} A_3, & x \in A_3; \\ \varphi A_3, & \text{otherwise.} \end{cases}$$

It is easy to show that this is a homomorphism; we do so presently.

Now comes the important observation: Look at the composition function $\eta \circ \mu$ whose domain is D_3 and whose range is $\mathbb{Z}_2$:

$$\begin{aligned}
(\mu \circ \eta)(\iota) &= \mu(\eta(\iota)) = \mu(A_3) = 0; \\
(\mu \circ \eta)(\rho) &= \mu(\eta(\rho)) = \mu(A_3) = 0; \\
(\mu \circ \eta)\left(\rho^2\right) &= \mu\left(\eta\left(\rho^2\right)\right) = \mu(A_3) = 0; \\
(\mu \circ \eta)(\varphi) &= \mu(\eta(\varphi)) = \mu(\varphi A_3) = 1; \\
(\mu \circ \eta)(\rho\varphi) &= \mu(\eta(\rho\varphi)) = \mu(\varphi A_3) = 1; \\
(\mu \circ \eta)\left(\rho^2\varphi\right) &= \mu\left(\eta\left(\rho^2\varphi\right)\right) = \mu(\varphi A_3) = 1.
\end{aligned}$$

We have

$$(\mu \circ \eta)(x) = \begin{cases} 0, & x \in A_3; \\ 1, & \text{otherwise,} \end{cases}$$

or in other words

$$\mu \circ \eta = f. \measuredangle$$

This remarkable correspondence can make it easier to study quotient groups G/A:

- find a group H that is "easy" to work with; and
- find a homomorphism $f : G \to H$ such that
  - $f(g) = e_H$ for all $g \in A$, and
  - $f(g) \neq e_H$ for all $g \notin A$.

If we can do this, then $H \cong G/A$, and as we saw in Section 4.2 studying G/A is equivalent to studying H.

The reverse is also true: suppose that a group G and its quotient groups are relatively easy to study, whereas another group H is difficult. The isomorphism theorem helps us identify a quotient group G/A that is isomorphic to H, making it easier to study.

We need to formalize this observation in a theorem, but first we have to confirm something that we claimed earlier:

Lemma 4.44: *Let G be a group and $A \triangleleft G$. The function $\eta : G \to G/A$ by*

$$\eta(g) = gA$$

is a homomorphism.

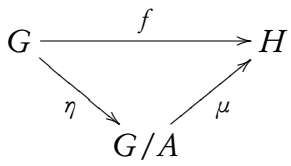
PROOF: You do it! See Exercise 4.47. □

Definition 4.45: We call the homomorphism η of Lemma 4.44 the **natural homomorphism**.

Recall the definition of a kernel (Theorem 4.15 on page 85). We can use this to formalize the observation of Example 4.43.

Theorem 4.46 (The Isomorphism Theorem): *Let G and H be groups, and $A \triangleleft G$. Let $\eta : G \to G/A$ be the natural homomorphism. If there exists a homomorphism $f : G \to H$ such that f is onto and $\ker f = A$, then $G/A \cong H$. Moreover, the isomorphism $\mu : G/A \to H$ satisfies $f = \mu \circ \eta$.*

We can illustrate Theorem 4.46 by the following diagram:



The idea is that "the diagram commutes", or $f = \mu \circ \eta$.

PROOF: We are given G, H, A, and η. Assume that there exists a homomorphism $f : G \to H$ such that $\ker f = A$. Define $\mu : G/A \to H$ in the following way:

$$\mu(X) = f(g), \text{ where } X = gA.$$

We claim that μ is an isomorphism from G/A to H, and moreover that $f = \mu \circ \eta$.

Since the domain of μ consists of cosets which may have different representations, we must show first that μ is well-defined. Suppose that $X \in G/A$ has two representations $X = gA = g'A$ where $g, g' \in G$ and $g \neq g'$. We need to show that $\mu(gA) = \mu(g'A)$. From Lemma 3.29(CE3), we know that $g^{-1}g' \in A$, so there exists $a \in A$ such that $g^{-1}g' = a$, so $g' = ga$. Applying the definition of μ and the homomorphism property,

$$\mu(g'A) = f(g') = f(ga) = f(g)f(a).$$

Recall that $a \in A = \ker f$, so $f(a) = e_H$. Substitution gives

$$\mu\left(g'A\right) = f(g) \cdot e_H = f(g) = \mu(gA).$$

Hence $\mu\left(g'A\right) = \mu(gA)$ and $\mu(X)$ is well-defined.

Is μ a homomorphism? Let $X, Y \in G/A$; we can represent $X = gA$ and $Y = g'A$ for some $g, g' \in G$. Applying the homomorphism property of f, we see that

$$\mu(XY) = \mu\left((gA)\left(g'A\right)\right) = \mu\left(\left(gg'\right)A\right) = f\left(gg'\right) = f(g) f\left(g'\right) = \mu(gA)\,\mu\left(g'A\right).$$

Thus μ is a homomorphism.

Is μ one-to-one? Let $X, Y \in G/A$ and assume that $\mu(X) = \mu(Y)$. Represent $X = gA$ and $Y = g'A$ for some $g, g' \in G$; by the homomorphism property of f, we see that

$$\begin{aligned} f\left(g^{-1}g'\right) &= f\left(g^{-1}\right) f\left(g'\right) \\ &= f(g)^{-1} f\left(g'\right) \\ &= \mu(gA)^{-1}\,\mu\left(g'A\right) \\ &= \mu(X)^{-1}\,\mu(Y) \\ &= \mu(Y)^{-1}\,\mu(Y) \\ &= e_H, \end{aligned}$$

so $g^{-1}g' \in \ker f$. It is given that $\ker f = A$, so $g^{-1}g' \in A$. Lemma 3.29(CE3) now tells us that $gA = g'A$, so $X = Y$. Thus μ is one-to-one.

Is μ onto? Let $h \in H$; we need to find an element $X \in G/A$ such that $\mu(X) = h$. It is given that f is onto, so there exists $g \in G$ such that $f(g) = h$. Then

$$\mu(gA) = f(g) = h,$$

so μ is onto.

We have shown that μ is an isomorphism; we still have to show that $f = \mu \circ \eta$, but the definition of μ makes this trivial: for any $g \in G$,

$$(\mu \circ \eta)(g) = \mu(\eta(g)) = \mu(gA) = f(g).$$

□

Exercises

Exercise 4.47: Prove Lemma 4.44.

Exercise 4.48: Recall the normal subgroup L of $\mathbb{R}^2$ from Exercises 3.15, 3.34, and 3.68 on pages 58, 63, and 71, respectively. In Exercise 4.24 on page 86 you found an explicit isomorphism $L \cong \mathbb{R}$.

(a) Use the Isomorphism Theorem to find an isomorphism $\mathbb{R}^2/L \cong \mathbb{R}$.
(b) Argue from this that $\mathbb{R}^2/\mathbb{R} \cong \mathbb{R}$.
(c) Describe geometrically how the cosets of $\mathbb{R}^2/L$ are mapped to elements of $\mathbb{R}$.

Exercise 4.49: Recall the normal subgroup $\langle -\mathbf{1} \rangle$ of Q_8 from Exercises 2.35 on page 33 and 3.65 on page 71.
(a) Use Lagrange's Theorem to explain why $Q_8/\langle -\mathbf{1} \rangle$ has order 4.
(b) We know from Exercise 2.31 on page 32 that there are only two groups of order 4, the Klein 4-group and the cyclic group of order 4, which we can represent by $\mathbb{Z}_4$. Use the Isomorphism Theorem to determine which of these groups is isomorphic to $Q_8/\langle -\mathbf{1} \rangle$.

4.4: Automorphisms and groups of automorphisms

In this final section of Chapter 4, we use a special kind isomorphism to build a new group.

Definition 4.50: Let G be a group. If $f : G \to G$ is an isomorphism, then we call f an **automorphism**.[a]

[a] The word comes Greek words that mean *self* and *shape*.

An automorphism is an isomorphism whose domain and range are the same set. Thus, to show that some function f is an automorphism, you must show first that the domain and the range of f are the same set. Afterwards, you show that f satisfies the homomorphism property, and then that it is both one-to-one and onto.

Example 4.51:
(a) An easy automorphism for any group G is the identity isomorphism $\iota(g) = g$:
- its range is by definition G;
- it is a *homomorphism* because $\iota(g \cdot g') = g \cdot g' = \iota(g) \cdot \iota(g')$;
- it is *one-to-one* because $\iota(g) = \iota(g')$ implies (by evaluation of the function) that $g = g'$; and
- it is *onto* because for any $g \in G$ we have $\iota(g) = g$.

(b) An automorphism in $(\mathbb{Z}, +)$ is $f(x) = -x$:
- its range is $\mathbb{Z}$ because of closure;
- it is a *homomorphism* because $f(x+y) = -(x+y) = -x - y = f(x) + f(y)$;
- it is *one-to-one* because $f(x) = f(y)$ implies that $-x = -y$, so $x = y$; and
- it is *onto* because for any $x \in \mathbb{Z}$ we have $f(-x) = x$.

(c) An automorphism in D_3 is $f(x) = \rho^2 x \rho$:
- its range is D_3 because of closure;
- it is a *homomorphism* because $f(xy) = \rho^2(xy)\rho = \rho^2(x \cdot \iota \cdot y)\rho = \rho^2(x \cdot \rho^3 \cdot y)\rho = (\rho^2 x \rho) \cdot (\rho^2 y \rho) = f(x) \cdot f(y)$;
- it is *one-to-one* because $f(x) = f(y)$ implies that $\rho^2 x \rho = \rho^2 y \rho$, and multiplication on the left by ρ and on the right by ρ^2 gives us $x = y$; and
- it is *onto* because for any $y \in D_3$, choose $x = \rho y \rho^2$ and then $f(x) = \rho^2(\rho y \rho^2)\rho = (\rho^2 \rho) \cdot y \cdot (\rho^2 \rho) = \iota \cdot y \cdot \iota = y$. ◿

The automorphism of Example 4.51(c) generalizes to an important automorphism.

Recall now the conjugation of one element of a group by another, introduced in Exercise 2.36 on page 33. By fixing the second element, we can turn this into a function on a group.

Definition 4.52: Let G be a group and $a \in G$. Define the function of **conjugation by** a to be $\text{conj}_a(x) = a^{-1}xa$. ◿

In Example 4.51(c), we had $a = \rho$ and $\text{conj}_a(x) = a^{-1}xa = \rho^2 x\rho$.

You have already worked with conjugation in previous exercises, such as showing that it can provide an alternate definition of a normal subgroup (Exercises 33 and 71). Beyond that, conjgating a subgroup *always* produces another subgroup:

Lemma 4.53: *Let G be a group, and $a \in G$. Then conj_a is an automorphism. Moreover, for any $H < G$,*

$$\{\text{conj}_a(h) : h \in H\} < G.$$

PROOF: You do it! See Exercise 4.61. □

The subgroup $\{\text{conj}_a(h) : h \in H\}$ is important enough to identify by a special name.

Definition 4.54: Suppose $H < G$, and $a \in G$. We say that $\{\text{conj}_a(h) : h \in H\}$ is the **group of conjugations of H by a**, and denote it by $\text{Conj}_a(H)$. ◿

Conjugation of a subgroup H by an arbitrary $a \in G$ is *not* necessarily an automorphism; there can exist $H < G$ and $a \in G \backslash H$ such that *not* have $H = \{\text{conj}_a(h) : h \in H\}$. (Here $G \backslash H$ indicates a set difference, not the set of right cosets.) On the other hand, if H is a *normal* subgroup of G then we *do* have $H = \{\text{conj}_a(h) : h \in H\}$; this property can act as an alternate definition of a normal subgroup. You will explore this in the exercises.

Now it is time to identify the new group that we promised at the beginning of the section.

Notation 4.55: Write $\text{Aut}(G)$ for the set of all automorphisms of G. We typically denote elements of $\text{Aut}(G)$ by Greek letters ($\alpha, \beta, \ldots$), rather than Latin letters ($f, g, \ldots$).

Example 4.56: We compute $\text{Aut}(\mathbb{Z}_4)$. Let $\alpha \in \text{Aut}(\mathbb{Z}_4)$ be arbitrary; what do we know about α? By definition, its range is $\mathbb{Z}_4$, and by Theorem 4.10 on page 84 we know that $\alpha(0) = 0$. Aside from that, we consider all the possibilities that preserve the isomorphism properties.

Recall from Theorem 3.84 on page 75 that $\mathbb{Z}_4$ is a cyclic group; in fact $\mathbb{Z}_4 = \langle 1 \rangle$. Corollary 4.13 on page 85 tells us that $\alpha(1)$ will tell us everything we want to know about α. So, what can $\alpha(1)$ be?

Case 1. Can we have $\alpha(1) = 0$? If so, then $\alpha(n) = 0$ for all $n \in \mathbb{Z}_4$. This is not one-to-one, so we cannot have $\alpha(1) = 0$.

Case 2. Can we have $\alpha(1) = 1$? Certainly $\alpha(1) = 1$ if α is the identity homomorphism ι, so we can have $\alpha(1) = 1$.

Case 3. Can we have $\alpha(1) = 2$? If so, then the homomorphism property implies that

$$\alpha(2) = \alpha(1+1) = \alpha(1) + \alpha(1) = 4 = 0.$$

An automorphism must be a homomorphism, but if $\alpha(1) = 2$ then α is not one-to-one: by Theorem 4.10 on page 84, $\alpha(0) = 0 = \alpha(2)$! So we *cannot* have $\alpha(1) = 2$.

Case 4. Can we have $\alpha(1) = 3$? If so, then the homomorphism property implies that

$$\begin{aligned}\alpha(2) &= \alpha(1+1) = \alpha(1) + \alpha(1) = 3+3 = 6 = 2; \text{ and}\\ \alpha(3) &= \alpha(2+1) = \alpha(2) + \alpha(1) = 2+3 = 5 = 1.\end{aligned}$$

In this case, α is both one-to-one *and* onto. We were careful to observe the homomorphism property when determining α, so we know that α is a homomorphism. So we *can* have $\alpha(1) = 2$.

We found only two possible elements of $\mathrm{Aut}(\mathbb{Z}_4)$: the identity automorphism and the automorphism determined by $\alpha(1) = 3$. ◿

If $\mathrm{Aut}(\mathbb{Z}_4)$ were a group, then the fact that it contains only two elements would imply that $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$. But *is* it a group?

Lemma 4.57: *For any group G, $\mathrm{Aut}(G)$ is a group under the operation of composition of functions.*

PROOF: Let G be any group. We show that $\mathrm{Aut}(G)$ satisfies each of the group properties from Definition 2.1.

(closure) Let $\alpha, \theta \in \mathrm{Aut}(G)$. We must show that $\alpha \circ \theta \in \mathrm{Aut}(G)$ as well:

- the domain and range of $\alpha \circ \theta$ are both G because the domain and range of both α and θ are both G;
- $\alpha \circ \theta$ is a *homomorphism* because for any $g, g' \in G$ we can apply the homomorphism property that applies to α and θ to obtain

$$\begin{aligned}(\alpha\circ\theta)(g\cdot g') &= \alpha\left(\theta\left(g\cdot g'\right)\right)\\ &= \alpha\left(\theta(g)\cdot\theta\left(g'\right)\right)\\ &= \alpha(\theta(g))\cdot\alpha\left(\theta\left(g'\right)\right)\\ &= (\alpha\circ\theta)(g)\cdot(\alpha\circ\theta)\left(g'\right);\end{aligned}$$

- $\alpha \circ \theta$ is *one-to-one* because $(\alpha \circ \theta)(g) = (\alpha \circ \theta)\left(g'\right)$ implies $\alpha(\theta(g)) = \alpha\left(\theta\left(g'\right)\right)$; since α is one-to-one we infer that $\theta(g) = \theta\left(g'\right)$; since θ is one-to-one we conclude that $g = g'$; and
- $\alpha \circ \theta$ is *onto* because for any $z \in G$,
  - α is onto, so there exists $y \in G$ such that $\alpha(y) = z$, and
  - θ is onto, so there exists $x \in G$ such that $\theta(x) = y$, so

$$\circ\ (\alpha\circ\theta)(x)=\alpha(\theta(x))=\alpha(y)=z.$$

We have shown that $\alpha\circ\theta$ satisfies the properties of an automorphism; hence, $\alpha\circ\theta\in\mathrm{Aut}(G)$, and $\mathrm{Aut}(G)$ is closed under the composition of functions.

(associativity) The associative property is sastisfied because the operation is composition of functions, which is associative.

(identity) Denote by ι the identity homomorphism; that is, $\iota(g)=g$ for all $g\in G$. We showed in Example 4.51(a) that ι is an automorphism, so $\iota\in\mathrm{Aut}(G)$. Let $f\in\mathrm{Aut}(G)$; we claim that $\iota\circ f=f\circ\iota=f$. Let $x\in G$ and write $f(x)=y$. We have

$$(\iota\circ f)(x)=\iota(f(x))=\iota(y)=y=f(x),$$

and likewise $(f\circ\iota)(x)=f(x)$. Since x was arbitrary in G, we have $\iota\circ f=f\circ\iota=f$.

(inverse) Let $\alpha\in\mathrm{Aut}(G)$. Since α is an automorphism, it is an isomorphism. You showed in Exercise 4.27 that α^{-1} is also an isomorphism. The domain and range of α are both G, so the domain and range of α^{-1} are also both G. Hence $\alpha^{-1}\in\mathrm{Aut}(G)$.

□

Since $\mathrm{Aut}(G)$ is a group, we can compute $\mathrm{Aut}(\mathrm{Aut}(G))$. In the exercises you will compute $\mathrm{Aut}(G)$ for some other groups.

Exercises.

Exercise 4.58: Show that $f(x)=x^2$ is an automorphism on the group $(\mathbb{R}^+,\times)$, but not on the group $(\mathbb{R},+)$.

Exercise 4.59: We consider $G=A_3$ and $H=D_3$.

(a) List the elements of $\mathrm{Conj}_\rho(A_3)$.

(b) List the elements of $\mathrm{Conj}_\varphi(A_3)$.

(c) In both (a) and (b), we saw that $\mathrm{Conj}_a(A_3)=A_3$ for $a=\rho,\varphi$. This makes sense, since $A_3\triangleleft D_3$. Find a subgroup K of D_3 and an element $a\in D_3$ where .

Exercise 4.60: Let $H=\langle \mathbf{i}\rangle<Q_8$. List the elements of $\mathrm{Conj}_{\mathbf{j}}(H)$.

Exercise 4.61: Prove Lemma 4.53 on page 98 in two parts:

(a) Show first that conj_g is an automorphism.

(b) Show that $\{\mathrm{conj}_a(h):\ h\in H\}$ is a group.

Exercise 4.62: Determine the automorphism group of $\mathbb{Z}_5$.

Exercise 4.63: Determine the automorphism group of D_3.

Chapter 5:
Groups of permutations

This chapter introduces groups of permutations, a fundamental object of study in group theory. Section 5.1 introduces you to groups of permutations. Section 5.1 describes a convenient way to write permutations. Sections 5.3 and 5.5 introduce you to two special classes of groups of permutation. The main goal of this chapter is to show that groups of permutations are, in some sense, "all there is" to group theory, which we accomplish in Section 5.4. We conclude with a great example of an application of symmetry groups in Section 5.6.

5.1: Permutations

Certain applications of mathematics involve the rearrangement of a list of n elements. It is common to refer to such rearrangements as *permutations*.

Definition 5.1: A **list** is a sequence. Let V be any finite list. A **permutation** is a one-to-one function whose domain and range are both V. ◿

We require V to be a list rather than a set because for a permutation, the order of the elements matters: the lists $(a,d,k,r) \neq (a,k,d,r)$ even though $\{a,d,k,r\} = \{a,k,d,r\}$. For the sake of convenience, we usually write V as a list of natural numbers between 1 and $|V|$, but it can be any finite list.

Example 5.2: Let $S = (a,d,k,r)$. Define a permutation on the elements of S by

$$f(x) = \begin{cases} r, & x = a; \\ a, & x = d; \\ k, & x = k; \\ d, & x = r. \end{cases}$$

Notice that f is one-to-one, and $f(S) = (r,a,k,d)$.

We can represent the same permutation on $V = (1,2,3,4)$, a generic list of four elements. Define a permutation on the elements of V by

$$\pi(i) = \begin{cases} 2, & i = 1; \\ 4, & i = 2; \\ 3, & i = 3; \\ 1, & i = 4. \end{cases}$$

Here π is one-to-one, and $\pi(i) = j$ is interpreted as "the jth element of the permuted list is the ith element of the original list." You could visualize this as

position in original list i		position in permuted list j
1	$\rightarrow$	2
2	$\rightarrow$	4
3	$\rightarrow$	3
4	$\rightarrow$	1

Thus $\pi(V) = (4,1,3,2)$. If you look back at $f(S)$, you will see that in fact the first element of the permuted list, $f(S)$, is the fourth element of the original list, S. ◿

Permutations have a convenient property.

Lemma 5.3: *The composition of two permutations is a permutation.*

PROOF: Let V be a set of n elements, and α, β permutations of V. Let $\gamma = \alpha \circ \beta$. We claim that γ is a permutation. To show this, we must show that γ is a one-to-one function whose domain and range are both V. From the definition of α and β, it follows that the domain and range of γ are both V; it remains to show that γ is one-to-one. Let $x, y \in V$ and assume that $\gamma(x) = \gamma(y)$; by definition of γ,

$$\alpha(\beta(x)) = \alpha(\beta(y)).$$

Because they are permutations, α and β are one-to-one functions. Since α is one-to-one, we can simplify the above equation to

$$\beta(x) = \beta(y);$$

and since β is one-to-one, we can simplify the above equation to

$$x = y.$$

Hence γ is a one-to-one function. We already explained why its domain and range are both V, so γ is a permutation. □

In Example 5.2, we wrote a permutation as a piecewise function. This is burdensome; we would like a more efficient way to denote permutations.

Notation 5.4: The **tabular notation** for a permutation on a list of n elements is a $2 \times n$ matrix

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$$

indicating that $\alpha(1) = \alpha_1$, $\alpha(2) = \alpha_2$, …, $\alpha(n) = \alpha_n$. Again, $\alpha(i) = j$ indicates that the jth element of the permuted list is the ith element of the original list.

Example 5.5: Recall V and π from Example 5.2. In tabular notation,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

because π moves

- the element in the first position to the second;

- the element in the second position to the fourth;
- the element in the third position nowhere; and
- the element in the fourth position to the first.

Then

$$\pi(1,2,3,4) = (4,1,3,2).$$

Notice that the tabular notation for π looks similar to the table in Example 5.2.

We can also use π to permute different lists, so long as the new lists have four elements:

$$\pi(3,2,1,4) = (4,3,1,2);$$
$$\pi(2,4,3,1) = (1,2,3,4);$$
$$\pi(a,b,c,d) = (d,a,c,b).\triangle$$

Definition 5.6: For $n \geq 2$, denote by S_n the set of all permutations of a list of n elements.

It turns out that S_n is a group for all $n \geq 2$.

Example 5.7: For $n = 2,3$ we have

$$S_2 = \{(1), (1\,2)\}$$
$$S_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.\triangle$$

How large is each S_n? To answer this, we must count the number of permutations of n elements. A counting argument called *the multiplication principle* shows that there are

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$$

such permutations. Why? Given any list of n elements,

- we have n positions to move the first element, including its current position;
- we have $n-1$ positions to move the second element, since the first element has already taken one spot;
- we have $n-2$ positions to move the third element, since the first and second elements have already take two spots;
- etc.

Thus $|S_n| = n!$.

We explained earlier that any permutation is really a one-to-one function; naturally, one can ask whether the set of all permutations on n elements behaves as a group under the operation of composition of functions.

Theorem 5.8: *For all $n \geq 2$ $(S_n, \circ)$ is a group.*

Notation 5.9: Normally we just write S_n, understanding from context that the operation is composition of functions. It is common to refer to S_n as the **symmetric group** of n elements.

PROOF: Let $n \geq 2$. We have to show that S_n satisfies the properties of a group under the operation of composition of functions:

- For closure, we must show that the composition of two permutations is a permutation. This is precisely Lemma 5.3 on page 102.
- The associative property follows from the fact that permutations are functions, and functions are associative.
- The identity function ι such that $\iota(x) = x$ for all $x \in \{1, 2, \ldots, n\}$ is also the identity of S_n under composition: for any $\alpha \in S_n$ and for any $x \in \{1, 2, \ldots, n\}$ we have

$$(\iota \circ \alpha)(x) = \iota(\alpha(x)) = \alpha(x);$$

since x was arbitrary, $\iota \circ \alpha = \alpha$. A similar argument shows that $\alpha \circ \iota = \alpha$.

- Every one-to-one function has an inverse function, so every element of S_n has an inverse element under composition.

□

Exercises

Exercise 5.10: How many elements are there of S_4?

Exercise 5.11: Write the elements of S_3 in tabular notation. Identify at least one normal subgroup, and at least one subgroup that is not normal.

5.2: Cycle notation

Permutations are frequently used to anyalyze problems that involves lists. Indeed they are used so frequently that even the tabular notation is considered burdensome; we need a simpler notation.

Definition 5.12: A **cycle** is a vector

$$\alpha = (\alpha_1\ \alpha_2\ \cdots\ \alpha_n)$$

that corresponds to the permutation where the entry in position α_1 is moved to position α_2; the entry in position α_2 is moved to position α_3, ... and the element in position α_n is moved to position α_1. If a position is not listed in α, then the entry in that position is not moved. We call such positions **stationary**. For the identity cycle where no entry is moved, we write

$$\iota = (1)\ .\!\!\measuredangle$$

The fact that the permutation α moves the entry in position α_n to position α_1 is the reason that this is called a *cycle;* applying it repeatedly cycles the list of elements around, and on the nth application the list returns to its original order.

Example 5.13: Recall π from Example 5.5. In tabular notation,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

To write it as a cycle, we can start with any position we like. However, the convention is to start with the smallest position that changes. Since π moves elements out of position 1, we start with

$$\pi = (1\,?)\,.$$

The second entry in cycle notation tells us where π moves the element whose position is that of the first entry. The first entry indicates position 1. From the tabular notation, we see that π moves the element in position 1 to position 2, so

$$\pi = (1\,2\,?)\,.$$

The third entry of cycle notation tells us where π moves the element whose position is that of the second entry. The second entry indicates position 2. From the tabular notation, we see that π moves the element in position 2 to position 4, so

$$\pi = (1\,2\,4\,?)\,.$$

The fourth entry of cycle notation tells us where π moves the element whose position is that of the third entry. The third element indicates position 4. From the tabular notation, we see that π moves the element in position 4 to position 1, so you might feel the temptation to write

$$\pi = (1\,2\,4\,1\,?)\,,$$

but there is no need. Since we have now returned to the first element in the cycle, we close it:

$$\pi = (1\,2\,4)\,.$$

The cycle $(1\,2\,4)$, indicates that

- the element in position 1 of a list moves to the position 2;
- the element in position 2 of a list moves to position 4;
- the element in position 4 of a list moves to position 1.

What about the element in position 3? Since it doesn't appear in the cycle notation, it must be stationary. This agrees with what we wrote in the piecewise and tabular notations for π. ◿

Not all permutations can be written as one cycle.

Example 5.14: Consider the permutation in tabular notation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

We can easily start the cycle with $\alpha = (1\,2)$, and this captures the behavior on the elements in the first and second positions of a list, but what about the third and fourth? ◿

To solve this temporary difficulty, we develop a simple arithmetic of cycles. On what operation shall we develop an arithmetic? Cycles represent permutations; permutations are one-to-one functions; functions can be *composed*. Hence the operation is *composition*.

Example 5.15: Consider the cycles

$$\beta = (2\,3\,4) \quad \text{and} \quad \gamma = (1\,2\,4).$$

What is the cycle notation for

$$\beta \circ \gamma = (2\,3\,4) \circ (1\,2\,4)?$$

We can answer this by considering an example list; let $V = (1,2,3,4)$ and compute $(\beta \circ \gamma)(V)$. Since $(\beta \circ \gamma)(x) = \beta(\gamma(x))$, first we apply γ:

$$\gamma(V) = (4,1,3,2),$$

followed by β:

$$\beta(\gamma(V)) = (4,2,1,3).$$

Thus

- the element in position 1 eventually moved to position 3;
- the element in position 3 eventually moved to position 4;
- the element in position 4 eventually moved to position 1;
- the element in position 2 did not move.

In cycle notation, we write this as

$$\beta \circ \gamma = (1\,3\,4). \text{◿}$$

Another phenomenon occurs when each permutation moves elements that the other does not.

Example 5.16: Consider the two cycles

$$\beta = (1\,3) \quad \text{and} \quad \gamma = (2\,4).$$

There is no way to simplify $\beta \circ \gamma$ into a *single* cycle, because β operates only on the first and third elements of a list, and γ operates only on the second and fourth elements of a list. The only way to write them is as the composition of two cycles,

$$\beta \circ \gamma = (1\,3) \circ (2\,4). \text{◿}$$

This motivates the following.

Definition 5.17: We say that two cycles are **disjoint** if none of their entries are common.

Disjoint cycles enjoy an important property.

Lemma 5.18: *Let α, β be two disjoint cycles. Then $\alpha \circ \beta = \beta \circ \alpha$.*

PROOF: Let $n \in \mathbb{N}^+$ be the largest entry in α or β. Let $V = (1, 2, \ldots, n)$. Let $i \in V$. We consider the following cases: □

Case 1. $\alpha(i) \neq i$.
Let $j = \alpha(i)$. The definition of cycle notation implies that j appears immediately after i in the cycle α. Recall that α and β are disjoint. Since i and j are entries of α, they cannot be entries of β. By definition of cycle notation, $\beta(i) = i$ and $\beta(j) = j$. Hence

$$(\alpha \circ \beta)(i) = \alpha(\beta(i)) = \alpha(i) = j = \beta(j) = \beta(\alpha(i)) = (\beta \circ \alpha)(i).$$

Case 1. $\alpha(i) = i$.
Subcase (a): $\beta(i) = i$.
We have $(\alpha \circ \beta)(i) = i = (\beta \circ \alpha)(i)$.
Subcase (b): $\beta(i) \neq i$.
Let $j = \beta(i)$. We have

$$(\beta \circ \alpha)(i) = \beta(\alpha(i)) = \beta(i) = j.$$

The definition of cycle notation implies that j appears immediately after i in the cycle β. Recall that α and β are disjoint. Since j is an entry of β, it cannot be an entry of α. By definition of cycle notation, $\alpha(j) = j$. Hence

$$(\alpha \circ \beta)(i) = \alpha(j) = j = (\beta \circ \alpha)(i).$$

PROOF: In both cases, we had $(\alpha \circ \beta)(i) = (\beta \circ \alpha)(i)$. Since i was arbitrary, $\alpha \circ \beta = \beta \circ \alpha$. □

Notation 5.19: Since the composition of two disjoint cycles $\alpha \circ \beta$ cannot be simplified, we normally write them consecutively, without the circle that indicates composition, for example

$$(1\,2)(3\,4).$$

By Lemma 5.18, we can also write this as

$$(3\,4)(1\,2).$$

That said, the usual convention for cycles is to write the smallest entry of a cycle first, and to write cycles with smaller first entries before cycles with larger first entries. Thus we prefer

$$(1\,4)\,(2\,3)$$

to either of

$$(1\,4)\,(3\,2) \quad \text{or} \quad (2\,3)\,(1\,4)\,.$$

The convention for writing a permutation in cycle form is the following:

1. Rotate each cycle sometimes that the first entry is the smallest entry in each cycle.
2. Simplify the permutation by computing the composition of cycles that are not disjoint. Discard all cycles of length 1.
3. The remaining cycles will be disjoint. From Lemma 5.18, we know that they commute; write them in order from smallest first entry to largest first entry.

Example 5.20: We return to Example 5.14, with

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

To write this permutation in cycle notation, we begin again with

$$\alpha = (1\,2)\ldots?$$

Since α also moves entries in positions 3 and 4, we need to add a second cycle. We start with the smallest position whose entry changes position, 3:

$$\alpha = (1\,2)\,(3\,?)\,.$$

Since α moves the element in position 3 to position 4, we write

$$\alpha = (1\,2)\,(3\,4\,?)\,.$$

Now α moves the element in position 4 to position 3, so we can close the second cycle:

$$\alpha = (1\,2)\,(3\,4)\,.$$

Now α moves no more entries, so the cycle notation is complete. ◿

We have come to the main result of this section.

Theorem 5.21: *Every permutation can be written as a composition of cycles.*

The proof is constructive.

PROOF: Let π be a permutation; denote its domain by V. Without loss of generality, we write $V = (1, 2, \ldots, n)$.

Let i_1 be the smallest element of V such that $\pi(i_1) \neq i_1$. Recall that the range of π has at most n elements; since π is one-to-one, eventually $\pi^{k+1}(i_1) = i_1$ for some $k \leq n$. Let $\alpha^{(1)}$ be the cycle $\left(i_1\ \pi(i_1)\ \pi(\pi(i_1)) \cdots \pi^k(i_1)\right)$.

At this point, either every element of V that is not stationary with respect to π appears in $\alpha^{(1)}$, or it does not. If there is some $i_2 \in V$ such that i_2 is not stationary with respect to π and $i_2 \notin \alpha^{(1)}$, then generate the cycle $\alpha^{(2)}$ by $\left(i_2\ \pi(i_2)\ \pi(\pi(i_2)) \cdots \pi^\ell(i_2)\right)$ where as before $\pi^{\ell+1}(i_2) = i_2$.

Repeat this process until every non-stationary element of V corresponds to a cycle, generating $\alpha^{(3)}$, ..., $\alpha^{(m)}$ for non-stationary $i_3 \notin \alpha^{(1)}, \alpha^{(2)}$, $i_4 \notin \alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}$, and so on until $i_m \notin \alpha^{(1)}, \ldots, \alpha^{(m-1)}$.

The remainder of the proof consists of two claims.

Claim 1: $\alpha^{(i)}$ and $\alpha^{(j)}$ are disjoint for any $i < j$.

Suppose to the contrary that there exists an integer r such that $r \in \alpha^{(i)}$ and $r \in \alpha^{(j)}$. By definition, the next entry of both $\alpha^{(i)}$ and $\alpha^{(j)}$ is $\pi(r)$. The subsequent entry of both is $\pi(\pi(r))$, and so forth. This cycles through both $\alpha^{(i)}$ and $\alpha^{(j)}$ until we reach $\pi^\lambda(r) = r$ for some $\lambda \in \mathbb{N}$. Hence $\alpha^{(i)} = \alpha^{(j)}$. But this contradicts the choice of the first element of $\alpha^{(j)}$ as an element of V that did *not* appear in $\alpha^{(i)}$.

Claim 2: $\pi = \alpha^{(1)}\alpha^{(2)}\cdots\alpha^{(m)}$.

Let $i \in V$. If $\pi(i) = i$, then by definition $\alpha^{(j)}(i) = i$ for all $j = 1, 2, \ldots, m$. Otherwise, i appears in $\alpha^{(j)}$ for some $j = 1, 2, \ldots, m$. By definition, $\alpha^{(j)}(i) = \pi(i)$. By Claim 1, both i and $\pi(i)$ appear in *only* one of the α. Hence

$$\begin{aligned}\left(\alpha^{(1)}\alpha^{(2)}\cdots\alpha^{(m)}\right)(i) &= \alpha^{(1)}\left(\alpha^{(2)}\left(\cdots\alpha^{(m-1)}\left(\alpha^{(m)}(i)\right)\right)\right)\\ &= \alpha^{(1)}\left(\alpha^{(2)}\left(\cdots\alpha^{(j-1)}\left(\alpha^{(j)}(i)\right)\right)\right)\\ &= \alpha^{(1)}\left(\alpha^{(2)}\left(\cdots\alpha^{(j-1)}(\pi(i))\right)\right)\\ &= \pi(i).\end{aligned}$$

We have shown that

$$\left(\alpha^{(1)}\alpha^{(2)}\cdots\alpha^{(m)}\right)(i) = \pi(i).$$

Since i is arbitrary, $\pi = \alpha^{(1)} \circ \alpha^{(2)} \circ \cdots \circ \alpha^{(m)}$. That is, π is a composition of cycles. Since π was arbitrary, every permutation is a composition of cycles. □

Example 5.22: Consider the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 3 & 2 & 4 & 8 & 1 & 6 \end{pmatrix}.$$

Using the proof of Theorem 5.21, we define the cycles

$$\alpha^{(1)} = (1\,7)$$
$$\alpha^{(2)} = (2\,5\,4)$$
$$\alpha^{(3)} = (6\,8)\,.$$

Notice that $\alpha^{(1)}$, $\alpha^{(2)}$, and $\alpha^{(3)}$ are disjoint. In addition, the only element of $V = (1,2,\ldots,8)$ that does not appear in an α is 3, because $\pi(3) = 3$. Inspection verifies that

$$\pi = \alpha^{(1)}\alpha^{(2)}\alpha^{(3)}.\triangle$$

We conclude with some examples of simplifying the composition of permutations.

Example 5.23: Let $\alpha = (1\,3)\,(2\,4)$ and $\beta = (1\,3\,2\,4)$. Notice that $\alpha \neq \beta$; check this on $V = (1,2,3,4)$ if this isn't clear. In addition, α and β are not disjoint.

1. We compute the cycle notation for $\gamma = \alpha \circ \beta$. We start with the smallest entry moved by either α or β:

   $$\gamma = (\ 1\ \ ?\ )\,.$$

   The notation $\alpha \circ \beta$ means to apply β first, *then* α. What does β do with the entry in position 1? It moves it to position 3. Subsequently, α moves the entry in position 3 back to the entry in position 1. The next entry in the first cycle of γ should thus be 1, but that's also the first entry in the cycle, so we close the cycle. So far, we have

   $$\gamma = (1)\ldots?$$

   We aren't finished, since α and β also move other entries around. The next smallest entry moved by either α or β is 2, so

   $$\gamma = (1)\,(2\,?)\,.$$

   Now β moves the entry in position 2 to the entry in position 4, and α moves the entry in position 4 to the entry in position 2. The next entry in the second cycle of γ should thus be 2, but that's also the first entry in the second cycle, so we close the cycle. So far, we have

   $$\gamma = (1)\,(2)\ldots?$$

   Next, β moves the entry in position 3, so

   $$\gamma = (1)\,(2)\,(3\,?)\,.$$

   Where does β move the entry in position 3? To the entry in position 2. Subsequently, α moves the entry in position 2 to the entry in position 4. We now have

   $$\gamma = (1)\,(2)\,(3\,4\,?)\,.$$

You can probably guess that 4, as the largest possible entry, will close the cycle, but to be safe we'll check: β moves the entry in position 4 to the entry in position 1, and α moves the entry in position 1 to the entry in position 3. The next entry of the third cycle will be 3, but this is also the first entry of the third cycle, so we close the third cycle and

$$\gamma = (1)\,(2)\,(3\,4)\,.$$

Finally, we simplify γ by not writing cycles of length 1, so

$$\gamma = (3\,4)\,.$$

Hence

$$((1\,3)\,(2\,4)) \circ (1\,3\,2\,4) = (3\,4)\,.$$

2. Now we compute the cycle notation for $\beta \circ \alpha$, but with less detail. Again we start with 1, which α moves to 3, and β then moves to 2. So we start with

$$\beta \circ \alpha = (1\,2\,?)\,.$$

Next, α moves 2 to 4, and β moves 4 to 1. This closes the first cycle:

$$\beta \circ \alpha = (1\,2)\ldots?$$

We start the next cycle with position 3: α moves it to position 1, which β moves back to position 3. This generates a length-one cycle, so there is no need to add anything. Likewise, the element in position 4 is also stable under $\beta \circ \alpha$. Hence we need write no more cycles;

$$\beta \circ \alpha = (1\,2)\,.$$

3. Let's look also at $\beta \circ \gamma$ where $\gamma = (1\,4)$. We start with 1, which γ moves to 4, and then β moves to 1. Since $\beta \circ \gamma$ moves 1 to itself, we don't have to write 1 in the cycle. The next smallest number that appears is 2: γ doesn't move it, and β moves 2 to 4. We start with

$$\beta \circ \gamma = (2\,4\,?)\,.$$

Next, γ moves 4 to 1, and β moves 1 to 3. This adds another element to the cycle:

$$\beta \circ \gamma = (2\,4\,3\,?)\,.$$

We already know that 1 won't appear in the cycle, so you might guess that we should not close the cycle. To be certain, we consider what $\beta \circ \gamma$ does to 3: γ doesn't move it, and β moves 3 to 2. The cycle is now complete:

$$\beta \circ \gamma = (2\,4\,3)\,.\!\!\triangle$$

Exercises.

Exercise 5.24: For the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 6 & 3 \end{pmatrix},$$

(a) Evaluate $\alpha(1,2,3,4,5,6)$.
(b) Evaluate $\alpha(1,5,2,4,6,3)$.
(c) Evaluate $\alpha(6,3,5,2,1,4)$.
(d) Write α in cycle notation.
(e) Write α as a piecewise function.

Exercise 5.25: For the permutation

$$\alpha = (1\,3\,4\,2),$$

(a) Evaluate $\alpha(1,2,3,4)$.
(b) Evaluate $\alpha(1,4,3,2)$.
(c) Evaluate $\alpha(3,1,4,2)$.
(d) Write α in tabular notation.
(e) Write α as a piecewise function.

Exercise 5.26: Let $\alpha = (1\,2\,3\,4)$, $\beta = (1\,4\,3\,2)$, and $\gamma = (1\,3)$. Compute $\alpha \circ \beta$, $\alpha \circ \gamma$, $\beta \circ \gamma$, $\beta \circ \alpha$, $\gamma \circ \alpha$, $\gamma \circ \beta$, α^2, β^2, and γ^2. (Here $\alpha^2 = \alpha \circ \alpha$.) What are the inverses of α, β, and γ?

Exercise 5.27: For

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

compute α^2, α^3, ... until you reach the identity permutation.

Exercise 5.28: Show that all the elements of S_3 can be written as compositions of of the cycles $\alpha = (1\,2\,3)$ and $\beta = (2\,3)$.

Exercise 5.29: For α and β as defined in Exercise 5.28, show that $\beta \circ \alpha = \alpha^2 \circ \beta$. (Notice that $\alpha, \beta \in S_n$ for all $n > 2$, so as a consequence of this exercise S_n is not abelian for $n > 2$.)

Exercise 5.30: Write the Cayley table for S_3.

Exercise 5.31: Show that $D_3 \cong S_3$ by showing that the function $f : D_3 \to S_3$ by $f\left(\rho^a \varphi^b\right) = \alpha^a \beta^b$ is an isomorphism.

Exercise 5.32: List the elements of S_4 using cycle notation.

Exercise 5.33: Compute the cyclic subgroup of S_4 generated by $\alpha = (1\,3\,4\,2)$. Compare your answer to that of Exercise 5.27.

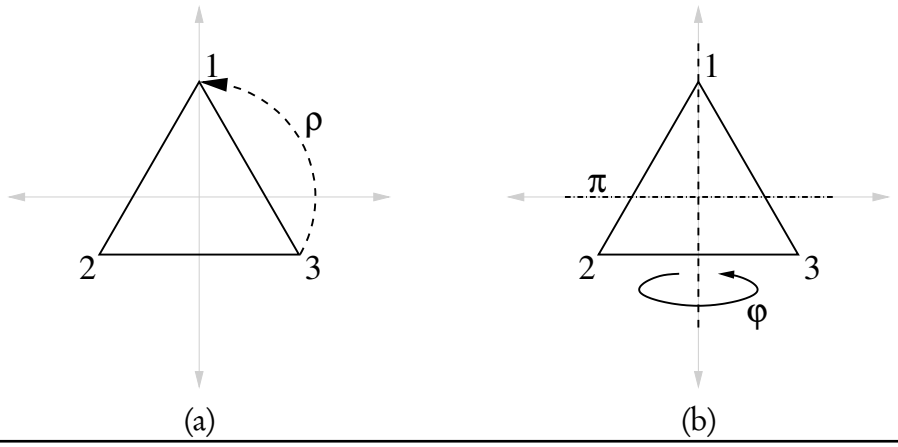


Figure 5.1. Rotation and reflection of an equilateral triangle centered at the origin

Exercise 5.34: Let $\alpha = (\alpha_1\ \alpha_2\ \cdots\ \alpha_m) \in S_n$. (Note $m < n$.) Show that we can write α^{-1} as

$$\beta = (\alpha_1\ \alpha_m\ \alpha_{m-1}\ \cdots\ \alpha_2).$$

For example, if $\alpha = (2\,3\,5\,6)$, $\alpha^{-1} = (2\,6\,5\,3)$.

5.3: Dihedral groups

In Section 2.2 we studied the symmetries of a triangle; we represented the group as the products of matrices ρ and φ, derived from the symmetries of *rotation* and *reflection about the y-axis*. Figure 5.1, a copy of Figure 2.1 on page 34, shows how ρ and φ correspond to the symmetries of an equilateral triangle centered at the origin. In Exercises 5.28–5.31 you showed that D_3 and S_3 are isomorphic.

We can develop matrices to reflect the symmetries of a regular n-sided polygon as well (the regular n-gon), motivating the definition of the set D_n of symmetries of the n-gon.

Definition 5.35: The **dihedral set** D_n is the set of symmetries of a regular polygon with n sides.

Is D_n always a group?

Theorem 5.36: *Let $n \in \mathbb{N}$ and $n \geq 3$. Then $(D_n, \circ)$ is a group with $2n$ elements, called the **dihedral group**.*

The proof of Theorem 5.36 depends on the following proposition, which we accept without proof. We could prove it using an argument from matrices as in Section 2.2, but proving it requires more energy than is appropriate for this section.

Proposition 5.37: *All the symmetries of a regular n-sided polygon can be generated by a composition of a power of the rotation ρ of angle $2\pi/n$ and a power of the flip φ across the y-axis. In addition, $\varphi^2 = \rho^n = \iota$ (the identity symmetry) and $\varphi\rho = \rho^{n-1}\varphi$.*

PROOF OF THEOREM 5.36: We must show that properties of a group are satisfied.

- Closure follows from Proposition 5.37.
- The associative property follows from the fact that permutations are functions, and the associative property applies to functions.
- Certainly there exists an identity element $\iota \in D_n$, which corresponds to the identity symmetry where no vertex is moved.
- It is obvious that the inverse of a symmetry of the regular n-gon is also a symmetry of the regular n-gon.

It remains to show that D_n has $2n$ elements. From the properties of ρ and φ in Proposition 5.37, all other symmetries are combinations of these two, which means that all symmetries are of the form $\rho^a \varphi^b$ for some $a \in \{0, \ldots, n-1\}$ and $b \in \{0, 1\}$. Since $\varphi^2 = \rho^n = \iota$, a can have n values and b can have 2 values. Hence there are $2n$ possible elements altogether. □

We have two goals in introducing the dihedral group: first, to give you another concrete and interesting group; and second, to serve as a bridge to Section 5.4. The next example starts starts us in that directions.

Example 5.38: Another way to represent the elements of D_3 is to consider how they re-arrange the vertices of the triangle. We can represent the vertices of a triangle as the list $V = (1, 2, 3)$. Application of ρ to the triangle moves

- vertex 1 to vertex 2;
- vertex 2 to vertex 3; and
- vertex 3 to vertex 1.

This is equivalent to the permutation $(1\,2\,3)$.

Application of φ to the triangle moves

- vertex 1 to itself—that is, vertex 1 does not move;
- vertex 2 to vertex 3; and
- vertex 3 to vertex 2.

This is equivalent to the permutation $(2\,3)$.

In the context of the symmetries of the triangle, it looks as if we can say that $\rho = (1\,2\,3)$ and $\varphi = (2\,3)$. Recall that ρ and φ generate all the symmetries of a triangle; likewise, these two cycles generate all the permutations of a list of three elements! (See Example 5.7 on page 103 and Exercise 2.43 on page 39.) ◿

We can do this with D_4 and S_4 as well.

Example 5.39: Using the tabular notation for permutations, we identify some elements of D_4, the set of symmetries of a square. Of course we have an identity permutation

$$\iota = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

and a 90° rotation

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

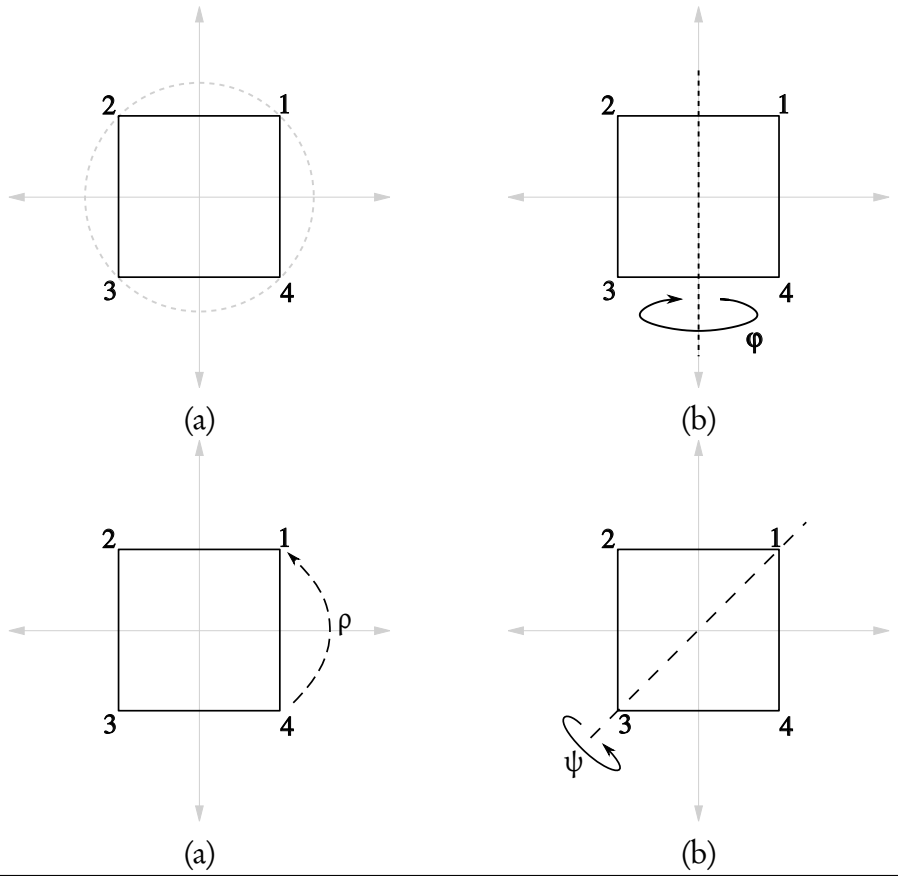


Figure 5.2. Rotation and reflection of a square centered at the origin

We can imagine three kinds of flips: one across the y-axis,

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix};$$

one across the x-axis,

$$\vartheta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix};$$

and one across a diagonal,

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

See Figure 5.2. We can also imagine other diagonals; but they can be shown to be superfluous, just as we show shortly that ϑ and ψ are superflulous. There may be other symmetries of the square, but we'll stop here for the time being.

Is it possible to write ψ as a composition of φ and ρ? It turns out that $\psi = \varphi \circ \rho$. To show this, we consider them as permutations of the vertices of the square, as we did with the triangle above, rather than repeat the agony of computing the matrices of isometries as in Section 2.2.

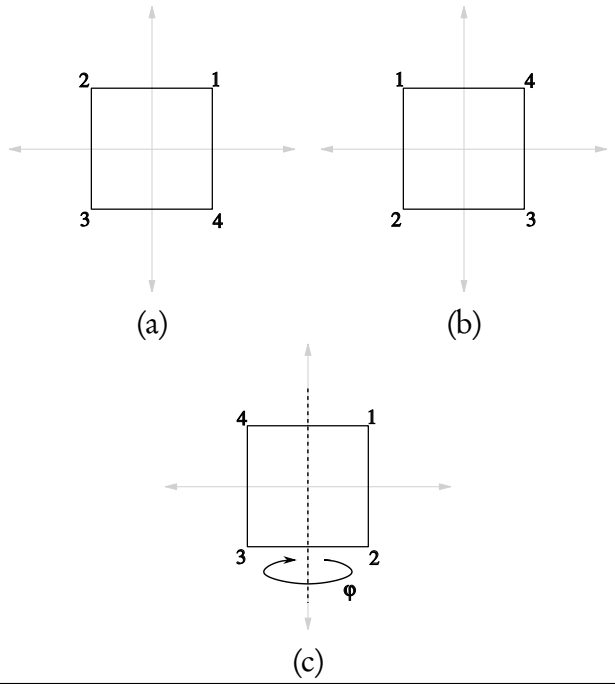


Figure 5.3. Rotation and reflection of a square centered at the origin

- Geometrically, ρ moves $(1,2,3,4)$ to $(4,1,2,3)$; subsequently φ moves $(4,1,2,3)$ to $(1,4,3,2)$; see Figure 5.3.
- We can use the tabular notation for ψ, φ, and ρ to show that the composition of the functions is the same. Starting with the list $(1,2,3,4)$ we see from the tabular notation above that

  $$\psi(1,2,3,4) = (1,4,3,2).$$

  On the other hand,

  $$\rho(1,2,3,4) = (4,1,2,3).$$

  Things get a little tricky here; we want to evaluate $\varphi \circ \rho$, and

  $$\begin{aligned}(\varphi \circ \rho)(1,2,3,4) &= \varphi(\rho(1,2,3,4)) \\ &= \varphi(4,1,2,3) \\ &= (1,4,3,2).\end{aligned}$$

  How did we get that last step? Look back at the tabular notation for φ: the element in the first entry is moved to the second. In the next-to-last line above, the element in the first entry is 4; it gets moved to the second entry in the last line:

  $$\begin{array}{llll} \mathbf{4}, & 1, & 2, & 3 \\ & \searrow & & \\ ?, & \mathbf{4}, & ?, & ? \end{array}$$

The tabular notation for φ also tells us to move the element in the second entry (1) to the first. Thus

$$\begin{array}{cccc} 4, & \mathbf{1}, & 2, & 3 \\ & \searrow\!\!\times & & \\ \mathbf{1}, & 4, & ?, & ? \end{array}$$

Likewise, φ moves the element in the third entry (2) to the fourth, and vice-versa, giving us

$$\begin{array}{cccc} 4, & 1, & \mathbf{2}, & \mathbf{3} \\ & \searrow\!\!\times & & \searrow\!\!\times \\ 1, & 4, & \mathbf{3}, & \mathbf{2} \end{array}$$

In both cases, we see that $\psi = \varphi \circ \rho$. A similar argument shows that $\vartheta = \varphi \circ \rho^2$, so it looks as if we need only φ and ρ to generate D_4. The reflection and the rotation have a property similar to that in S_3:

$$\varphi \circ \rho = \rho^3 \circ \varphi,$$

so unless there is some symmetry of the square that cannot be described by rotation or reflection on the y-axis, we can list all the elements of D_4 using a composition of some power of ρ after some power of φ. There are four unique 90° rotations and two unique reflections on the y-axis, implying that D_4 has at least eight elements:

$$D_4 \supseteq \left\{\iota, \rho, \rho^2, \rho^3, \varphi, \rho\varphi, \rho^2\varphi, \rho^3\varphi\right\}.$$

Can D_4 have other elements? There are in fact $|S_4| = 4! = 24$ possible permutations of the vertices, but are they all symmetries of a square? Consider the permutation from $(1,2,3,4)$ to $(2,1,3,4)$: in the basic square, the distance between vertices 1 and 3 is $\sqrt{2}$, but in the configuration $(2,1,3,4)$ vertices 1 and 3 are adjacent on the square, so the distance between them has diminished to 1. Meanwhile, vertices 2 and 3 are no longer adjacent, so the distance between them has increased from 1 to $\sqrt{2}$. Since the distances between points on the square was not preserved, the permutation described, which we can write in tabular notation as

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

is *not* an element of D_4. The same can be shown for the other fifteen permutations of four elements.

Hence D_4 has eight elements, making it smaller than S_4, which has $4! = 24$. ◿

Corollary 5.40: *For any $n \geq 3$ D_n is isomorphic to a subgroup of S_n. If $n = 3$, then $D_3 \cong S_3$ itself.*

PROOF: You already proved that $D_3 \cong S_3$ in Exercise 5.31. □

Exercises.

Exercise 5.41: Write all eight elements of D_4 in cycle notation.

Exercise 5.42: Construct the composition table of D_4. Compare this result to that of Exercise 2.35.

Exercise 5.43: Show that the symmetries of any n-gon can be described as a power of ρ and φ, where φ is a flip about the y-axis and ρ is a rotation of $2\pi/n$ radians.

5.4: Cayley's Theorem

The mathematician Arthur Cayley discovered a lovely fact about the permutation groups.

Theorem 5.44 (Cayley's Theorem): *Every group of order n is isomorphic to a subgroup of S_n.*

We're going to give an example *before* we give the proof. Hopefully the example will help explain how the proof of the theorem works.

Example 5.45: Consider the Klein 4-group; this group has four elements, so Cayley's Theorem tells us that it must be isomorphic to a subgroup of S_4. We will build the isomorphism by looking at the multiplication table for the Klein 4-group:

$\times$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

To find a permutation appropriate to each element, we'll do the following. First, we label each element with a certain number:

$$\begin{aligned} e &\leftrightsquigarrow 1, \\ a &\leftrightsquigarrow 2, \\ b &\leftrightsquigarrow 3, \\ ab &\leftrightsquigarrow 4. \end{aligned}$$

We will use this along with tabular notation to determine the isomorphism. Define a map f from the Klein 4-group to S_4 by

$$f(x) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \ell(x \cdot e) & \ell(x \cdot a) & \ell(x \cdot b) & \ell(x \cdot ab) \end{pmatrix}, \tag{8}$$

where $\ell(y)$ is the label that corresponds to y.

Sometimes, the right choice of notation makes things easier to read, and this is one example. Again, f maps an element g of the Klein 4-group to a permutation $f(x) = \sigma$ of S_4. Any permutation of S_4 is a one-to-one function on a list of 4 elements, say $(1,2,3,4)$. If $\sigma = (1\,2)(3\,4)$, then $\sigma(2) = 1$. Since $\sigma = f(x)$, we can likewise say that $(f(x))(2) = 1$. This double-evaluation is hard to look at, so we adopt the following notation to emphasize that $f(x)$ is a function:

$$f(x) = f_x.$$

It's much easier now to look at $f_x(2) = 1$.

First let's compute f_a:

$$f_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ ? & ? & ? & ? \end{pmatrix}.$$

The first entry has the value $\ell(a \cdot e) = \ell(a) = 2$, telling us that

$$f_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & ? & ? & ? \end{pmatrix}.$$

The next entry has the value $\ell(a \cdot a) = \ell(a^2) = \ell(e) = 1$, telling us that

$$f_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & ? & ? \end{pmatrix}.$$

The third entry has the value $\ell(a \cdot b) = \ell(ab) = 4$, telling us that

$$f_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & ? \end{pmatrix}.$$

The final entry has the value $\ell(a \cdot ab) = \ell(a^2 b) = \ell(b) = 3$, telling us that

$$f_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

So applying the formula in equation (8) definitely gives us a permutation.

In fact, we could have filled out the bottom row of the permutation by looking above at the multiplication table for the Klein 4-group, locating the row for the multiples of a (the second row of the multiplication table), and filling in the labels for the entries in that row! Doing this

or applying equation (8) to the other elements of the Klein 4-group tells us that

$$f_e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$
$$f_b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$
$$f_{ab} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

We now have a subset of S_4; written in cycle notation, it is

$$\begin{aligned} W &= \{f_e, f_a, f_b, f_{ab}\} \\ &= \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}. \end{aligned}$$

Verifying that W is a group, and therefore a subgroup of S_4, is straightforward; you will do so in the homework. What we need to ensure is that f is indeed an isomorphism. Inspection shows that f is one-to-one and onto; the hard part is the homomorphism property. We will use a little cleverness for this. Let x, y in the Klein 4-group.

- Recall that f_x, f_y, and f_{xy} are permutations, and by definition one-to-one, onto functions on a list of four elements.
- Notice that ℓ is also a one-to-one function, and it has an inverse.
- Let $m \in (1,2,3,4)$. For any z in the Klein 4-group, $\ell(z) = m$ if we listed z as the mth entry of the group. Thus $\ell^{-1}(m)$ indicates the element of the Klein four-group that is labeled by m. For instance, $\ell^{-1}(b) = 3$.
- Since f_x is a permutation of a list of four elements, we can look at $f_x(m)$ as the place where f_x moves m.
- By definition, f_x moves m to $\ell(z)$ where $z = x \cdot \ell^{-1}(m)$; that is,

  $$f_x(m) = \ell\left(x\ell^{-1}(m)\right).$$

  Similar statement holds for how f_y and f_{xy} move m.
- Applying these facts, we observe that

$$\begin{aligned} \left(f_x \circ f_y\right)(m) &= f_x\left(f_y(m)\right) \\ &= f_x\left(\ell\left(y \cdot \ell^{-1}(m)\right)\right) \\ &= \ell\left(x \cdot \ell^{-1}\left(\ell\left(y \cdot \ell^{-1}(m)\right)\right)\right) \\ &= \ell\left(x \cdot \left(y \cdot \ell^{-1}(m)\right)\right) \\ &= \ell\left(xy \cdot \ell^{-1}(m)\right) \\ &= f_{xy}(m). \end{aligned}$$

- Since m was arbitrary in $\{1,2,3,4\}$, f_{xy} and $f_x \circ f_y$ are identical functions.
- Since x, y were arbitrary in the Klein 4-gorup, $f_{xy} = f_x f_y$.

We conclude that f is a homomorphism; since it is one-to-one and onto, f is an isomorphism. ◿

You should read through Example 5.45 carefully two or three times, and make sure you understand it, since in the homework you will construct a similar isomorphism for a different group, and also because we do the same thing now in the proof of Cayley's Theorem.

PROOF OF CAYLEY'S THEOREM: Let G be a finite group of n elements. Label the elements in any order $G = \{g_1, g_2, \ldots, g_n\}$ and for any $x \in G$ denote $\ell(x) = i$ such that $x = g_i$. Define a relation

$$f : G \to S_n \qquad \text{by} \qquad f(g) = \begin{pmatrix} 1 & 2 & \cdots & n \\ \ell(g \cdot g_1) & \ell(g \cdot g_2) & \cdots & \ell(g \cdot g_n) \end{pmatrix}.$$

As we explained in Example 5.45 for the Klein 4-group, this assigns to each $g \in G$ the permutation that, in tabular notation, has the labels for each entry in the row corresponding to g of the Cayley table for G. By this fact we know that f is one-to-one and onto (see also Theorem 2.12 on page 29). The proof that f is a homomorphism is identical to the proof for Example 5.45: nothing in that argument required x, y, or z to be elements of the Klein 4-group; the proof was for a general group! Hence f is an isomorphism, and $G \cong f(G) < S_n$. □

What's so remarkable about this result? One way of looking at it is the following: since every finite group is isomorphic to a subgroup of a group of permutations, *everything you need to know about finite groups can be learned from studying the groups of permutations!* A more flippant summary is that *the theory of finite groups is all about studying how to rearrange lists.*

In theory, I could go back and rewrite these notes, introducing the reader first to lists, then to permutations, then to S_2, to S_3, to the subgroups of S_4 that correspond to the cyclic group of order 4 and the Klein 4-group, and so forth, making no reference to these other groups, nor to the dihedral group, nor to any other finite group that we have studied. But it is more natural to think in terms other than permutations (geometry for D_n is helpful); and it can be tedious to work only with permutations. While Cayley's Theorem has its uses, it does not suggest that we should always consider groups of permutations in place of the more natural representations.

Exercises.

Exercise 5.46: In Example 5.45 we found W, a subgroup of S_4 that is isomorphic to the Klein 4-group. It turns out that $W < D_4$ as well. Draw the geometric representations for each element of W, using a square and writing labels in the appropriate places, as we did in Figures 2.1 on page 34 and 5.2.

Exercise 5.47: Apply Cayley's Theorem to find a subgroup of S_4 that is isomorphic to $\mathbb{Z}_4$. Write the permutations in both tabular and cycle notations.

Exercise 5.48: The subgroup of S_4 that you identified in Exercise 5.47 is also a subgroup of D_4. Draw the geometric representations for each element of this subgroup, using a square and writing labels in the appropriate places.

Exercise 5.49: Since S_3 has six elements, we know it is isomorphic to a subgroup of S_6. In fact, it can be isomorphic to more than one subgroup; Cayley's Theorem tells us only that it is isomorphic to *at least* one. Identify one such subgroup *without* using the isomorphism used in the proof of Cayley's Theorem.

5.5: Alternating groups

A special kind of group of permutations, with very important implications for later topics, are the *alternating groups*. To define them, we need to study permutations a little more closely, in particular the cycle notation.

Definition 5.50: Let $n \in \mathbb{N}^+$. An **n-cycle** is a permutation that can be written as one cycle with n entries. A **transposition** is a 2-cycle.

Example 5.51: The permutation $(1\,2\,3) \in S_3$ is a 3-cycle. The permutation $(2\,3) \in S_3$ is a transposition. The permutation $(1\,3)(2\,4) \in S_4$ cannot be written as only one n-cycle for any $n \in \mathbb{N}^+$: it is the composition of two disjoint transpositions, and any cycle must move 1 to 3, so it would start as $(1\,3\,?)$. If we fill in the blank with anything besides 1, we have a different permutation. So we must close the cycle before noting that 2 moves to 4. ◿

Remark 5.52: Notice that *any transposition is its own inverse.* Why? Consider the product $(i\,j)(i\,j)$: every element in a list is stationary except the ith and jth elements. The rightmost $(i\,j)$ swaps these two, and the leftmost $(i\,j)$ swaps them back. Hence $(i\,j)(i\,j) = (1)$.

Thanks to 1-cycles, any permutation can be written with many different numbers of cycles: for example,

$$(1\,2\,3) = (1\,2\,3)(1) = (1\,2\,3)(1)(3) = (1\,2\,3)(1)(3)(1) = \cdots.$$

In addition, a neat trick allows us to write every permutation as a composition of transpositions.

Example 5.53: $(1\,2\,3) = (1\,3)(1\,2)$. Also

$$(1\,4\,8\,2\,3) = (1\,3)(1\,2)(1\,8)(1\,4).$$

Also $(1) = (1\,2)(1\,2)$. ◿

Lemma 5.54: *Any permutation can be written as a composition of transpositions.*

PROOF: You do it! See Exercise 5.65. □

Remark 5.55: Given an expression of σ as a product of transpositions, say $\sigma = \tau_1 \cdots \tau_n$, it is clear from Remark 5.52 that we can write $\sigma^{-1} = \tau_n \cdots \tau_1$, because

$$\begin{aligned}(\tau_1 \cdots \tau_n)(\tau_n \cdots \tau_1) &= (\tau_1 \cdots \tau_{n-1})(\tau_n \tau_n)(\tau_{n-1} \cdots \tau_1) \\ &= (\tau_1 \cdots \tau_{n-1})\left(\begin{smallmatrix}1\end{smallmatrix}\right)(\tau_{n-1} \cdots \tau_1) \\ &\vdots \\ &= (1)\,.\end{aligned}$$

At this point it is worth looking at Example 5.53 and the discussion before it. Can we write $\left(\begin{smallmatrix}1 & 2 & 3\end{smallmatrix}\right)$ with many different numbers of *transpositions?* Yes:

$$\begin{aligned}(1\,2\,3) &= (1\,3)(1\,2) \\ &= (1\,3)(1\,2)(2\,3)(2\,3) \\ &= (1\,3)(1\,2)(1\,3)(1\,3) \\ &= \cdots\,.\end{aligned}$$

Notice something special about the representation of $(1\,2\,3)$. No matter how you write it, it always has an *even* number of transpositions. By contrast, consider

$$\begin{aligned}(2\,3) &= (2\,3)(2\,3)(2\,3) \\ &= (2\,3)(1\,2)(1\,3)(1\,3)(1\,2) = \cdots\,.\end{aligned}$$

No matter how you write it, you always represent $(2\,3)$ with an *odd* number of transpositions.

Is this always the case?

Theorem 5.56: *Let $\alpha \in S_n$.*

- *If α can be written as the composition of an even number of transpositions, then it cannot be written as the composition of an odd number of transpositions.*
- *If α can be written as the composition of an odd number of transpositions, then it cannot be written as the composition of an even number of transpositions.*

PROOF: Suppose that $\alpha \in S_n$. Consider the polynomials

$$g = \prod_{1 \le i < j \le n} \left(x_i - x_j\right) \qquad \text{and} \qquad g_\alpha := \prod_{1 \le i < j \le n} \left(x_{\alpha(i)} - x_{\alpha(j)}\right).$$

Since the value of g_α depends on the permutation α, and permutations are one-to-one functions, g_α is well-defined; that is, it won't change regardless of how we write α in terms of transpositions.

But what, precisely, *is* g_α? Sometimes $g = g_\alpha$; for example, if $\alpha = \left(\begin{smallmatrix}1 & 3 & 2\end{smallmatrix}\right)$ then

$$g = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

and

$$g_\alpha = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = [(-1)(x_1 - x_3)][(-1)(x_2 - x_3)](x_1 - x_2) = g. \quad (9)$$

Is it always the case that $g_\alpha = g$? Not necessarily: if $\alpha = \begin{pmatrix} 1 & 2 \end{pmatrix}$ then $g = x_1 - x_2$ and $g_\alpha = x_2 - x_1 \neq g$. On the other hand, $g_\alpha = -g$ in this case.

Failing this, can we write g_α *in terms of* g? Try the following. We know from Lemma 5.54 that α is a composition of transpositions, so let's think about what happens when we compute g_τ for any transposition $\tau = \begin{pmatrix} i & j \end{pmatrix}$. Without loss of generality, we may assume that $i < j$. Let k be another positive integer.

- We know that $x_i - x_j$ is a factor of g. After applying τ, $x_j - x_i$ is a factor of g_τ. This factor of g has changed in g_τ, since $x_j - x_i = -\left(x_i - x_j\right)$.
- If $i < j < k$, then $x_i - x_k$ and $x_j - x_k$ are factors of g. After applying τ, $x_i - x_k$ and $x_j - x_k$ are factors of g_τ. These factors of g have not changed in g_τ.
- If $k < i < j$, then $x_k - x_i$ and $x_k - x_j$ are factors of g. After applying τ, $x_k - x_j$ and $x_k - x_i$ are factors of g_τ.These factors of g have not changed in g_τ.
- If $i < k < j$, then $x_i - x_k$ and $x_k - x_j$ are factors of g. After applying τ, $x_j - x_k$ and $x_k - x_i$ are factors of g_τ. These factors of g have changed in g_τ, but the changes cancel each other out, since

$$\left(x_j - x_k\right)(x_k - x_i) = \left[-\left(x_k - x_j\right)\right][-(x_i - x_k)] = (x_i - x_k)\left(x_k - x_j\right).$$

Since $x_i - x_j$ is the only factor that changes sign *and* does not pair with another factor that changes sign, $g_\tau = -g$.

Return to g_α. Again, α is a composition of transpositions; suppose we can write it as $\alpha = \tau_1 \tau_2 \cdots \tau_n$. Then

$$g_\alpha = g_{\tau_1 \cdots \tau_n} = -g_{\tau_2 \cdots \tau_n} = (-1)^2 g_{\tau_3 \cdots \tau_n} = \cdots = (-1)^n g.$$

Since g_α is well-defined, and depends only on α, *and not on its representation,* it must be that

- if α can be written as an even number of transpositions, say $\alpha = \tau_1 \cdots \tau_{2m}$, then $g_\alpha = (-1)^{2m} g = g$, so α *cannot* be written as an odd number of transpositions; and
- if α can be written as an odd number of transpositions, say $\alpha = \tau_1 \cdots \tau_{2m+1}$, then $g_\alpha = (-1)^{2m+1} g = -g$, so α *cannot* be written as an even number of transpositions.

□

So Lemma (5.54) tells us that any permutation can be written as a composition of transpositions, and Theorem 5.56 tells us that for any given permutation, this number is always either an even or odd number of transpositions. This relationship merits a definition.

Definition 5.57: If a permutation can be written with an even number of permutations, then we say that the permutation is **even**. Otherwise, we say that the permutation is **odd**.

Example 5.58: The permutation $\rho = (1\,2\,3) \in S_3$ is even, since as we saw earlier $\rho = (1\,3)\,(1\,2)$. So is the permutation $\iota = (1) = (1\,2)\,(1\,2)$.

The permutation $\varphi = (2\,3)$ is odd. ◿

At this point we are ready to define a new group.

Definition 5.59: Let $n \in \mathbb{N}^+$ and $n \geq 2$. Let $A_n = \{\alpha \in S_n : \alpha \text{ is even}\}$. We call A_n **the set of alternating permutations**.

Remark 5.60: Although A_3 is not the same as "A_3" in Example 3.58 on page 69, the two are isomorphic because $D_3 \cong S_3$.

Theorem 5.61: *For all $n \geq 2$, $A_n < S_n$.*

PROOF: Let $n \geq 2$, and let $x, y \in A_n$. By the definition of A_n, we can write $x = \sigma_1 \cdots \sigma_{2m}$ and $y = \tau_1 \cdots \tau_{2n}$, where $m, n \in \mathbb{Z}$ and each σ_i or τ_j is a transposition. From Remark 5.55,

$$y^{-1} = \tau_{2n} \cdots \tau_1,$$

so

$$xy^{-1} = (\sigma_1 \cdots \sigma_{2m})\,(\tau_{2n} \cdots \tau_1).$$

Thus xy^{-1} can be written as a product of $2m + 2n = 2(m+n)$ transpositions; in other words, $xy^{-1} \in A_n$. By the Subgroup Theorem, $A_n < S_n$. Thus A_n is a group. □

How large is A_n, relative to S_n?

Theorem 5.62: *For any $n \geq 2$, there are half as many even permutations as there are permutations. That is, $|A_n| = |S_n|/2$.*

PROOF: We use Lagrange's Theorem from page 65, and show that there are two cosets of $A_n < S_n$.

Let $X \in S_n/A_n$. Let $\alpha \in S_n$ such that $X = \alpha A_n$. If α is an even permutation, then $X = A_n$. Otherwise, α is odd. Let β be any other odd permutation. Write out the odd number of transpositions of α^{-1}, followed by the odd number of transpositions of β, to see that $\alpha^{-1}\beta$ is an even permutation. Hence $\alpha^{-1}\beta \in A_n$, and by Lemma 3.29 on page 62 $\alpha A_n = \beta A_n$.

We have shown that any coset of A_n is either A_n itself or αA_n for some odd permutation α. Thus there are only two cosets of A_n in S_n: A_n itself, and the coset of odd permutations. By Lagrange's Theorem,

$$\frac{|S_n|}{|A_n|} = |S_n/A_n| = 2,$$

and a little algebra rewrites this equation to $|A_n| = |S_n|/2$. □

Corollary 5.63: *For any $n \geq 2$, $A_n \triangleleft S_n$.*

PROOF: You do it! See Exercise 5.68. □

There are a number of *exciting* facts regarding A_n that have to wait until a later class; in particular, A_n has a pivotal effect on whether one can solve polynomial equations by radicals (such as the quadratic formula). In comparison, the facts presented here are relatively dull.

I say that only in comparison, though. The facts presented here are quite striking in their own right: A_n is half the size of S_n, and it is a normal subgroup of S_n. If I call these facts "rather dull", that tells you just how interesting group theory can get!

Exercises.

Exercise 5.64: List the elements of A_2, A_3, and A_4 in cycle notation.

Exercise 5.65: Show that any permutation can be written as a product of transpositions.

Exercise 5.66: Show that the inverse of any transposition is a transposition.

Exercise 5.67: Show that the function swp α defined in Theorem 5.56 satisfies the property that for any two cycles α, β we have $(-1)^{\text{swp}\,(\alpha\beta)} = (-1)^{\text{swp}\,\alpha}\,(-1)^{\text{swp}\,\beta}$.

Exercise 5.68: Show that for any $n \geq 2$, $A_n \triangleleft S_n$.

5.6: The 15-puzzle

The 15-puzzle is similar to a toy you probably played with as a child. It looks like a 4×4 square, with all the squares numbered except one. The numbering starts in the upper left and proceeds consecutively until the lower right; the only squares that aren't in order are the last two, which are swapped:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

The challenge is to find a way to rearrange the squares so that they are in order, like so:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

The only permissible moves are those where one "slides" a square left, right, above, or below the empty square. Given the starting position above, the following moves are permissible:

1	2	3	4
5	6	7	8
9	10	11	12
13	15		14

or

1	2	3	4
5	6	7	8
9	10	11	
13	15	14	12

but the following moves are *not* permissible:

1	2	3	4
5	6	7	8
9	10		12
13	15	14	11

or

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

.

We will use groups of permutations to show that that the challenge is impossible.

How can we do this? Since the problem is one of rearranging a list of elements, it is a problem of permutations. Every permissible move consists of transpositions τ in S_{16} where:

- $\tau = \begin{pmatrix} x & y \end{pmatrix}$ where
  - $x < y$;
  - one of x or y is the position of the empty square in the current list; and
  - legal moves imply that either
    - $y = x + 1$ and $x \notin 4\mathbb{Z}$; or
    - $y = x + 4$.

Example 5.69: The legal moves illustrated above correspond to the transpositions

- $\begin{pmatrix} 15 & 16 \end{pmatrix}$, because square 14 was in position 15, and the empty space was in position 16: notice that $16 = 15 + 1$; and
- $\begin{pmatrix} 12 & 16 \end{pmatrix}$, because square 12 was in position 12, and the empty space was in position 16: notice that $16 = 12 + 4$ and since $[12] = [0]$ in $\mathbb{Z}_4$, $[16] = [0]$ in $\mathbb{Z}_4$.

The illegal moves illustrated above correspond to the transpositions

- $\begin{pmatrix} 11 & 16 \end{pmatrix}$, because square 11 was in position 11, and the empty space was in position 16: notice that $16 = 11 + 5$; and
- $\begin{pmatrix} 13 & 14 \end{pmatrix}$, because in the original configuration, neither 13 nor 14 contains the empty square.

Likewise $\begin{pmatrix} 12 & 13 \end{pmatrix}$ would be an illegal move in any configuration, because it crosses rows: even though $y = 13 = 12 + 1 = x + 1$, $x = 12 \in 4\mathbb{Z}$. ◿

How can we use this to show that it is impossible to solve 15-puzzle? Answering this requires several steps. The first shows that if there is a solution, it must belong to a particular group.

Lemma 5.70: *If there is a solution to the 15-puzzle, it is a permutation $\sigma \in A_{16}$, where A_{16} is the alternating group.*

PROOF: Any permissible move corresponds to a transposition τ as described above. Now any solution contains the empty square in the lower right hand corner. As a consequence, we must have the following: For any move $\begin{pmatrix} x & y \end{pmatrix}$, there must eventually be a corresponding move $\begin{pmatrix} x' & y' \end{pmatrix}$ where $[x'] = [x]$ in $\mathbb{Z}_4$ and $[y'] = [y]$ in $\mathbb{Z}_4$. If not:

- for above-below moves, the empty square could never return to the bottom row; and
- for left-right moves, the empty square could never return to the rightmost row unless we had some $\begin{pmatrix} x & y \end{pmatrix}$ where $[x] = [0]$ and $[y] \neq [0]$, a contradiction.

Thus moves come in pairs, and the solution is a permutation σ consisting of an even number of transpositions. By Theorem 5.56 on page 123 and Definitions 5.57 and 5.59, $\sigma \in A_{16}$. □

We can now show that there is no solution to the 15-puzzle.

Theorem 5.71: *The 15-puzzle has no solution.*

PROOF: By way of contradiction, assume that it has a solution σ. Then $\sigma \in A_{16}$. Because A_{16} is a subgroup of S_{16}, and hence a group in its own right, $\sigma^{-1} \in A_{16}$. Notice $\sigma^{-1}\sigma = \iota$, the permutation which corresponds to the configuration of the solution.

Now σ^{-1} is a permutation corresponding to the moves that change the arrangement

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

into the arrangement

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

which corresponds to $\begin{pmatrix} 14 & 15 \end{pmatrix}$. So regardless of the transpositions used in the representation of σ^{-1} , the composition must simplify to $\sigma^{-1} = \begin{pmatrix} 14 & 15 \end{pmatrix} \notin A_{16}$, a contradiction. □

As a historical note, the 15-puzzle was developed in 1878 by an American puzzlemaker, who promised a $1,000 reward to the first person to solve it. Most probably, the puzzlemaker knew that no one would ever solve it: if we account for inflation, the reward would correspond to $22,265 in 2008 dollars.[24]

The textbook [Lau03] contains a more general discussions of solving puzzles of this sort using algebra.

Exercises

Exercise 5.72: Determine which of these configurations, if any, is solvable by the same rules as the 15-puzzle:

1	2	3	4
5	6	7	8
9	10	12	11
13	14	15	

,

1	2	3	4
5	10	6	8
13	9	7	11
14	15	12	

,

3	6	4	7
1	2	12	8
5	15	10	14
9	13	11	

.

[24] According to the website `http://www.measuringworth.com/ppowerus/result.php`.

Chapter 6:
Number theory

The theory of groups was originally developed by mathematicians who were trying to answer questions about the roots of polynomials. From such beginnings it has grown to many applications that would seem completely unrelated to this topic. Some of the most widely-used applications in recent decades are in number theory, the study of properties of the integers.

This chapter introduces several of these applications of group theory to number theory. Section 6.1 fills some background with two of the most important tools in computational algebra and number theory. The first is a fundamental definition; the second is a fundamental algorithm. Both recur throughout the chapter, and later in the notes. Section 6.2 moves us to our first application of group theory, the *Chinese Remainder Theorem*, used thousands of years ago for the task of counting the number of soldiers who survived a battle. We will use it to explain the card trick described on page 1.

The rest of the chapter moves us toward Section 6.5, the RSA cryptographic scheme, a major component of internet communication and commerce. In Section 3.5 you learned of additive clockwork groups; in Section 6.3 you will learn of multiplicative clockwork groups. These allows us to describe in Section 6.4 the theoretical foundation of RSA, Euler's number and Euler's Theorem.

6.1: The Euclidean Algorithm

Until now, we've focused on division mostly when it made sense as an inverse operation (the Division Theorem being a notable exception). Many problems in number theory concern themselves with the integers as a monoid under multiplication, and division is important when it is possible. Recall that we say the integer a divides the integer b when we can find another integer x such that $ax = b$.

Definition 6.1: Let $m, n \in \mathbb{Z}$. We say that $d \in \mathbb{Z}$ is a **common divisor of m and n if $d \mid m$ and $d \mid n$.**

Example 6.2: Common divisors of 36 and 210 are 1, 2, 3, and 6.

In grade school, you learned how to compute the greatest common divisor of two integers. For example, given the integers 36 and 210, you should be able to determine that the greatest common divisor is 6. Computing greatest common divisors—not only of integers, but of other objects as well—turns out to be one of the most interesting problems in mathematics, with a large number of important applications.

But do they always exist?

Theorem 6.3: *Let $m, n \in \mathbb{Z}$. There exists a unique greatest common divisor of m, n.*

Algorithm 1. The Euclidean algorithm

inputs
  $m, n \in \mathbb{Z}$
outputs
  $\gcd(m, n)$
do
  Let $s = \max(m, n)$
  Let $t = \min(m, n)$
  Let $k = 1$
  repeat while $t \neq 0$
    Let $q, r_k \in \mathbb{Z}$ be the result of dividing s by t
    Let $s = t$
    Let $t = r$
    Increment k
  return s

PROOF: Let D be the set of common divisors of m, n that are also in $\mathbb{N}^+$. We know that $D \neq \emptyset$ because 1 divides any integer. We also know that any $d \in D$ must satisfy $d \leq \min(m, n)$; otherwise, the remainder from the Division Algorithm would be nonzero for at least one of m, n. Hence D is finite, and since any two integers can be compared, we can pick a maximal element of D, which is the greatest common divisor. □

How can we compute the greatest common divisor? One way is to make a list of all common divisors, and find the largest. To do that, we need to list all possible divisors of each integer, and identify the largest integer that appears in both lists. In practice, this takes a Very Long Time™, so we need a different method. One such method was described by the ancient Greek mathematician, Euclid.

Theorem 6.4 (The Euclidean Algorithm): *Let $m, n \in \mathbb{Z}$. We can compute the greatest common divisor of m, n in the following way:*

1. *Let $s = \max(m, n)$ and $t = \min(m, n)$.*
2. *Repeat the following steps until $t = 0$:*
   (a) *Let q be the quotient and r the remainder after dividing s by t.*
   (b) *Assign s the current value of t.*
   (c) *Assign t the current value of r.*

The final value of s is $\gcd(m, n)$.

It is common to write algorithms in a form called *pseudocode*. You can see this done in Algorithm 1.

Before proving that the Euclidean algorithm gives us a correct answer, let's do an example.

Example 6.5: We compute $\gcd(36,210)$. At the outset, we let $s = 210$ and $t = 36$. Subsequently:

1. Dividing 210 by 36 gives $q = 5$ and $r = 30$. Let $s = 36$ and $t = 30$.
2. Dividing 36 by 30 gives $q = 1$ and $r = 6$. Let $s = 30$ and $t = 6$.
3. Dividing 30 by 6 gives $q = 5$ and $r = 0$. Let $s = 6$ and $t = 0$.

Now that $t = 0$, we stop, and conclude that $\gcd(36,210) = s = 6$. This agrees with Example 6.2

To prove that the Euclidean algorithm generates a correct answer, we will argue that it computes $\gcd(m,n)$ by arguing that

$$\gcd(m,n) = \gcd(m,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{k-1},0)$$

where r_i is the remainder from division of the previous two integers in the chain, and r_{k-1} is the final non-zero remainder from division.

Lemma 6.6: *Let $s,t \in \mathbb{Z}$. Let q and r be the quotient and remainder, respectively, of division of s by t, as per the Division Theorem from page 9. Then* $\gcd(s,t) = \gcd(t,r)$.

Example 6.7: We can verify this using the numbers from Example 6.5. We know that $\gcd(36,210) = 6$. The remainder from division of 36 by 210 is $r = 36$. The lemma claims that $\gcd(36,210) = \gcd(36,30)$; it should be clear to you that $\gcd(36,30) = 6$.

The example also shows that the lemma doesn't care whether $m < n$ or vice versa. We turn to the proof.

PROOF: Let $d = \gcd(s,t)$. First we show that d is a divisor of r. From Definition 1.20 on page 10, there exist $a,b \in \mathbb{Z}$ such that $s = ad$ and $t = bd$. From the Division Theorem, we know that $s = qt + r$. Substitution gives us $ad = q(bd) + r$; rewriting the equation, we have

$$r = (a - qb)\,d.$$

Hence $d \mid r$.

Since d is a common divisor of s, t, and r, it is a common divisor of t and r. Now we show that $d = \gcd(t,r)$. Let $d' = \gcd(t,r)$; since d is also a common divisor of t and r, the definition of *greatest* common divisor implies that $d \leq d'$. Since d' is a common divisor of t and r, Definition 1.20 again implies that there exist $x,y \in \mathbb{Z}$ such that $t = d'x$ and $r = d'y$. Substituting into the equation $s = qt + r$, we have $s = q(d'x) + d'y$; rewriting the equation, we have

$$s = (qx + y)\,d'.$$

So $d' \mid s$. We already knew that $d' \mid t$, so d' is a common divisor of s and t.

Recall that $d = \gcd(s,t)$; since d' is also a common divisor of t and r, the definition of *greatest* common divisor implies that $d' \leq d$. Earlier, we showed that $d \leq d'$. Hence $d \leq d' \leq d$, which implies that $d = d'$.

Substitution gives the desired conclusion: $\gcd(s,t) = \gcd(t,r)$. □

We can finally prove that the Euclidean algorithm gives us a correct answer. This requires two stages, necessary for any algorithm.

1. **Correctness.** If the algorithm terminates, we have to guarantee that it terminates with the correct answer.
2. **Termination.** What if the algorithm doesn't terminate? If you look at the Euclidean algorithm, you see that one of its instructions asks us to repeat some steps "while $t \neq 0$." What if t never attains the value of zero? It's conceivable that its values remain positive at all times, or jump over zero from positive to negative values. That would mean that we never receive any answer from the algorithm, let alone a correct one.

We will identify both stages of the proof clearly. In addition, we will refer back to the the Division Theorem as well as the well-ordering property of the integers from Section 1.1; you may wish to review those.

PROOF OF THE EUCLIDEAN ALGORITHM: First we show that the algorithm terminates. The only repetition in the algorithm occurs in line 9. The first time we compute line 10, we compute the quotient q and remainder r of division of s by t. By the Division Theorem,

$$0 \leq r < t. \tag{10}$$

Denote this value of r by r_1. In the next lines we set s to t, then t to $r_1 = r$. Thanks to equation (10), the value of $t_{\text{new}} = r$ is smaller than $s_{\text{new}} = t_{\text{old}}$. If $t \neq 0$, then we return to line 10 and divide s by t, again obtaining a new remainder r. Denote this value of r by r_2; by the Division Theorem $r_2 = r < t$, so

$$0 \leq r_2 < r_1.$$

Let $R = \{r_1, r_2, \ldots\}$ be the set of remainders generated by the algorithm. Notice that $R \subsetneq \mathbb{N}$. The well-ordering property of the natural numbers implies that R has a smallest element r_i; this implies in turn that after i repetitions, the repetition must end; otherwise, we would generate $r_{i+1} < r_i$, contradicting the choice of r_i as the smallest element of R. Since the repetition end, the algorithm terminates.

Now we show that the algorithm terminates *with the correct answer*. If line 10 of the algorithm repeated k times, then $r_k = 0$. Apply Lemma 6.6 repeatedly to the remainders to obtain the chain of equalities

$$\begin{aligned}
\gcd(r_{k-1}, r_{k-2}) &= \gcd(r_{k-2}, r_{k-3}) \\
&= \gcd(r_{k-3}, r_{k-4}) \\
&\vdots \\
&= \gcd(r_2, r_1) \\
&= \gcd(r_1, s) \\
&= \gcd(t, s) \\
&= \gcd(m, n).
\end{aligned}$$

What is $\gcd(r_{k-1}, r_{k-2})$? Since $r_k = 0$, $r_{k-2} = q\,r_{k-1} + 0$, so $r_{k-1} \mid r_{k-2}$, making r_{k-1} a common divisor of r_{k-1} and r_{k-2}. No integer larger than r_{k-1} divides r_{k-1}, so the greatest common divisor of r_{k-1} and r_{k-2} must be r_{k-1}. Following the chain of equalities, we conclude that $\gcd(m,n) = r_{k-1}$: the Euclidean Algorithm terminates with the correct answer. □

Exercises.

Exercise 6.8: Compute the greatest common divisor of 100 and 140 by (a) listing all divisors, then identifying the largest; and (b) the Euclidean Algorithm.

Exercise 6.9: Compute the greatest common divisor of 4343 and 4429 by the Euclidean Algorithm.

Exercise 6.10: In Lemma 6.6 we showed that $\gcd(m,n) = \gcd(m,r)$ where r is the remainder after division of m by n. Prove the following more general statement: for all $m,n,q \in \mathbb{Z}$ $\gcd(m,n) = \gcd(m,m-qn)$.

6.2: The Chinese Remainder Theorem

In this section we explain how the card trick on page 1 works. The result is based on an old Chinese observation. Recall from Section 3.5 that for any $m \neq 0$ there exists a group $\mathbb{Z}_m$ of m elements, under the operation of adding, then taking remainder after division by m. We often write $[x]$ for the elements of $\mathbb{Z}_m$ if we want to emphasize that its elements are cosets.

Theorem 6.11 (The Chinese Remainder Theorem,[a] simple version): *Let $m,n \in \mathbb{Z}$ such that $\gcd(m,n) = 1$. Let $\alpha,\beta \in \mathbb{Z}$. There exists a solution $x \in \mathbb{Z}$ to the system of linear congruences*

$$\begin{cases} [x] = [\alpha] \text{ in } \mathbb{Z}_m; \\ [x] = [\beta] \text{ in } \mathbb{Z}_n; \end{cases}$$

and $[x]$ is unique in $\mathbb{Z}_N$ where $N = mn$.

[a] I asked Dr. Ding what the Chinese call this theorem. He looked it up in one of his books, and told me that they call it Sun Tzu's Theorem. But this is not the same Sun Tzu who wrote *The Art of War*.

Before giving a proof, let's look at an example.

Example 6.12 (The card trick): In the card trick, we took twelve cards and arranged them

- once in groups of three; and
- once in groups of four.

Each time, the player identified the *column* in which the mystery card lay. giving the remainders α from division by three and β from division by four. This corresponds to a system of linear congruences,

$$\begin{cases} [x] = [\alpha] \text{ in } \mathbb{Z}_3; \\ [x] = [\beta] \text{ in } \mathbb{Z}_4; \end{cases}$$

where x is the location of the mystery card. The simple version of the Chinese Remainder Theorem guarantees a solution for x, which is unique in $\mathbb{Z}_{12}$. Since there are only twelve cards, the solution is unique in the game: as long as the dealer can compute x, s/he can identify the card infallibly.

"Well, and good," you think, "but knowing only the existence of a solution seems rather pointless. I also need to know *how* to compute x, so that I can pinpoint the location of the card." It turns out that the *proof* of the Chinese Remainder Theorem will provide us with this method. However, the proof requires us to revisit our friend, the Euclidean Algorithm.

Theorem 6.13 (The Extended Euclidean Algorithm): *Let $m, n \in \mathbb{Z}$. There exist $a, b \in \mathbb{Z}$ such that $am + bn = \gcd(m, n)$. Both a and b can be found by reverse-substituting the chain of equations obtained by the repeated division in the Euclidean algorithm.*

Example 6.14: Recall from Example 6.5 the computation of $\gcd(210, 36)$. The divisions gave us a series of equations:

$$210 = 5 \cdot 36 + 30 \tag{11}$$
$$36 = 1 \cdot 30 + 6 \tag{12}$$
$$30 = 5 \cdot 6 + 0.$$

We concluded from the Euclidean Algorithm that $\gcd(210, 36) = 6$. The Extended Euclidean Algorithm gives us a way to find $a, b \in \mathbb{Z}$ such that $6 = 210a + 36b$. Start by rewriting equation (12):

$$36 - 1 \cdot 30 = 6. \tag{13}$$

This looks a little like what we want, but we need 210 instead of 30. Equation (11) allows us to rewrite 30 in terms of 210 and 36:

$$30 = 210 - 5 \cdot 36. \tag{14}$$

Substituting this result into equation (13), we have

$$36 - 1 \cdot (210 - 5 \cdot 36) = 6 \quad \Longrightarrow \quad 6 \cdot 36 + (-1) \cdot 210 = 6.$$

We have found integers $m = 6$ and $n = -1$ such that for $a = 36$ and $b = 210$, $\gcd(a, b) = 6$.

The method we applied in Example (6.14) is what we use both to prove correctness of the algorithm, and to find a and b in general.

PROOF OF THE EXTENDED EUCLIDEAN ALGORITHM: Look back at the proof of the Euclidean algorithm to see that it computes a chain of k quotients $\{q_i\}$ and remainders $\{r_i\}$ such that

$$\begin{aligned} m &= q_1 n + r_1 \\ n &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \qquad (15) \\ r_{k-2} &= q_k r_{k-1} + r_k \qquad (16) \\ r_{k-1} &= q_{k+1} r_k + 0 \\ \text{and } r_k &= \gcd(m,n). \end{aligned}$$

Rewrite equation 16 as

$$r_{k-2} = q_k r_{k-1} + \gcd(m,n).$$

Solving for $\gcd(m,n)$, we have

$$r_{k-2} - q_k r_{k-1} = \gcd(m,n). \qquad (17)$$

Solve for r_{k-1} in equation (15) to obtain

$$r_{k-3} - q_{k-1} r_{k-2} = r_{k-1}.$$

Substitute this into equation (17) to obtain

$$\begin{aligned} r_{k-2} - q_k \left(r_{k-3} - q_{k-1} r_{k-2}\right) &= \gcd(m,n) \\ \left(q_{k-1} + 1\right) r_{k-2} - q_k r_{k-3} &= \gcd(m,n). \end{aligned}$$

Proceeding in this fashion, we exhaust the list of equations, concluding by rewriting the first equation in the form $am + bn = \gcd(m,n)$ for some integers a, b. □

Pseudocode appears in Algorithm 2. One can also derive a method of computing both $\gcd(m,n)$ and the representation $am + bn = \gcd(m,n)$ simultaneously, which is to say, without having to reverse the process. We will not consider that here.

This ability to write $\gcd(m,n)$ as a sum of integer multiples of m and n is the key to unlocking the Chinese Remainder Theorem. Before doing so, we need an important lemma about numbers whose gcd is 1.

Lemma 6.15: *Let $d, m, n \in \mathbb{Z}$. If $m \mid nd$ and $\gcd(m,n) = 1$, then $m \mid d$.*

PROOF: Assume that $m \mid nd$ and $\gcd(m,n) = 1$. By definition of divisibility, there exists $q \in \mathbb{Z}$ such that $qm = nd$. Use the Extended Euclidean Algorithm to choose $a, b \in \mathbb{Z}$ such that

Algorithm 2. Extended Euclidean Algorithm

inputs
  $m, n \in \mathbb{N}^+$ such that $m > n$
outputs
  $\gcd(m,n)$ and $a, b \in \mathbb{Z}$ such that $\gcd(m,n) = am + bn$
do
  Let $r_0 = m$ and $r_1 = n$
  if $r_1 = 0$
    Let $d = r_0$, $a = 1$, $b = 0$
  else
    Let $i = 1$
    repeat while $r_i \neq 0$
      Increment i by 1
      Let q_i, r_i be the quotient and remainder from division of r_{i-2} by r_{i-1}
    Let $d = r_{i-1}$ and $p = r_{i-2} - q_i r_{i-1}$
    Decrement i by 1
    repeat while $i \geq 0$
      Substitute $r_i = r_{i-2} - q_i r_{i-1}$ into p
      Decrement i by 1
    Let a be the coefficient of r_0 in p, and b be the coefficient of r_1 in p
  return d, a, b

$am + bn = \gcd(m,n) = 1$. Multiplying both sides of this equation by d, we have

$$\begin{aligned}(am+bn)\,d &= 1\cdot d\\ amd + b\,(nd) &= d\\ adm + b\,(qm) &= d\\ (ad+bq)\,m &= d.\end{aligned}$$

Hence $m \mid d$. □

We finally prove the Chinese Remainder Theorem. You should study this proof carefully, not only to understand the theorem better, but because the proof tells you how to solve the system. You will want to recall Lemma 3.82 on page 74, which we use without pointing it out.

PROOF OF THE CHINESE REMAINDER THEOREM, SIMPLE VERSION: Recall that the system is

$$\begin{cases}[x] = [\alpha] \text{ in } \mathbb{Z}_m; & \text{and}\\ [x] = [\beta] \text{ in } \mathbb{Z}_n.\end{cases}$$

We have to prove two things: first, that a solution x exists; second, that $[x]$ is unique in $\mathbb{Z}_N$.

Existence: Because $\gcd(m,n) = 1$, the Extended Euclidean Algorithm tells us that there exist $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Rewriting this equation two different ways, we have $bn = 1 + (-a)\,m$ and $am = 1 + (-b)\,n$. In terms of cosets of subgroups of $\mathbb{Z}$, these two equations tell us that $bn \in 1 + m\mathbb{Z}$ and $am \in 1 + n\mathbb{Z}$. In the bracket notation, $[bn]_m = [1]_m$ and $[am]_n = [1]_n$. By Lemmas 3.79 and 3.82 on page 74, $[\alpha]_m = \alpha\,[1]_m = \alpha\,[bn]_m = [\alpha bn]_m$ and likewise $[\beta]_n = [\beta am]_n$. Apply similar reasoning to see that $[\alpha bn]_n = [0]_n$ and $[\beta am]_m = [0]_m$ in $\mathbb{Z}_m$. Hence,

$$\begin{cases}[\alpha bn + \beta am]_m = [\alpha]_m; \text{ and}\\ [\alpha bn + \beta am]_n = [\beta]_n.\end{cases}$$

Thus $x = \alpha bn + \beta am$ is a solution to the system.

Uniqueness: Suppose that there exist $[x], [y] \in \mathbb{Z}_N$ that both satisfy the system. Since $[x] = [y]$ in $\mathbb{Z}_m$, $[x-y] = [0]$, so $m \mid (x-y)$. By definition of divisibility, there exists $q \in \mathbb{Z}$ such that $mq = x - y$. Since $[x]_n = [y]_n$, $[x-y]_n = [0]_n$, and by Lemma 3.85 on page 75, $n \mid (x-y)$. By substitution, $n \mid mq$. By Lemma 6.15, $n \mid q$. By definition of divisibility, there exists $q' \in \mathbb{Z}$ such that $q = nq'$. By substitution,

$$x - y = mq = mnq' = Nq'.$$

Hence $N \mid (x-y)$, and again by Lemma 3.85 $[x]_N = [y]_N$, which means that the solution x is unique in $\mathbb{Z}_N$, as desired. □

Pseudocode to solve the Chinese Remainder Theorem appears as Algorithm 3 on the following page.

Algorithm 3. Solution to Chinese Remainder Theorem, simple version

inputs
  $m, n \in \mathbb{Z}$ such that $\gcd(m,n) = 1$
  $\alpha, \beta \in \mathbb{Z}$
outputs
  $x \in \mathbb{Z}$ satisfying the Chinese Remainder Theorem
do
  Use the Extended Euclidean Algorithm to find $a, b \in \mathbb{Z}$ such that $am + bn = 1$
  return $[\alpha bn + \beta am]_N$

Example 6.16: The algorithm of Corollary 3 finally explains the method of the card trick. We have $m = 3$, $n = 4$, and $N = 12$. Suppose that the player indicates that his card is in the first column when they are grouped by threes, and in the third column when they are grouped by fours; then $\alpha = 1$ and $\beta = 3$.

Using the Extended Euclidean Algorithm, we find that $a = -1$ and $b = 1$ satisfy $am + bn = 1$; hence $am = -3$ and $bn = 4$. We can therefore find the mystery card by computing

$$x = 1 \cdot 4 + 3 \cdot (-3) = -5;$$

by adding 12, we obtain another representation for $[x]$ in $\mathbb{Z}_{12}$:

$$[x] = [-5 + 12] = [7],$$

which implies that the player chose the 7th card. In fact, $[7] = [1]$ in $\mathbb{Z}_3$, and $[7] = [3]$ in $\mathbb{Z}_4$, which agrees with the information given. ◿

The Chinese Remainder Theorem can be generalized to larger systems with more than two equations under certain circumstances.

Theorem 6.17 (Chinese Remainder Theorem on $\mathbb{Z}$): *Let $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ and assume that $\gcd(m_i, m_j) = 1$ for all $1 \le i < j \le n$. Let $\alpha_1, \alpha_2, \ldots \alpha_n \in \mathbb{Z}$. There exists a solution $x \in \mathbb{Z}$ to the system of linear congruences*

$$\begin{cases} [x] &= [\alpha_1] \text{ in } \mathbb{Z}_{m_1}; \\ [x] &= [\alpha_2] \text{ in } \mathbb{Z}_{m_2}; \\ &\vdots \\ [x] &= [\alpha_n] \text{ in } \mathbb{Z}_{m_n}; \end{cases}$$

and $[x]$ is unique in $\mathbb{Z}_N$ where $N = m_1 m_2 \cdots m_n$.

Before we can prove this version of the Chinese Remainder Theorem, we need to make an observation of $m_1, m_2, \ldots, m_n$.

Lemma 6.18: *Let $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ such that $\gcd\left(m_i, m_j\right) = 1$ for all $1 \leq i < j \leq n$. For each $i = 1, 2, \ldots, n$ define $N_i = N/m_i$ where $N = m_1 m_2 \cdots m_n$; that is, N_i is the product of all the m's except m_i. Then $\gcd(m_i, N_i) = 1$.*

PROOF: We show that $\gcd(m_1, N_1) = 1$; for $i = 2, \ldots, n$ the proof is similar.

Use the Extended Euclidean Algorithm to choose $a, b \in \mathbb{Z}$ such that $am_1 + bm_2 = 1$. Use it again to choose $c, d \in \mathbb{Z}$ such that $cm_1 + dm_3 = 1$. Then

$$\begin{aligned} 1 &= (am_1 + bm_2)(cm_1 + dm_3) \\ &= (acm_1 + adm_3 + bcm_2)m_1 + (bd)(m_2 m_3). \end{aligned}$$

Let $x = \gcd(m_1, m_2 m_3)$; the previous equation shows that x is also a divisor of 1. However, the only divisors of 1 are ± 1; hence $x = 1$. We have shown that $\gcd(m_1, m_2 m_3) = 1$.

Rewrite the equation above as $1 = a'm_1 + b'm_2 m_3$; notice that $a', b' \in \mathbb{Z}$. Use the Extended Euclidean Algorithm to choose $e, f \in \mathbb{Z}$ such that $em_1 + fm_4 = 1$. Then

$$\begin{aligned} 1 &= (a'm_1 + b'm_2 m_3)(em_1 + fm_4) \\ &= (a'em_1 + a'fm_4 + b'em_2 m_e)m_1 + (b'f)(m_2 m_3 m_4). \end{aligned}$$

An argument similar to the one above shows that $\gcd(m_1, m_2 m_3 m_4) = 1$.

Repeating this process with each m_i, we obtain $\gcd(m_1, m_2 m_3 \cdots m_n) = 1$. Since $N_1 = m_2 m_3 \cdots m_n$, we have $\gcd(m_1, N_1) = 1$. □

We can now prove the Chinese Remainder Theorem on $\mathbb{Z}$.

PROOF OF THE CHINESE REMAINDER THEOREM ON $\mathbb{Z}$.: *Existence:* Write $N_i = N/m_i$ for $i = 1, 2, \ldots, n$. By Lemma 6.18, $\gcd(m_i, N_i) = 1$. Use the Extended Euclidean Algorithm to compute $a_1, b_1, a_2, b_2, \ldots, a_n, b_n$ such that

$$\begin{aligned} a_1 m_1 + b_1 N_1 &= 1 \\ a_2 m_2 + b_2 N_2 &= 1 \\ &\vdots \\ a_n m_n + b_n N_n &= 1. \end{aligned}$$

Put $x = \alpha_1 b_1 N_1 + \alpha_2 b_2 N_2 + \cdots + \alpha_n b_n N_n$. Now $b_1 N_1 = 1 + (-a_1)m_1$ so $[b_1 N_1] = [1]$ in $\mathbb{Z}_{m_1}$, so $[\alpha_1 b_1 N_1] = [\alpha_1]$ in $\mathbb{Z}_{m_1}$. Moreover, for $i = 2, 3, \ldots, n$ inspection of N_i verifies that $m_1 \mid N_i$, so $\alpha_i b_i N_i = q_i m_1$ for some $q_i \in \mathbb{Z}$, implying that $[\alpha_i b_i N_i]_{m_1} = [0]_{m_1}$. Hence

$$\begin{aligned} [x] &= [\alpha_1 b_1 N_1 + \alpha_2 b_2 N_2 + \cdots + \alpha_n b_n N_n] \\ &= [\alpha_1] + [0] + \cdots + [0] \end{aligned}$$

in $\mathbb{Z}_{m_1}$, as desired. A similar argument shows that $[x] = [\alpha_i]$ in $\mathbb{Z}_{m_i}$ for $i = 2, 3, \ldots, n$.

Uniqueness: As in the previous case, let $[x], [y]$ be two solutions to the system in $\mathbb{Z}_N$. Then $[x-y] = [0]$ in $\mathbb{Z}_{m_i}$ for $i = 1, 2, \ldots, n$, implying that $m_i \mid (x-y)$ for $i = 1, 2, \ldots, n$.

Since $m_1 \mid (x-y)$, the definition of divisibility implies that there exists $q_1 \in \mathbb{Z}$ such that $x - y = m_1 q_1$.

Since $m_2 \mid (x-y)$, substitution implies $m_2 \mid m_1 q_1$, and Lemma 6.15 implies that $m_2 \mid q_1$. The definition of divisibility implies that there exists $q_2 \in \mathbb{Z}$ such that $q_1 = m_2 q_2$. Substitution implies that $x - y = m_1 m_2 q_2$.

Since $m_3 \mid (x-y)$, substitution implies $m_3 \mid m_1 m_2 q_2$. By Lemma 6.18, $\gcd(m_1 m_2, m_3) = 1$, and Lemma 6.15 implies that $m_3 \mid q_2$. The definition of divisibility implies that there exists $q_3 \in \mathbb{Z}$ such that $q_2 = m_3 q_3$. Substitution implies that $x - y = m_1 m_2 m_3 q_3$.

Continuing in this fashion, we show that $x - y = m_1 m_2 \cdots m_n q_n$ for some $q_n \in \mathbb{Z}$. By substition, $x - y = N q_n$, so $[x-y] = [0]$ in $\mathbb{Z}_N$, so $[x] = [y]$ in $\mathbb{Z}_n$. That is, the solution to the system is unique in $\mathbb{Z}_N$. □

The algorithm to solve such systems is similar to that given for the simple version, in that it can be obtained from the proof of existence of a solution.

Exercises

Exercise 6.19: Solve the system of linear congruences

$$\begin{cases} [x] &= [2] \text{ in } \mathbb{Z}_4; \\ [x] &= [2] \text{ in } \mathbb{Z}_9. \end{cases}$$

Express your answer so that $0 \leq x < 36$.

Exercise 6.20: Solve the system of linear congruences

$$\begin{cases} [x] &= [2] \text{ in } \mathbb{Z}_5; \\ [x] &= [2] \text{ in } \mathbb{Z}_6; \\ [x] &= [2] \text{ in } \mathbb{Z}_7. \end{cases}$$

Exercise 6.21: Solve the system of linear congruences

$$\begin{cases} [x] &= [33] \text{ in } \mathbb{Z}_{16}; \\ [x] &= [-4] \text{ in } \mathbb{Z}_{33}; \\ [x] &= [17] \text{ in } \mathbb{Z}_{504}. \end{cases}$$

This problem is a little tougher than the previous, since $\gcd(16, 504) \neq 1$ and $\gcd(33, 504) \neq 1$.

Exercise 6.22: Give directions for a similar card trick on all 52 cards, where the cards are grouped first by 4's, then by 13's. Do you think this would be a practical card trick?

Exercise 6.23: Is it possible to modify the card trick to work with only ten cards instead of 12? If so, how; if not, why not?

Exercise 6.24: Is it possible to modify the card trick to work with only eight cards instead of 12? If so, how; if not, why not?

Exercise 6.25: Let $m, n \in \mathbb{Z}$. The Extended Euclidean Algorithm (Theorem 6.13) shows that we can find $a, b \in \mathbb{Z}$ such that $am + bn = \gcd(m, n)$. It is not necessarily true that $am + bn = \gcd(m, n)$ for any $a, b \in \mathbb{Z}$. However, we can show the following. Let $S = \{am + bn : a, b \in \mathbb{Z}\}$, and $M = S \cap \mathbb{N}$. Since M is a subset of $\mathbb{N}$, the well-ordering property of $\mathbb{Z}$ implies that it has a smallest element; call it d. Show that $d = \gcd(m, n)$.

6.3: Multiplicative clockwork groups

Recall that $\mathbb{Z}_n$ is an additive group, but not multiplicative. In this section we find a subset of $\mathbb{Z}_n$ that we can turn into a multiplicative group. Before that, we need a little more number theory, starting with a definition which you probably don't expect.

Definition 6.26: Let $n \in \mathbb{N}^+$ and assume $n > 1$. We say that n is **irreducible** if the only integers that divide n are ± 1 and $\pm n$.

You may read this and think, "Oh, he's talking about prime numbers." Yes and no. We'll have a *lot* to say about that, eventually.

Example 6.27: The integer 36 is not irreducible, because $36 = 6 \times 6$. The integer 7 is irreducible, because the only integers that divide 7 are ± 1 and ± 7.

One useful aspect to irreducible integers is that, aside from ± 1, any integer is divisible by at least one irreducible integer.

Theorem 6.28: *Let $n \in \mathbb{Z}$, $n \neq \pm 1$. There exists at least one irreducible integer p such that $p \mid n$.*

PROOF: *Case 1:* If $n = 0$, then 2 is a divisor of n, and we are done.

Case 2: Assume that $n > 1$. If n is not irreducible, then by definition $n = a_1 b_1$ such that $a_1, b_1 \in \mathbb{Z}$ and $a_1, b_1 \neq \pm 1$. Without loss of generality, we may assume that $a_1, b_1 \in \mathbb{N}^+$ (otherwise both a, b are negative and we can replace them with their opposites). Observe further that $a_1 < n$ (this is a consequence of Exercise 1.26 on page 11). If a_1 is irreducible, then we are done; otherwise, we can write $a_1 = a_2 b_2$ where $a_2, b_2 \in \mathbb{N}^+$ and $a_2 < a_1$.

Continuing in this fashion, we build a set $S = \{a_1, a_2, \ldots,\} \subseteq \mathbb{N}^+$; by the well-ordering property of $\mathbb{N}$, S has a least element. Notice that $a_i > a_{i+1}$ for each i, so the least element must be the a_i with maximal index i; call it a_m. We claim that a_m is irreducible; otherwise, we could factor it and add a smaller element to S, as we did for $a_1, a_2, \ldots$. Thus

$$n = a_1 b_1 = (a_2 b_2)\, b_1 = \cdots = (a_m b_m)\left(b_{m-1} \cdots b_1\right) = a_m \left(b_{m-1} \cdots b_1\right).$$

That is, a_m is an irreducible integer that divides n.

Case 3: Assume that $n < 1$. Then $n = -(-n)$; since $-n > 1$, there exists an irreducible integer p such that $p \mid (-n)$, say $-n = qp$ for some $q \in \mathbb{Z}$. By substitution, $n = -qp = (-q)p$, so $p \mid n$. □

Let's turn now to the term you might have expected for the above notion: a *prime* number. For reasons that you will discover later, we actually associate a different notion with this term.

Definition 6.29: Let $p \in \mathbb{N}^+$ and assume $p > 1$. We say that p is **prime** if for any two integers a, b

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ or } p \mid b.$$

Example 6.30: Let $a = 68$ and $b = 25$. It is easy to recognize that 10 divides $ab = 1700$. However, 10 divides neither a nor b, so 10 is not a prime number.

It is also easy to recognize that 17 divides $ab = 1700$. Here, 17 must divide one of a or b; in fact, $17 \times 4 = 68 = a$. If we were to look at every possible product ab divisible by 17, we would find that 17 always divides one of the factors a or b. Thus, 17 is prime.

If the next-to-last sentence in the example, bothers you, *good.* I've claimed something about every product divisible by 17, but haven't explained why that is true. In other words, I've cheated. I'm not supposed to do that.

Fair enough; if I'm going to claim that 17 is prime, I need a better explanation than my say-so. I also need a better explanation than, "if we were to look at every possible product," because there are an infinite number of possibilities to consider, and we can't do that in finite time. I need a finite criterion.

To get this criterion, I'll return to the notion of an irreducible number. Previously, you were probably taught that a *prime* number was what we have here called *irreducible.* Now, I've given two definitions that seem different.

Could it be that the definitions are *distinctions without a difference?* In fact, they are equivalent!

Theorem 6.31: *Any integer is irreducible if and only if it is prime.*

PROOF: There are two parts to this proof. You will show in Exercise 6.43 that if an integer is prime, then it is irreducible. Here we show the converse.

Let $n \in \mathbb{N}^+$ and assume that $n > 1$ and n is irreducible. To show that n is prime, we must take arbitrary $a, b \in \mathbb{Z}$ and show that if $n \mid ab$, then $n \mid a$ or $n \mid b$. Therefore, let $a, b \in \mathbb{Z}$ and assume that $n \mid ab$. Without loss of generality, assume that $n \nmid a$; we must show that $n \mid b$. Since $n \nmid a$ and n is irreducible, the only common factors of n and a are ± 1; thus, $\gcd(n, a) = 1$. By Lemma 6.15, $n \mid b$. Hence n is prime. □

If the two definitions are equivalent, why would we give a different definition? It turns out that the concepts are equivalent *for the integers,* but not for other sets; you will see this later in Sections 8.3 and 9.1.

The following theorem is a cornerstone of Number Theory.

Theorem 6.32 (The Fundamental Theorem of Arithmetic): *Let $n \in \mathbb{N}^+$. If $n \neq 1$, we can write*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

where $p_1, p_2, \ldots, p_r$ are irreducible and $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$. The representation is unique if we order $p_1 < p_2 < \ldots < p_n$.

Since prime integers are irreducible and vice versa, you can replace "irreducible" by "prime" and obtain the expression of this theorem found more commonly in number theory textboks. We use "irreducible" here to lay the groundwork for Definition 9.15 on page 218.

PROOF: The proof has two parts: a proof of existence and a proof of uniqueness.

Existence: We proceed by induction on positive integers not equal to two.

Inductive base: If $n = 2$, then n is irreducible, and we are finished.

Inductive hypothesis: Assume that the integers $2, 3, \ldots, n-1$ satisfy the theorem.

Inductive step: If n is irreducible, then we are finished. Otherwise, n is not irreducible. By Lemma 6.28, there exists an irreducible integer p_1 such that $p_1 \mid n$ and $p \neq \pm 1, n$. Choose the largest $\alpha_1 \in \mathbb{N}$ such that $p_1^{\alpha_1} \mid n$. (Such a largest integer exists since otherwise

$$\left\{ \frac{n}{p_1}, \frac{n}{p_1^2}, \ldots \right\}$$

would be a subset of $\mathbb{N}$ with no smallest element, contradicting the well-ordering of $\mathbb{N}$.) Use the definition of divisibility (Definition 1.20 on page 10) to find $q \in \mathbb{Z}$ such that $n = q p_1^{\alpha_1}$. By the definition of irreducible, we know that $p_1 \neq 1$, so $q < n$. Since p_1 is not negative, $q \in \mathbb{N}^+$ and $q \neq 1$. Thus q satisfies the inductive hypothesis, and we can write $q = p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}$. Thus

$$n = q p_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

as claimed.

Uniqueness: Here we use the fact that irreducible numbers are also prime (Lemma 6.31). Assume that $p_1 < p_2 < \cdots < p_r$ and we can factor n as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}.$$

Without loss of generality, we may assume that $\alpha_1 \leq \beta_1$. It follows that

$$p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r} = p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_r^{\beta_r}.$$

This equation implies that $p_1^{\beta_1 - \alpha_1}$ divides the expression on the left hand side of the equation. Since p_1 is irreducible, hence prime, $\beta_1 - \alpha_1 > 0$ implies that p_1 divides one of $p_2, p_3, \ldots, p_r$. This contradicts the irreducibility of $p_2, p_3, \ldots, p_r$. Hence $\beta_1 - \alpha_1 = 0$. A similar argument

shows that $\beta_i = \alpha_i$ for all $i = 1, 2, \ldots, r$; hence the representation of n as a product of irreducible integers is unique. □

To turn $\mathbb{Z}_n$ into a multiplicative group, we would like to define multiplication in an "intuitive" way. By "intuitive", we mean that we would like to say

$$[2] \cdot [3] = [2 \cdot 3] = [6] = [1] .$$

Before we can address the questions of whether $\mathbb{Z}_n$ can become a group under this operation, we have to remember that cosets can have various representations, and different representations may lead to different results: is this operation well-defined?

Lemma 6.33: *The proposed multiplication of elements of $\mathbb{Z}_n$ as*

$$[a]\,[b] = [ab]$$

is well-defined.

PROOF: Let $x, y \in \mathbb{Z}_n$ and represent $x = [a] = [c]$ and $y = [b]$. Then

$$xy = [a]\,[b] = [ab] \quad \text{and} \quad xy = [c]\,[b] = [cb] .$$

We need to show that $[ab] = [cb]$. Since these are sets, we have to show that each is a subset of the other.

By assumption, $[a] = [c]$; this notation means that $a + n\mathbb{Z} = c + n\mathbb{Z}$. Lemma 3.29 on page 62 tells us that $a - c \in n\mathbb{Z}$. Hence $a - c = nt$ for some $t \in \mathbb{Z}$. Now $(a-c)\,b = nu$ where $u = tb \in \mathbb{Z}$, so $ab - cb \in n\mathbb{Z}$. Lemma 3.29 again tells us that $[ab] = [cb]$ as desired, so the proposed multiplication of elements in $\mathbb{Z}_n$ is well-defined. □

Example 6.34: Recall that $\mathbb{Z}_5 = \mathbb{Z}/\langle 5 \rangle = \{[0], [1], [2], [3], [4]\}$. The elements of $\mathbb{Z}_5$ are cosets; since $\mathbb{Z}$ is an additive group, we were able to define easily an addition on $\mathbb{Z}_5$ that turns it into an additive group in its own right.

Can we also turn it into a multiplicative group? We need to identify an identity, and inverses. Certainly $[0]$ won't have a multiplicative inverse, but what about $\mathbb{Z}_5 \setminus \{[0]\}$? This generates a multiplication table that satisfies the properties of an abelian (but non-additive) group:

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

That is a group! We'll call it $\mathbb{Z}_5^*$.

In fact, $\mathbb{Z}_5^* \cong \mathbb{Z}_4$; they are both the cyclic group of four elements. In $\mathbb{Z}_5^*$, however, the nominal operation is multiplication, whereas in $\mathbb{Z}_4$ the nominal operation is addition.

You might think that this trick of dropping zero and building a multiplication table always works, *but it doesn't*.

Example 6.35: Recall that $\mathbb{Z}_4 = \mathbb{Z}/\langle 4\rangle = \{[0],[1],[2],[3]\}$. Consider the set $\mathbb{Z}_4\backslash\{[0]\} = \{[1],[2],[3]\}$. The multiplication table for this set *is not closed* because

$$[2]\cdot[2] = [4] = [0] \notin \mathbb{Z}_4\backslash\{[0]\}.$$

The next natural question: Is *any* subset of $\mathbb{Z}_4$ a multiplicative group? Try to fix the problem by removing [2] as well. This time the multiplication table for $\mathbb{Z}_4\backslash\{[0],[2]\} = \{[1],[3]\}$ works out:

$\times$	1	3
1	1	3
3	3	1

That is a group! We'll call it $\mathbb{Z}_4^*$.

In fact, $\mathbb{Z}_4^* \cong \mathbb{Z}_2$; they are both the cyclic group of two elements. In $\mathbb{Z}_4^*$, however, the operation is multiplication, whereas in $\mathbb{Z}_2$, the operation is addition.

You can determine for yourself that $\mathbb{Z}_2\backslash\{[0]\} = \{[1]\}$ and $\mathbb{Z}_3\backslash\{[0]\} = \{[1],[2]\}$ are also multiplicative groups. In this case, as in $\mathbb{Z}_5^*$, we need remove only 0. For $\mathbb{Z}_6$, however, we have to remove nearly all the elements! We only get a group from $\mathbb{Z}_6\backslash\{[0],[2],[3],[4]\} = \{[1],[5]\}$.

Why do we need to remove more numbers from $\mathbb{Z}_n$ for some values of n than for others? Aside from zero, which clearly has no inverse under the operation specified, the elements we've had to remove are invariably those elements whose multiplication tries to re-introduce zero into the group. That already seems strange: we have non-zero elements that, when multiplied by other non-zero elements, produce a product of zero. Here is an instance where $\mathbb{Z}_n$ superficially behaves *very differently* from the integers. This is important enough to give a special name.

Definition 6.36: We say that $x, y \in \mathbb{Z}_n$ are **zero divisors** if $xy = [0]$.

In other words, zero divisors are non-zero elements of $\mathbb{Z}_n$ that violate the zero-product property of multiplication.

Can we find a criterion to detect this?

Lemma 6.37: *Let $x \in \mathbb{Z}_n$, with $x \neq [0]$. The following are equivalent:*

(A) *x is a zero divisor.*

(B) *There exists non-zero $y \in \mathbb{Z}_n$ such that $xy = [0]$.*

(C) *For any representation $[a]$ of x, $\gcd(a,n) \neq 1$.*

PROOF: (A) is equivalent to (B) by Definition 6.37.

That (C) implies (B): Let $[a]$ be any representation of x, and assume that a and n share a common divisor, d. Use the definition of divisibility to choose $q \in \mathbb{Z}$ such that $n = qd$. Likewise choose t such that $a = td$. Then

$$qx = q[a] = q[td].$$

Lemma 3.82 implies that

$$q[td] = [qtd] = t[qd] = t[n] = [0].$$

We conclude that if we let $y = [q]$, then $xy = [a]\,[q]$, which we just showed was $[0]$.

That (B) implies (C): Let $y \in \mathbb{Z}_n$, and suppose that $y \neq [0]$ but $xy = [0]$. Choose $a, b \in \mathbb{Z}$ such that $x = [a]$ and $y = [b]$. Since $xy = [0]$, Lemma 3.85 implies that $n \mid (ab - 0)$, so we can find $k \in \mathbb{Z}$ such that $ab = kn$. Let p_0 be any irreducible number that divides n. Then p_0 also divides kn. Since $kn = ab$, we see that $p_0 \mid ab$. Since p_0 is irreducible, hence prime, it must divide one of a or b. If it divides a, then a and n have a common divisor p_0 that is not ± 1, and we are done; otherwise, it divides b. Use the definition of divisibility to find $n_1, b_1 \in \mathbb{Z}$ such that $n = n_1 p_0$ and $a = b_1 p_0$; it follows that $ab_1 = kn_1$. Again, let p_2 be any irreducible number that divides n_2; the same logic implies that p_2 divides ab_2; being prime, p_2 must divide a or b_2.

As long as we can find prime divisors of the n_i that divide b_i but not a, we repeat this process to find triplets $(n_2, b_2, p_2), (n_3, b_3, p_3), \ldots$ satisfying for all i the properties

- $ab_i = kn_i$; and
- $b_{i-1} = p_i b_i$ and $n_{i-1} = p_i n_i$.

By the well-ordering property, the set $\{n, n_1, n_2, \ldots\}$ has a least element; since $n > n_1 > n_2 \cdots$, we cannot continue finding pairs indefinitely, and must terminate with the least element (n_r, b_r). Observe that

$$b = p_1 b_1 = p_1 (p_2 b_2) = \cdots = p_1 (p_2 (\cdots (p_r b_r))) \tag{18}$$

and

$$n = p_1 n_1 = p_1 (p_2 n_2) = \cdots = p_1 (p_2 (\cdots (p_r n_r))).$$

Case 1. If $n_r > 1$, then n and a must have a common divisor that is not ± 1.

Case 2. If $n_r = 1$, then $n = p_1 p_2 \cdots p_r$. By substitution into equation 18, $b = nb_r$. By the definition of divisibility, $n \mid b$. By the definition of $\mathbb{Z}_n$, $y = [b] = [0]$. This contradicts the hypothesis.

Hence n and a share a common divisor that is not ± 1. □

We can now make a *multiplicative* group out of the set of elements of $\mathbb{Z}_n$ that do not violate the zero product rule.

Definition 6.38: Let $n \in \mathbb{Z}$, with $n > 1$. Let $x, y \in \mathbb{Z}_n$, and represent $x = [a]$ and $y = [b]$.

1. Define a multiplication operation on $\mathbb{Z}_n$ by $xy = [ab]$.
2. Define the set $\mathbb{Z}_n^*$ to be the set of elements in $\mathbb{Z}_n$ that are neither zero nor zero divisors. That is,

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \setminus \{0\} : \forall y \in \mathbb{Z}_n \; xy \neq [0]\}.$$

We claim that $\mathbb{Z}_n^*$ is a group under multiplication. Note that while it is a sub*set* of $\mathbb{Z}_n$, it is not a sub*group*: $\mathbb{Z}_n$ is not a group under multiplication, and subgroups maintain the operation of the parent group.

Theorem 6.39: *$\mathbb{Z}_n^*$ is an abelian group under its multiplication.*

PROOF: We showed in Lemma 6.33 that the operation is well-defined. We check each of the requirements of a group:

(closure) Let $x, y \in \mathbb{Z}_n^*$; represent $x = [a]$ and $y = [b]$. By definition of $\mathbb{Z}_n^*$, x and y are not zero divisors. Assume to the contrary that $xy \notin \mathbb{Z}_n^*$; that would imply either that $xy = [0]$ or xy is a zero divisor. In either case, $\gcd(ab, n) = n \neq 1$. Let p be an irreducible integer that divides n (p exists on account of the Fundamental Theorem of Arithmetic). Since n divides ab and p divides n, p also divides ab. Since irreducible integers are prime, and $p \mid ab$, by definition $p \mid a$ or $p \mid b$. Without loss of generality, $p \mid a$. But now $\gcd(a, n) \geq p > 1$, so that a and n have a common divisor. Lemma 6.37 implies that $x = [a]$ is a zero divisor, but this contradicts the choice of $x \in \mathbb{Z}_n^*$. As a result, $xy = [ab] \in \mathbb{Z}_n^*$.

(associativity) Let $x, y, z \in \mathbb{Z}_n^*$; represent $x = [a]$, $y = [b]$, and $z = [c]$. Then

$$x(yz) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = (xy)z.$$

(identity) We claim that $[1]$ is the identity of this group. Let $x \in \mathbb{Z}_n^*$; represent $x = [a]$. Then

$$x \cdot [1] = [a \cdot 1] = [a] = x;$$

a similar argument shows that $[1] \cdot x = x$.

We still have to show that $[1] \in \mathbb{Z}_n^*$, but this is easy: $\gcd(1, n) = 1$, so Lemma 6.37 tells us that $[1]$ is not a zero divisor. Hence $[1] \in \mathbb{Z}_n^*$.

(inverse) Let $x \in \mathbb{Z}_n^*$. By definition of $\mathbb{Z}_n^*$, $x \neq 0$ and x is not a zero divisor in $\mathbb{Z}_n$. Represent $x = [m]$. Since $x \neq 0$, $n \nmid m$. From Lemma 6.37, m and n have no common divisors except ± 1; hence $\gcd(m, n) = 1$. Using the Extended Euclidean Algorithm, find $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Hence

$$\begin{aligned} am &= 1 + n(-b) \\ \therefore am &\in 1 + n\mathbb{Z} \\ \therefore am + n\mathbb{Z} &= 1 + n\mathbb{Z} \\ \therefore [am] &= [1] \\ \therefore [a][m] &= [1] \end{aligned}$$

by (respectively) the definition of the coset $1 + n\mathbb{Z}$, Lemma 3.29 on page 62, the notation for elements of $\mathbb{Z}_n$, and the definition of multiplication in $\mathbb{Z}_n^*$ given above. Let $y = [a]$; by substitution, the last equation becomes

$$yx = [1].$$

But is $a \in \mathbb{Z}_n^*$? Recall that $am + bn = 1$; any common divisor of a and n

would divide the left hand side of this equation, so it would also divide the right. But only ± 1 divide 1, so $\gcd(a,n) = 1$. So $y \in \mathbb{Z}_n^*$, and x has an inverse in $\mathbb{Z}_n^*$.

(commutativity) Let $x, y \in \mathbb{Z}_n^*$; represent $x = [a]$ and $y = [b]$. Then

$$xy = [ab] = [ba] = yx.$$

□

By removing elements that share non-trivial common divisors with n, we have managed to eliminate those elements that do not satisfy the zero-product rule, and would break closure by trying to re-introduce zero in the multiplication table. We have thereby created a clockwork group for multiplication, $\mathbb{Z}_n^*$.

Example 6.40: We look at $\mathbb{Z}_{10}^*$. To find its elements, we collect the elements of $\mathbb{Z}_{10}$ that are not zero divisors; by Lemma 6.37, those are the elements whose representations $[a]$ satisfy $\gcd(a,n) \neq 1$. Thus

$$\mathbb{Z}_{10}^* = \{[1], [3], [7], [9]\}.$$

Theorem 6.39 tells us that $\mathbb{Z}_{10}^*$ is a group. Since it has four elements, it must be isomorphic to either the Klein 4-group, or to $\mathbb{Z}_4$. Which is it? In this case, it's probably easiest to look at the multiplication table (we omit the brackets since it's obvious the elements are in $\mathbb{Z}_{10}^*$):

$\times$	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Notice that $3^{-1} \neq 3$. In the Klein 4-group, every element is its own inverse, so $\mathbb{Z}_{10}^*$ cannot be isomorphic to the Klein 4-group. Instead, it must be isomorphic to $\mathbb{Z}_4$.

Exercises.

Exercise 6.41: List the elements of $\mathbb{Z}_7^*$ using their canonical representations, and construct its multiplication table. Use the table to identify the inverse of each element.

Exercise 6.42: List the elements of $\mathbb{Z}_{15}^*$ using their canonical representations, and construct its multiplication table. Use the table to identify the inverse of each element.

Exercise 6.43: Show that any prime integer p is irreducible.

6.4: Euler's Theorem

In Section 6.3 we defined the group $\mathbb{Z}_n^*$ for all $n \in \mathbb{N}^+$ where $n > 1$. This group satisfies an important property called *Euler's Theorem*, a result about Euler's φ-function.

Definition 6.44: Euler's φ-function is $\varphi(n) = \left|\mathbb{Z}_n^*\right|$.

In other words, Euler's φ-function counts the number of positive integers smaller than n that share no common factors with it.

Theorem 6.45 (Euler's Theorem): *For all* $x \in \mathbb{Z}_n^*$, $x^{\varphi(n)} = 1$.

Proofs of Euler's Theorem based only on Number Theory are not very easy. They aren't particularly difficult, either: they just aren't easy. See for example the proof on pages 18–19 of [Lau03].

On the other hand, a proof of Euler's Theorem using algebra is trivial.

PROOF: Let $x \in \mathbb{Z}_n^*$. By Corollary 3.46 to Lagrange's Theorem, $\operatorname{ord}(x) \mid \left|\mathbb{Z}_n^*\right|$. By definition, $\varphi(n) = \left|\mathbb{Z}_n^*\right|$, so by substitution, $\operatorname{ord}(x) \mid \varphi(n)$; use the definition of divisibility to write $\varphi(n) = d \cdot \operatorname{ord}(x)$ for some $d \in \mathbb{Z}$. Hence

$$x^{\varphi(n)} = x^{d \cdot \operatorname{ord}(x)} = \left(x^{\operatorname{ord}(x)}\right)^d = [1]^d = [1].$$

□

Corollary 6.46: *For all* $x \in \mathbb{Z}_n^*$, $x^{-1} = x^{\varphi(n)-1}$.

PROOF: You do it! See Exercise 6.55. □

Corollary 6.46 says that we can compute x^{-1} for any $x \in \left|\mathbb{Z}_n^*\right|$ "relatively easily;" all we need to know is $\varphi(n)$. The natural followup question is, what is $\varphi(n)$? For irreducible integers, this is easy: if p is irreducible, $\varphi(p) = p - 1$. For reducible integers, it is not so easy. Checking a few examples, no clear pattern emerges:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\left\|\mathbb{Z}_n^*\right\|$	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Computing $\varphi(n)$ turns out to be quite hard for arbitrary $n \in \mathbb{N}^+$. This difficulty is what makes the RSA algorithm secure (see Section 6.5).

One way to do it would be to factor n and compute all the positive integers that do not share any common factors. For example,

$$28 = 2^2 \cdot 7,$$

so to compute $\varphi(28)$, we could look at all the positive integers smaller than 28 that do not have 2 or 7 as factors. However, this requires us to know first that 2 and 7 are factors of 28, and no one knows a very *efficient* way to do this.

Another way would be to compute $\varphi(m)$ for each factor m of n, then recombine them. But how?

Lemma 6.47: *Let* $n \in \mathbb{N}^+$. *If* $n = pq$ *and* $\gcd(p,q) = 1$, *then* $\varphi(n) = \varphi(p)\varphi(q)$.

Example 6.48: In the table above, we have $\varphi(15) = 8$. Notice that this satisfies

$$\varphi(15) = \varphi(5 \times 3) = \varphi(5)\,\varphi(3) = 4 \times 2 = 8.$$

PROOF: Recall from Exercise 2.24 on page 31 that $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ is a group; the size of this group is $\left|\mathbb{Z}_p^*\right| \times \left|\mathbb{Z}_q^*\right| = \varphi(p)\,\varphi(q)$. We show that $\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

Let $f : \mathbb{Z}_n^* \to \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ by $f\left([a]_n\right) = \left([a]_p, [a]_q\right)$. First we show that f is a homomorphism: Let $a, b \in \mathbb{Z}_n^*$; then

$$\begin{aligned} f\left([a]_n [b]_n\right) = f\left([ab]_n\right) &= \left([ab]_p, [ab]_q\right) \\ &= \left([a]_p [b]_p, [a]_q [b]_q\right) \\ &= \left([a]_p, [a]_q\right)\left([b]_p, [b]_q\right) \\ &= f\left([a]_n\right) f\left([b]_n\right) \end{aligned}$$

(where Lemma 6.33 on page 144 and the definition of the operation in $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ justify the second two equations).

It remains to show that f is one-to-one and onto. Rather amazingly, we can get the Chinese Remainder Theorem to do most of the work for us. To show that f is onto, let $\left([a]_p, [b]_q\right) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. We need to find $x \in \mathbb{Z}_n^*$ such that $f\left([x]_n\right) = \left([a]_p, [b]_q\right)$. Consider the system of linear congruences

$$\begin{aligned} [x] &= [a] \text{ in } \mathbb{Z}_p; \\ [x] &= [b] \text{ in } \mathbb{Z}_q. \end{aligned}$$

The Chinese Remainder Theorem tells us not only that such x exists in $\mathbb{Z}_n$, but that x is unique in $\mathbb{Z}_n$.

We are not quite done; we have shown that a solution x exists in $\mathbb{Z}_n$, but what we really need is that $x \in \mathbb{Z}_n^*$. To see that indeed $x \in \mathbb{Z}_n^*$, let d be any common divisor of x and n. By way of contradiction, assume $d \neq \pm 1$; by Theorem 6.28, we can find an irreducible divisor r of d; by Exercise 1.32 on page 11, $r \mid n$ and $r \mid x$. Recall that $n = pq$, so $r \mid pq$, so $r \mid p$ or $r \mid q$. Without loss of generality, we may assume that $r \mid p$. Since $[x]_p = [a]_p$, Lemma 3.85 on page 75 tells us that $p \mid (x - a)$. Let $y \in \mathbb{Z}$ such that $py = x - a$. Rewrite this equation as $x - py = a$. Recall that $r \mid x$ and $r \mid p$; we can factor r from the left-hand side of the equation, rewriting it as $rz = a$ for some $z \in \mathbb{Z}$. Thus $r \mid a$, but this and $r \mid a$ contradict the hypothesis that $a \in \mathbb{Z}_p^*$! Our assumption that $d \neq 1$ must have been false; we conclude that the only common divisor of x and n is in fact ± 1. Hence $x \in \mathbb{Z}_n^*$. □

Corollary 6.46 gives us an "easy" way to compute the inverse of any $x \in \mathbb{Z}_n^*$. However, it can take a long time to compute $x^{\varphi(n)}$, so we conclude with a brief discussion of how to compute canonical forms of exponents in this group. We will take two steps towards a fast exponentiation in $\mathbb{Z}_n^*$.

Lemma 6.49: *For any $n \in \mathbb{N}^+$, $[x^a] = [x]^a$ in $\mathbb{Z}_n^*$.*

PROOF: You do it! See Exercise 6.57 on the following page. □

Example 6.50: In $\mathbb{Z}_{15}^*$ we can easily determine that $\left[4^{20}\right] = [4]^{20} = \left([4]^2\right)^{10} = [16]^{10} = [1]^{10} = [1]$. Notice that this is a *lot* faster than computing $4^{20} = 1099511627776$ and dividing to find the canonical form.

Theorem 6.51 (Fast Exponentiation): *Let $a \in \mathbb{N}$ and $x \in \mathbb{Z}$. We can compute x^a in the following way:*

1. *Let b be the largest integer such that $2^b \leq a$.*
2. *Use the Division Theorem to divide a repeatedly by 2^b, 2^{b-1}, …, 2^1, 2^0 in that order; let the quotients of each division be q_b, q_{b-1}, …, q_1, q_0.*
3. *Write $a = q_b 2^b + q_{b-1} 2^{b-1} + \cdots + q_1 2^1 + q_0 2^0$.*
4. *Let $y = 1$, $z = x$ and $i = 0$.*
5. *Repeat the following until $i > b$:*
   (a) *If $q_i \neq 0$ then replace y with the product of y and z.*
   (b) *Replace z with z^2.*
   (c) *Replace i with $i + 1$.*

This ends with $x^a = y$.

Theorem 6.51 effectively computes the *binary representation* of a and uses this to square x repeatedly, multiplying the result only by those powers that matter for the representation. Its algorithm is especially effective on computers, whose mathematics is based on binary arithmetic. Combining it with Lemma 6.49 gives an added bonus.

Example 6.52: Since $10 = 2^3 + 2^1$, we can compute $4^{10} = 4^{2^3+2^1}$ following the algorithm of Theorem 6.51:

1. We have $q_3 = 1$, $q_2 = 0$, $q_1 = 1$, $q_0 = 0$.
2. Let $y = 1$, $z = 4$ and $i = 0$.
3. When $i = 0$:
   (a) We do not change y because $q_0 = 0$.
   (b) Put $z = 4^2 = 16$.
   (c) Put $i = 1$.
4. When $i = 1$:
   (a) Put $y = 1 \cdot 16 = 16$.
   (b) Put $z = 16^2 = 256$.
   (c) Put $i = 2$.
5. When $i = 2$:
   (a) We do not change y because $q_2 = 0$.
   (b) Put $z = 256^2 = 65,536$.
   (c) Put $i = 3$.

6. When $i = 3$:
   (a) Put $y = 16 \cdot 65,536 = 1,048,576$.
   (b) Put $z = 65,536^2 = 4,294,967,296$.
   (c) Put $i = 4$.

We conclude that $4^{10} = 1,048,576$. Hand computation the long way, or a half-decent calculator, will verify this.

PROOF OF FAST EXPONENTIATION:

Termination: Termination follows from the fact that b is a finite number, and the algorithm assigns to i the values $0, 1, \ldots, b+1$ in succession.

Correctness: Since b is the largest integer such that $2^b \leq a$, $q_b \in \{0,1\}$; otherwise, $2^{b+1} = 2 \cdot 2^b \leq a$, contradicting the choice of b. For $i = b-1, \ldots, 1, 0$, we have the remainder from division by 2^{i+1} smaller than 2^i, and we immediately divide by $2^b = 2^{i-1}$, so that $q_i \in \{0,1\}$ as well. Hence $q_i \in \{0,1\}$ for $i = 0, 1, \ldots, b$ and if $q_i \neq 0$ then $q_i = 1$. The algorithm therefore multiplies $z = x^{2^i}$ to y only if $q_i \neq 0$, which agrees with the binary representation

$$x^a = x^{q_b 2^b + q_{b-1} 2^{b-1} + \cdots + q_1 2^1 + q_0 2^0}.$$

□

Exercises.

Exercise 6.53: Compute 3^{28} in $\mathbb{Z}$ using fast exponentiation. Show each step.
Exercise 6.54: Compute 24^{28} in $\mathbb{Z}_7^*$ using fast exponentiation. Show each step.
Exercise 6.55: Prove that for all $x \in \mathbb{Z}_n^*$, $x^{\varphi(n)-1} = x^{-1}$.
Exercise 6.56: Prove that for all $x \in \mathbb{N}^+$, if x and n have no common divisors, then $n \mid \left(x^{\varphi(n)} - 1\right)$.
Exercise 6.57: Prove that for any $n \in \mathbb{N}^+$, $[x^a] = [x]^a$ in $\mathbb{Z}_n^*$.

6.5: RSA Encryption

From the viewpoint of practical applications, some of the most important results of group theory and number theory are those that enable security in internet commerce. We described this problem on page 1: when you buy something online, you usually submit some private information, at least a credit card or bank account number, and usually more. There is no guarantee that, as this information passes through the internet, it will pass only through servers run by disinterested persons. It is quite possible for the information to pass through a computer run by at least one ill-intentioned hacker, and possibly even organized crime. You probably don't want criminals looking at your credit card number.

Given the inherent insecurity of the internet, the solution is to disguise private information so that disreputable snoopers cannot understand it. A common method in use today is the RSA encryption algorithm.[25] First we describe the algorithms for encryption and decryption;

[25] RSA stands for Rivest (of MIT), Shamir (of the Weizmann Institute in Israel), and Adleman (of USC).

afterwards we explain the ideas behind each stage, illustrating with an example; finally we prove that it succesfully encrypts and decrypts messages.

Theorem 6.58 (RSA algorithm): *Let M be a list of positive integers obtained by converting the letters of a message. Let p, q be two irreducible integers such that:*

- $\gcd(p,q) = 1$*; and*
- $(p-1)(q-1) > \max\{m : m \in M\}$.

Let $N = pq$, and let $e \in \mathbb{Z}^*_{\varphi(N)}$, where φ is the Euler phi-function. If we apply the following algorithm to M:

1. *Let $e \in \mathbb{Z}^*_{\varphi(N)}$.*
2. *Let C be a list of positive integers found by computing the canonical representation of $[m^e]_N$ for each $m \in M$.*

and subsequently apply the following algorithm to C:

1. *Let $d = e^{-1} \in \mathbb{Z}^*_{\varphi(N)}$.*
2. *Let D be a list of positive integers found by computing the canonical representation of $\left[c^d\right]_N$ for each $c \in C$.*

then $D = M$.

Example 6.59: Consider the text message

ALGEBRA RULZ.

We convert the letters to integers in the fashion that you might expect: A=1, B=2, ..., Z=26. We also assign 0 to the space. This allows us to encode the message as,

$$M = (1,12,7,5,2,18,1,0,18,21,12,26).$$

Let $p = 5$ and $q = 11$; then $N = 55$. Let $e = 3$; note that

$$\gcd(3,\varphi(N)) = \gcd(3,\varphi(5)\cdot\varphi(11)) = \gcd(3,4\times 10) = \gcd(3,40) = 1.$$

Encrypt by computing m^e for each $m \in M$:

$$\begin{aligned} C &= \left(1^3,12^3,7^3,5^3,2^3,18^3,1^3,0^3,18^3,21^3,12^3,26^3\right) \\ &= (1,23,13,15,8,2,1,0,2,21,23,31). \end{aligned}$$

A snooper who intercepts C and tries to read it as a plain message would have several problems trying to read it. First, it contains 31, a number that does not fall in the range 0 and 26. If he gave that number the symbol _, he would see

AWMOHBA BUW_

which is not an obvious encryption of ALGEBRA RULZ.

The inverse of $3 \in \mathbb{Z}^*_{40}$ is $d = 27$ (we could compute this using Corollary 6.46, but it's

not hard to see that $3 \times 27 = 81$ and $[81] = [1]$ in $\mathbb{Z}_{40}^*$). Decrypt by computing c^d for each $c \in C$:

$$\begin{aligned} D &= \left(1^{27}, 23^{27}, 13^{27}, 15^{27}, 8^{27}, 2^{27}, 1^{27}, 0^{27}, 2^{27}, 21^{27}, 23^{27}, 31^{27}\right) \\ &= (1, 12, 7, 5, 2, 18, 1, 0, 18, 21, 12, 26)\,. \end{aligned}$$

Trying to read this as a plain message, we have

ALGEBRA RULZ.

Doesn't it?

A few observations are in order.

1. Encrypting messages letter-by-letter is spectacularly weak; in a stronger approach, letters should be grouped together and converted to integers. For example, the first four letters of the secret message above are

   ALGE

   and we can convert this to a number using any of several methods; for example

   $$\text{ALGE} \quad \to \quad 1 \times 26^3 + 12 \times 26^2 + 7 \times 26 + 5 = 25{,}785.$$

   In order to encrypt this, we would need larger values for p and q. This becomes too burdensome to carry out by hand, so you want a computer to help. We give an example in the homework.
2. RSA is an example of a *public-key cryptosystem.* In effect, that means that person A broadcasts to the world, "Anyone who wants to send me a secret message can use the RSA algorithm with values $N = \ldots$ and $e = \ldots$." So a snooper knows the method, the modulus, N, and the encryption key, e!
3. If the snooper knows the method, N, and e, what makes RSA safe? To decrypt, the snooper needs to compute $d = e^{-1} \in \mathbb{Z}_{\varphi(N)}^*$. This would be relatively easy if he knew $\varphi(N)$; using Corollary 6.46, it's a matter of computing $e^{\varphi(N)-1}$. You might think that, since the snooper knows the method, and therefore he knows that $N = pq$, it would be a simple matter of factoring N and applying Lemma 6.47 to compute $\varphi(N) = (p-1)(q-1)$. In practice, however, p and q are *very* large numbers (many digits long), and there is *no known method* of computing $\varphi(N)$ "quickly" if N is sufficiently large. There is a careful science to choosing p and q in such a way that makes it hard to determine their values from N and e.
4. It is time-consuming to perform these computations by hand; a computer algebra system will do the trick nicely. At the end of this section, after the exercises, we list programs that will help you perform these computations in the Sage and Maple computer algebra systems. The programs are:
   - `scramble`, which accepts as input a plaintext message like "ALGEBRA RULZ" and turns it into a list of integers;
   - `descramble`, which accepts as input a list of integers and turns it into plaintext;
   - `en_de_crypt`, which encrypts or decrypts a message, depending on whether you

feed it the encryption or decryption exponent.

Examples of usage:

- in Sage:
  - to determine the list of integers M, type `M = scramble("ALGEBRA RULZ")`
  - to encrypt M, type `C = en_de_crypt(M,3,55)`
  - to decrypt C, type `en_de_crypt(C,27,55)`
- in Maple:
  - to determine the list of integers M, type `M := scramble("ALGEBRA RULZ");`
  - to encrypt M, type `C := en_de_crypt(M,3,55);`
  - to decrypt C, type `en_de_crypt(C,27,55);`

Now, *why* does the RSA algorithm work?

PROOF OF THE RSA ALGORITHM: Let $i \in \{1,2,\ldots,|C|\}$. Let $c \in C$. By definition of C, $c = m^e \in \mathbb{Z}_N^*$ for some $m \in M$. We need to show that $c^d = (m^e)^d = m$.

Since $[e] \in \mathbb{Z}_{\varphi(N)}^*$, we know that it has an inverse element, $[d]$. That is, $[de] = [d][e] = [1]$. By Lemma 3.85, $\varphi(N) \mid (1-de)$, so we can find $b \in \mathbb{Z}$ such that $b \cdot \varphi(N) = 1-de$, or $de = 1 - b\varphi(N)$.

We claim that $[m]^{de} = [m] \in \mathbb{Z}_N$. To do this, we will show two subclaims about the behavior of the exponentiation in $\mathbb{Z}_p$ and $\mathbb{Z}_q$.

Claim 1: $[m]^{de} = [m] \in \mathbb{Z}_p$.

If $p \mid m$, then $[m] = [0] \in \mathbb{Z}_p$. Without loss of generality, $d, e \in \mathbb{N}^+$, so

$$[m]^{de} = [0]^{de} = [0] = [m] \in \mathbb{Z}_p.$$

Otherwise, $p \nmid m$. Recall that p is irreducible, so $\gcd(m,p) = 1$. By Euler's Theorem,

$$[m]^{\varphi(p)} = [1] \in \mathbb{Z}_p^*.$$

Recall that $\varphi(N) = \varphi(p)\varphi(q)$; thus,

$$[m]^{\varphi(N)} = [m]^{\varphi(p)\varphi(q)} = \left([m]^{\varphi(p)}\right)^{\varphi(q)} = [1].$$

Thus, in $\mathbb{Z}_p^*$,

$$[m]^{de} = [m]^{1-b\varphi(N)} = [m] \cdot [m]^{-b\varphi(N)} = [m]\left([m]^{\varphi(N)}\right)^{-b} = [m] \cdot [1]^{-b} = [m].$$

What is true for $\mathbb{Z}_p^*$ is also true in $\mathbb{Z}_p$, since the former is a subset of the latter. Hence,

$$[m]^{de} = [m] \in \mathbb{Z}_p.$$

Claim 2: $[m]^{1-b\varphi(N)} = [m] \in \mathbb{Z}_q$.

The argument is similar to that of the first claim.

Since $[m]^{de} = [m]$ in both $\mathbb{Z}_p$ and $\mathbb{Z}_q$, properties of the quotient groups $\mathbb{Z}_p$ and $\mathbb{Z}_q$ tell us that $\left[m^{de} - m\right] = [0]$ in both $\mathbb{Z}_p$ and $\mathbb{Z}_q$ as well. In other words, both p and q divide $m^{de} - m$. You will show in Exercise 156 that this implies that N divides $m^{de} - m$.

From the fact that N divides $m^{de} - m$, we have $[m]_N^{ed} = [m]_N$. Thus, computing $(m^e)^d$ in $\mathbb{Z}_{\varphi(N)}$ gives us m. □

Exercises.

Exercise 6.60: The phrase

$$[574, 1, 144, 1060, 1490, 0, 32, 1001, 574, 243, 533]$$

is the encryption of a message using the RSA algorithm with the numbers $N = 1535$ and $e = 5$. You will decrypt this message.

(a) Factor N.
(b) Compute $\varphi(N)$.
(c) Find the appropriate decryption exponent.
(d) Decrypt the message.

Exercise 6.61: In this exercise, we encrypt a phrase using more than one letter in a number.

(a) Rewrite the phrase GOLDEN EAGLES as a list M of three positive integers, each of which combines four consecutive letters of the phrase.
(b) Find two prime numbers whose product is larger than the largest number you would get from four letters.
(c) Use those two prime numbers to compute an appropriate N and e to encrypt M using RSA.
(d) Find an appropriate d that will decrypt M using RSA.
(e) Decrypt the message to verify that you did this correctly.

Exercise 6.62: Let $m, p, q \in \mathbb{Z}$ and suppose that $\gcd(p, q) = 1$.

(a) Show that if $p \mid m$ and $q \mid m$, then $pq \mid m$.
(b) Explain why this completes the proof of the RSA algorithm; that is, since p and q both divide $m^{de} - m$, then so does N.

Sage programs

The following programs can be used in Sage to help make the amount of computation involved in the exercises less burdensome:

```
def scramble(s):
  result = []
  for each in s:
    if ord(each) >= ord("A") and ord(each) <= ord("Z"):
      result.append(ord(each)-ord("A")+1)
    else:
      result.append(0)
  return result


def descramble(M):
  result = ""
  for each in M:
    if each == 0:
      result = result + " "
    else:
      result = result + chr(each+ord("A") - 1)
  return result


def en_de_crypt(M,p,N):
  result = []
  for each in M:
    result.append((each^p).mod(N))
  return result
```

Maple programs

The following programs can be used in Maple to help make the amount of computation involved in the exercises less burdensome:

```
scramble := proc(s)
  local result, each, ord;
  ord := StringTools[Ord];
  result := [];
  for each in s do
    if ord(each) >= ord("A") and ord(each) <= ord("Z") then
      result := [op(result),
        ord(each) - ord("A") + 1];
    else
      result := [op(result), 0];
    end if;
  end do;
  return result;
end proc:


descramble := proc(M)
  local result, each, char, ord;
  char := StringTools[Char];
  ord := StringTools[Ord];
  result := "";
  for each in M do
    if each = 0 then
      result := cat(result, " ");
    else
      result := cat(result, char(each + ord("A") - 1));
    end if;
  end do;
  return result;
end proc:


en_de_crypt := proc(M,p,N)
  local result, each;
  result := [];
  for each in M do
    result := [op(result), (each^p) mod N];
  end do;
```

```
  return result;
end proc:
```

Part III
Rings

Chapter 7:
Rings

Groups and monoids are simple in the following respect: a group or monoid is defined by *one* operation. When we studied the set of matrices $\mathbb{R}^{m\times n}$ as a group, for example, we considered only the operation of addition. Likewise, when we studied $\mathbb{Z}$ as a group, we considered only the operation of addition. With other groups, we studied other operations, but we only studied one operation at a time.

In some cases, however, we want to analyze how both addition and multiplication interact in a given set. This motivates the study of a structure that incorporates common properties of both operations.

Section 7.1 of this chapter introduces us to this structure, called a *ring*. The rest of the chapter examines special kinds of rings. In Section 7.2 we introduce special kinds of rings that model useful properties of $\mathbb{Z}$ and $\mathbb{Q}$. In Section 7.3 we introduce rings of polynomials. The Euclidean algorithm, which proved so important in chapter 6, serves as the model for a special kind of ring described in Section 7.4.

7.1: A structure for addition and multiplication

What sort of properties do we associate with both addition and multiplication?

Definition 7.1: Let R be a set *with at least two elements*, and $+$ and $\times$ two binary operations on that set. We say that $(R,+,\times)$ is a **ring** if it satisfies the following properties:

(R1) $(R,+)$ is an abelian group.

(R2) R is closed under multiplication: that is,
for all $a,b\in R$, $ab\in R$.

(R3) R is associative under multiplication: that is,
for all $a,b,c\in R$, $(ab)c=a(bc)$.

(R4) R satisfies the distributive property of addition over multiplication: that is,
for all $a,b,c\in R$, $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$.

Notation 7.2: As with groups, we usually refer simply to R as a group, rather than $(R,+,\times)$.

Since $(R,+)$ is an abelian group, the ring has an additive identity, 0. We sometimes write 0_R to emphasize that it is the additive identity of R. Likewise, if there is a multiplicative identity, we write 1 or 1_R, and not e.

Notice the following:

- While addition is commutative on account of (R1), we do *not* know whether multiplication is commutative.

- If R is a ring and $a, b \in R$ then if there exists $r \in R$ such that $ar = b$ or $ra = b$, we say that a **divides** b, and that b is **divisible** by a.
- There is no requirement that a multiplicative identity exists.
- There is no requirement that multiplicative inverses exist.
- There is no guarantee (yet) that the additive identity satisfies any properties that you remember from past experience: in particular, there is *no guarantee* that
  - the zero-product rule holds; or even that
  - $0_R \cdot a = 0_R$ for any $a \in R$.

Example 7.3: Let $R = \mathbb{R}^{m \times m}$ for some positive integer m. It turns out that R is a ring under the usual addition and multiplication of matrices. The details are tedious, and can be found in any linear algebra book.

However, we do want to point out something that should make you at least a *little* uncomfortable. Let

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Routine computation shows that

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

even though $A, B \neq 0$. Hence

We can never assume in any ring R the **zero product property** that

$$\forall a, b \in R \qquad ab = 0 \implies a = 0 \text{ or } b = 0.$$

Likewise, the following sets with which you are long familiar are also rings:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under their usual addition and multiplication;
- the sets of univariate polynomials $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ under their usual addition and multiplication;
- the sets of multivariate polynomials $\mathbb{Z}[x_1, \ldots, x_n]$, etc. under their usual addition and multiplication.

You will study other example rings in the exercises. For now, we prove a familiar property of the additive identity.

Proposition 7.4: *For all $r \in R$, $r \cdot 0_R = 0_R \cdot r = 0_R$.*

PROOF: Let $r \in R$. Since $(R, +)$ is an abelian group, we know that $0_R + 0_R = 0_R$. By substitution, $r(0_R + 0_R) = r \cdot 0_R$. By distribution, $r \cdot 0_R + r \cdot 0_R = r \cdot 0_R$. Since $(R, +)$ is an abelian group, $r \cdot 0_R$ has an additive inverse; call it s. Applying the properties of a ring, we have

$$\begin{aligned} s + (r \cdot 0_R + r \cdot 0_R) &= s + r \cdot 0_R \\ (s + r \cdot 0_R) + r \cdot 0_R &= s + r \cdot 0_R \\ 0_R + r \cdot 0_R &= 0_R \\ r \cdot 0_R &= 0_R. \end{aligned}$$

A similar argument shows that $0_R \cdot r = 0_R$. □

We now turn our attention to two properties that, while pleasant, are not necessary for a ring.

Definition 7.5: Let R be a ring. If R has a multiplicative identity 1_R such that

$$r \cdot 1_R = 1_R \cdot r = r \quad \forall r \in R,$$

we say that R is a **ring with unity**. (Another name for the multiplicative identity is **unity**.)
If R is a ring and the multiplicative operation is commutative, so that

$$rs = sr \quad \forall r \in R,$$

then we say that R is a **commutative ring**.

Example 7.6: The set of matrices $\mathbb{R}^{m\times m}$ is a ring with unity, where I_m is the multiplicative identity. However, it is not a commutative ring.

You will show in Exercise 7.9 that $2\mathbb{Z}$ is a ring. It is a commutative ring, but not a ring with unity.

For a commutative ring with unity, consider $\mathbb{Z}$.

Remark 7.7: Although non-commutative rings are interesting, we will ignore them for the rest of these notes. Henceforth,

all rings we consider are commutative,

unless otherwise noted.

As with groups, we can characterize all rings with only two elements.

Example 7.8: Let R be a ring with only two elements. There are two possible structures for R.

Why? Since $(R,+)$ is an abelian group, by Example 2.8 on page 27 the addition table of R has the form

$+$	0_R	a
0_R	0_R	a
a	a	0_R

.

By Proposition 7.4, we know that the multiplication table *must* have the form

$\times$	0_R	a
0_R	0_R	0_R
a	0_R	?

where $a \cdot a$ is undetermined. Nothing in the properties of a ring tell us whether $a \cdot a = 0_R$ or $a \cdot a = a$; in fact, rings exist with both properties:

- if $R = \mathbb{Z}_2$ (see Exercise 7.10 to see that this is a ring), then $a = [1]$ and $a \cdot a = a$; but
- if

$$R = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\} \subsetneq (\mathbb{Z}_2)^{2\times 2},$$

then $a \cdot a = 0 \neq a$.

Exercises

Exercise 7.9:
(a) Show that $2\mathbb{Z}$ is a ring under the usual addition and multiplication of integers.
(b) Show that for any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a ring under the usual addition and multiplication of integers.

Exercise 7.10: Define a multiplication in $\mathbb{Z}_n$ in the following way: for $[a], [b] \in \mathbb{Z}_n$, $[a][b] = [ab]$.
(a) Show that this notion of multiplication is well-defined; that is, if $a \neq x$, $b \neq y$, while $[a] = [x]$ and $[b] = [y]$, $[a][b] = [x][y]$.
(b) Show that $\mathbb{Z}_2$ is a ring under the addition and multiplication of cosets define in Section 3.5.
(c) Show that for any $n \in \mathbb{Z}$ where $n > 1$, $\mathbb{Z}_n$ is a ring under the addition and multiplication of cosets defined in Section 3.5.

Exercise 7.11: Let R be a ring.
(a) Show that for all $r, s \in R$, $(-r)s = r(-s) = -(rs)$.
(b) Suppose that R has unity. Show that $-r = -1_R \cdot r$ for all $r \in R$.

Exercise 7.12: Let R be a ring with unity. Show that $1_R = 0_R$ if and only if R has only one element.

Exercise 7.13: Consider the two possible ring structures from Example 7.8. Show that if a ring R has only two elements, one of which is unity, then it can have only one of the structures.

Exercise 7.14: Let $R = \{T, F\}$ with the additive operation $\oplus$ (Boolean xor) where

$$\begin{aligned} F \oplus F &= F \\ F \oplus T &= T \\ T \oplus F &= T \\ T \oplus T &= F \end{aligned}$$

and a multiplicative operation $\wedge$ (Boolean and) where

$$\begin{aligned} F \wedge F &= F \\ F \wedge T &= F \\ T \wedge F &= F \\ T \wedge T &= T. \end{aligned}$$

(see also Exercises 2.18 and 2.19 on page 30). Is $(R, \oplus, \wedge)$ a ring? If it is a ring, then
(a) what is the zero element?
(b) does it have a unity element? if so, what is it?
(c) is it commutative?

7.2: Integral Domains and Fields

Example 7.3 illustrates an important point: not all rings satisfy properties that we might like to take for granted. Not only does the ring of matrices illustrate that the zero product property is not satisfied for all rings, it also demonstrates that multiplicative inverses do not necessarily exist in all rings. Both the zero product property and multiplicative inverses are very useful—think of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$—so we should give them special attention.

In this section, we always assume that R is a commutative ring with unity.

Definition 7.15: If the elements of R satisfy the zero product property, then we call R an **integral domain**. Otherwise, we call any two non-zero elements $a, b \in R$ such that $ab = 0$ **zero divisors**.

Example 7.16: Naturally, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are integral domains.

In Exercise 7.10, you showed that $\mathbb{Z}_n$ was a ring under ordinary addition and multiplication. However, it need not be an integral domain. For example, in $\mathbb{Z}_6$ we have $[2]\cdot[3] = [6] = [0]$, making $[2]$ and $[3]$ zero divisors. On the other hand, it isn't hard to see that $\mathbb{Z}_2$, $\mathbb{Z}_3$, and $\mathbb{Z}_5$ are integral domains, if only via an exhaustive check. What about $\mathbb{Z}_4$?

Definition 7.17: If R has unity and every non-zero element of R has a multiplicative inverse, then we call R a **field**.

Example 7.18: The rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

On the other hand, define **the set of fractions over** a ring R

$$\text{Frac}(R) := \left\{ \frac{p}{q} : \ p, q \in R \text{ and } q \neq 0 \right\},$$

with addition and multiplication defined in the usual way for "fractions", and equality defined by

$$\frac{a}{b} = \frac{p}{q} \quad \Longleftrightarrow \quad aq = bp.$$

This should remind you of $\mathbb{Q}$, and for good reason. You might think as a result that $\text{Frac}(R)$ is a field, just as $\mathbb{Q}$ is, but it turns out that this is not always true: $\text{Frac}(R)$ is not a field *unless R is an integral domain.* Indeed, addition and subtraction *might not even be defined* in $\text{Frac}(R)$ unless R is an integral domain; that is, for all $a, b, c \in R$

$$\frac{ac}{bc} = \frac{ca}{cb} = \frac{a}{b}.$$

See Exercises 7.24 and 7.25.

Let's show that, if R is an integral domain, then $\text{Frac}(R)$ is a ring. Assume that R is an integral domain. First we show that $\text{Frac}(R)$ is an additive group. Let $f, g, h \in R$; choose $a, b, p, q, r, s \in \text{Frac}(R)$ such that $f = a/b$, $g = p/q$, and $h = r/s$. First we show that $\text{Frac}(R)$ is an abelian group.

closure: This is fairly routine, using common denominators and the fact that R is a domain:

$$\begin{aligned} f+g &= \frac{a}{b}+\frac{p}{q} \\ &= \frac{aq}{bq}+\frac{bp}{bq} \\ &= \frac{aq+bp}{bq} \\ &\in \mathrm{Frac}(R). \end{aligned}$$

Why did we need R do be an integral domain? If not, then it is possible that $bq = 0$, and if so, $f+g \notin \mathrm{Frac}(R)$!

associative: This is the hardest one:

$$\begin{aligned} (f+g)+h &= \frac{aq+bp}{bq}+\frac{r}{s} \\ &= \frac{(aq+bp)s}{(bq)s}+\frac{(bq)r}{(bq)s} \\ &= \frac{((aq)s+(bp)s)+(bq)r}{(bq)s} \\ &= \frac{a(qs)+(b(ps)+b(qr))}{b(qs)} \\ &= \frac{a(qs)}{b(qs)}+\frac{b(ps)+b(qr)}{b(qs)} \\ &= \frac{a}{b}+\frac{ps+qr}{qs} \\ &= \frac{a}{b}+\left(\frac{p}{q}+\frac{r}{s}\right) \\ &= f+(g+h.) \end{aligned}$$

identity: The ring identity of $\mathrm{Frac}(R)$ is $0_R/1_R$. This is easy to see, since

$$f+\frac{0_R}{1_R} = \frac{a}{b}+\frac{0_R\cdot b}{1_R\cdot b} = \frac{a}{b}+\frac{0_R}{b} = \frac{a}{b} = f.$$

additive inverse: For each $f = p/q$, $(-p)/q$ is the additive inverse.

commutative: We have

$$\begin{aligned} f+g &= \frac{a}{b}+\frac{c}{d} \\ &= \frac{ad}{bd}+\frac{bc}{bd} \\ &= \frac{ad+bc}{bd} \\ &= \frac{cb+da}{db} \\ &= \frac{cb}{db}+\frac{da}{db} \\ &= \frac{c}{d}+\frac{a}{b} \\ &= g+f. \end{aligned}$$

Next we have to show that $\mathrm{Frac}(R)$ satisfies the requirements of a ring.

closure: Using closure in R and the fact that R is an integral domain, this is straightforward: $fg = (ap)/(bq) \in \mathrm{Frac}(R)$.

associative: Using the associative property of R, this is straightforward:

$$(fg)h = \left(\frac{ap}{bq}\right)\frac{r}{s} = \frac{(ap)r}{(bq)s} = \frac{a(pr)}{b(qs)} = \frac{a}{b}\frac{(pr)}{qs} = f(gh).$$

distributive: We rely on the distributive property of R:

$$f(g+h) = \frac{a}{b}\left(\frac{p}{q}+\frac{r}{s}\right) = \frac{a}{b}\left(\frac{ps+qr}{qs}\right) = \frac{a(ps+qr)}{b(qs)}$$

$$= \frac{a(ps)+a(qr)}{b(qs)} = \frac{a(ps)}{b(qs)}+\frac{a(qr)}{b(qs)} = \frac{ap}{bq}+\frac{ar}{bs}$$

$$= fg+fh.$$

Finally, we show that $\mathrm{Frac}(R)$ is a field. We have to show that it is commutative, that it has a multiplicative identity, and that every non-zero element has a multiplicative inverse.

commutative: We claim that the multiplication of $\mathrm{Frac}(R)$ is commutative. This follows from the fact that R, as an integral domain, has a commutative multiplication, so

$$fg = \frac{a}{b}\cdot\frac{p}{q} = \frac{ap}{bq} = \frac{pa}{qb} = \frac{p}{q}\cdot\frac{a}{b} = gf.$$

multiplicative identity: We claim that $\frac{1_R}{1_R}$ is a multiplicative identity for $\mathrm{Frac}(R)$. Then

$$f \cdot \frac{1_R}{1_R} = \frac{a}{b} \cdot \frac{1_R}{1_R} = \frac{a \cdot 1_R}{b \cdot 1_R} = \frac{a}{b} = f.$$

multiplicative inverse: Let $f \in \mathrm{Frac}(R)$ be a non-zero element. You will show in Exercise 7.24 that any $0_R/a \in \mathrm{Frac}(R)$ is equivalent to the additive identity $0_R/1_R = 0_{\mathrm{Frac}(R)}$, so we may write f as a/b with $a, b \in R$, $b \neq 0$, and even $a \neq 0$. Let $g = b/a$; then

$$fg = \frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab}.$$

In Exercise 7.24, you will show that

$$\frac{ab}{ab} = 1_{\mathrm{Frac}(R)}.$$

Definition 7.19: For any integral domain R, we call $\mathrm{Frac}(R)$ the **ring of fractions of** R.

Already in Example 7.18 we see that there is a relationship between integral domains and fields: we needed R to be an integral domain in order to get a field out of the ring of rational expressions. It turns out that the relationship is even closer.

Theorem 7.20: *Every field is an integral domain.*

PROOF: Let $\mathbb{F}$ be a field. We claim that $\mathbb{F}$ is an integral domain: that is, the elements of $\mathbb{F}$ satisfy the zero product property. Let $a, b \in \mathbb{F}$ and assume that $ab = 0$. We need to show that $a = 0$ or $b = 0$. Assume that $a \neq 0$; since $\mathbb{F}$ is a field, a has a multiplicative inverse. Multiply both sides of $ab = 0$ on the left by a^{-1} and apply Proposition 7.4 to obtain

$$b = 1 \cdot b = \left(a^{-1}a\right) b = a^{-1}(ab) = a^{-1} \cdot 0 = 0.$$

Hence $b = 0$.

We had assumed that $ab = 0$ and $a \neq 0$. By concluding that $b = 0$, the fact that a and b are arbitrary show that $\mathbb{F}$ is an integral domain. Since $\mathbb{F}$ is an arbitrary field, every field is an integral domain. □

Not every integral domain is a field, however. The most straightforward example is $\mathbb{Z}$.

Exercises.

Exercise 7.21: Explain why $n\mathbb{Z}$ is always an integral domain. Is it also a field?

Exercise 7.22: Show that $\mathbb{Z}_n$ is an integral domain if and only if n is irreducible. Is it also a field in these cases?

Exercise 7.23: You might think from Exercise 7.22 that we can turn $\mathbb{Z}_n$ into a field, or at least an integral domain, in the same way that we turned $\mathbb{Z}_n$ into a multiplicative group: that is, working with $\mathbb{Z}_n^*$. Explain that this doesn't work in general, because $\mathbb{Z}_n^*$ isn't even a ring.

Exercise 7.24: Show that if R is an integral domain, then the set of fractions has the following properties for any nonzero $a, b, c \in R$:

$$\frac{ac}{bc} = \frac{ca}{cb} = \frac{a}{b} \qquad \text{and} \qquad \frac{0_R}{a} = \frac{0_R}{1} = 0_{\mathrm{Frac}(R)} \qquad \text{and} \qquad \frac{a}{a} = \frac{1_R}{1_R} = 1_{\mathrm{Frac}(R)}.$$

Exercise 7.25: To see concretely why $\mathrm{Frac}(R)$ is not a field if R is not a domain, consider $R = \mathbb{Z}_4$. Find nonzero $b, q \in \mathrm{Frac}(R)$ such that $bq = 0$, and use them to find $f, g \in \mathrm{Frac}(R)$ such that $fg \notin \mathrm{Frac}(R)$.

7.3: Polynomial rings

Polynomials make useful motivating examples for some of the remaining topics, and it turns out that we can identify rings of polynomials. The following definition may seem pedantic, but it is important to fix these terms now to avoid confusion later.

Definition 7.26: Let R be a ring.

- An **indeterminate variable of** R is a symbol that represents an arbitrary value of R. A **constant of** R is a symbol that represents a fixed value of R. Usually we refer to an indeterminate variable as simply "a variable".
- A **monomial over** R is a finite product ($\times$) of variables of R.
  - The **total degree** of a monomial is the number of factors in the product.
  - We say that two monomials are **like monomials** if the factors of each are identical.
- A **term over** R is a constant, *or* the product of a monomial over R and a constant of R. The constant in a term is called the **coefficient** of the term. Two terms are **like terms** if their monomials are like monomials.
- A **polynomial over** R is a finite sum ($+$) of terms over R. We can write a generic polynomial f as $f = a_1t_1 + a_2t_2 + \cdots + a_mt_m$ where each $a_i \in R$ and each t_i is a monomial. If we write T_f for the set of monomials of f with non-zero coefficient, then we can also write f as

$$f = \sum_{i=1,\ldots,\#T_f} a_i t_i = \sum_{t \in T_f} a_t t.$$

  - We say that the polynomial f is a **zero polynomial** if, whenever we substitute arbitrary values of R for the variables, f simplifies to zero. (We will see that this can happen even if $f \neq 0_R$.)
  - We say that f is a **constant polynomial** if all the non-constant terms have coefficient zero. Notice that 0_R is thus a constant polynomial.
  - We say that two polynomials f and g are equal if $T_f = T_g$ and the coefficients of corresponding monomials are equal.
- $R[x]$ is the set of **univariate** polynomials in in the variable x over R. That is, $f \in R[x]$ if and only if there exist $m \in \mathbb{N}$ and $a_m, a_{m-1}, \ldots, a_1 \in R$ such that

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0.$$

- The set $R[x,y]$ is the set of **bivariate** polynomials in the variables x and y whose coefficients are in R.
- For $n \geq 2$, the set $R[x_1, x_2, \ldots, x_n]$ is the set of **multivariate** polynomials in the variables $x_1, x_2, \ldots, x_n$ whose coefficients are in R.
- The **degree** of a univariate polynomial f, written $\deg f$, is the largest of the total degrees of the monomials of f. We write $\mathrm{lm}(f)$ for the monomial of f with that degree, and $\mathrm{lc}(f)$ for its coefficient. Unless we say otherwise, the degree of a multivariate

Example 7.27: Definition 7.26 tells us that $\mathbb{Z}_6[x,y]$ is the set of bivariate polynomials in x and y whose coefficients are in $\mathbb{Z}_6$. For example,

$$f(x,y) = 5x^3 + 2x \in \mathbb{Z}_6[x,y] \quad \text{and} \quad g(x,y) = x^2y^2 - 2x^3 + 4 \in \mathbb{Z}_6[x,y].$$

The ground ring for both f and g is $\mathbb{Z}_6$. Observe that f can be considered a univariate polynomial, in which case $\deg f = 3$.

We also consider constants to be polynomials of degree 0; thus $4 \in \mathbb{Z}_6[x,y]$ and even $0 \in \mathbb{Z}_6[x,y]$.

Example 7.28: If f is a zero polynomial, that does *not* imply that f is the constant polynomial 0. For example, let $f(x) = x^2 + x \in \mathbb{Z}_2[x]$. Observe that

$$f(0) = 0^2 + 0 \text{ and}$$
$$f(1) = 1^2 + 1 = 0 \text{ (in } \mathbb{Z}_2\text{!)}.$$

Here f is a zero polynomial *even though it is not zero.*

Our goal is to show that $R[x_1,\ldots,x_n]$ is a ring for any $n \in \mathbb{N}^+$. Before we can do that, let us make precise our notions of addition and multiplication of polynomials.

Definition 7.29: To define **addition** of polynomials, let $f,g \in R[x_1,\ldots,x_n]$ and $T = T_f \cup T_g$. Write

$$f = \sum_{t\in T} a_t t$$
$$g = \sum_{t\in T} b_t t.$$

We define addition in $R[x]$ by

$$f + g = \sum_{t\in T} (a_t + b_t)\, t.$$

We define polynomial multiplication by

$$fg = \sum_{t\in T} \left[a_t t \left(\sum_{u\in T} b_u u \right) \right];$$

that is, polynomial multiplication is simply the sum of the term multiples of the second polynomial with the terms of the first. Notice that in the second summand we use u instead of t to distinguish the terms appearing in g from those appearing in f.

So when is the zero polynomial the constant polynomial 0?

Proposition 7.30: *If R is a non-zero integral domain, then the following are equivalent.*
(A) *0 is the only zero polynomial in $R[x_1,\ldots,x_n]$.*
(B) *R has infinitely many elements.*

Before proving Proposition 7.30, we need the following lemma.

Theorem 7.31 (The Factor Theorem): *If R is a non-zero integral domain, $f \in R[x]$, and $a \in R$, then $f(a) = 0$ iff $x-a$ divides $f(x)$.*

PROOF: If $x-a$ divides $f(x)$, then there exists $q \in R[x]$ such that $f(x) = (x-a)\cdot q(x)$. By substitution, $f(a) = (a-a)\cdot q(a) = 0_R \cdot q(a) = 0_R$.

Conversely, assume $f(a) = 0$. You will show in Exercise 7.35 that we can write $f(x) = q(x)\cdot(x-a) + r$ for some $r \in R$. Thus

$$0 = f(a) = q(a)\cdot(a-a) + r = r,$$

and substitution yields $f(x) = q(x)\cdot(x-a)$. In other worse, $x-a$ divides $f(x)$, as claimed. □

We now turn our attention to proving Proposition 7.30.

PROOF OF LEMMA 7.30: Assume that R is a non-zero integral domain.

(A) ⇒ (B): We proceed by the contrapositive. Assume that R has finitely many elements. We can label them all as $r_1, r_2, \ldots, r_m$. Let

$$f(x_1,\ldots,x_n) = (x_1 - r_1)(x_1 - r_2)\cdots(x_1 - r_m).$$

Let $b_1,\ldots,b_n \in R$. By assumption, R is finite, so $b_1 = r_i$ for some $i \in \{1,2,\ldots,m\}$. By substitution,

$$f(b_1,b_2,\ldots,b_n) = (r_i - r_1)\cdots(r_i - r_{i-1})(r_i - r_i)(r_i - r_{i+1})\cdots(r_i - r_m).$$

Now $r_i - r_i = 0$ by the properties of a ring, and by the properties of zero $f(b_1,b_2,\ldots,b_n) = 0$. Since a was arbitrary in R, f is a zero polynomial—but it is not the constant polynomial 0. We have shown that ¬(B) implies ¬(A); thus (A) implies (B).

(A) ⇐ (B): Assume that R has infinitely many elements. Let f be any zero polynomial. We proceed by induction on n, the number of variables in $R[x_1,\ldots,x_n]$.

Inductive base: Let $a \in R$. By definition of the zero polynomial, $f(a) = 0$. By Lemma 7.31, $x-a$ divides f. Since a is arbitrary, all $x-a$ divide f. There are infinitely many such $x-a$, but f has only finitely many terms, and so can have only finitely many factors (otherwise the degree would not be finite, or R would not be an integral domain). Hence f is the zero polynomial.

Inductive hypothesis: Assume that for all $i < n$, if $f \in R[x_1,\ldots,x_i]$ is a zero polynomial, then f is the constant polynomial 0.

Inductive step: Let $f \in R[x_1,\ldots,x_n]$ be a zero polynomial. Let $a_n \in R$ be non-zero, and substitute $x_n = a_n$ into f. Denote the resulting polynomial as g. Observe that $g \in R\left[x_1,\ldots,x_{n-1}\right]$.

We claim that g is a zero polynomial in $R\left[x_1,\ldots,x_{n-1}\right]$. By way of contradiction, assume that it is not. Then there exist non-zero $a_1,\ldots,a_{n-1}$ such that substituting $x_i = a_i$ gives us a non-zero value. However, we have also substituted non-zero a_n for x_n; thus $f(a_1,\ldots,a_n) \neq 0$. This contradicts the definition of a zero polynomial. Hence g is a zero polynomial in $R\left[x_1,\ldots,x_{n-1}\right]$.

By the inductive hypothesis, g is the constant polynomial 0. Since a_n is arbitrary, this is true for all $a_n \in R$. This implies that any the terms of f containing any of the variables $x_1,\ldots,x_{n-1}$ has a coefficient of zero. The only non-zero terms are those whose only variables are x_n, so $f \in R[x_n]$. Again, the inductive hypothesis implies that f is zero. □

We come to the main purpose of this section.

Theorem 7.32: *The univariate and multivariate polynomial rings over a ring R are themselves rings.*

PROOF: Let $n \in \mathbb{N}^+$ and R a ring. We claim that $R[x_1,\ldots,x_n]$ is a ring. To consider the requirements of a ring; select $f,g,h \in R[x]$ and let $T = T_f \cup T_g \cup T_h$. Write

$$f = \sum_{t\in T} a_t t, \quad g = \sum_{t\in T} b_t t, \quad h = \sum_{t\in T} c_t t.$$

(R1) First we show that $R[x_1,\ldots,x_n]$ is an abelian group.

(closure) By the definition of polynomial addition,

$$(f+g)(x) = \sum_{t\in T} (a_t + b_t)\, t.$$

Since R is closed under addition, $f+g \in R[x_1,\ldots,x_n]$.

(associativity) We rely on the associative property of R:

$$\begin{aligned} f+(g+h) &= \sum a_t t + \left(\sum b_t t + \sum c_t t\right) \\ &= \sum a_t t + \sum (b_t + c_t)\, t \\ &= \sum [a_t + (b_t + c_t)]\, t \\ &= \sum [(a_t + b_t) + c_t]\, t \\ &= \sum (a_t + b_t)\, t + \sum_{t\in T} c_t t \\ &= \left(\sum a_t t + \sum b_t t\right) + \sum c_t t \\ &= (f+g)+h. \end{aligned}$$

(identity) We claim that the constant polynomial 0 is the identity. To see this, let $u \in T$; then

$$\begin{aligned} f + 0 &= \sum a_t t + 0 \\ &= \sum a_t t + \sum 0 \cdot t \\ &= \sum (a_t + 0)\, t \\ &= f. \end{aligned}$$

(inverse) Let $p = \sum_{t \in T} (-a_t)\, t$. We claim that p is the additive inverse of f. In fact,

$$\begin{aligned} p + f &= \sum (-a_t)\, t + \sum a_t t \\ &= \sum (-a_t + a_t)\, t \\ &= \sum 0 \cdot t \\ &= 0. \end{aligned}$$

(In the definition of p, I should state that the sum is over $t \in T$; otherwise it isn't clear.)

(commutativity) By the definition of polynomial addition, $g + f = \sum (b_t + a_t)\, t$. Since R is commutative under addition, addition of coefficeints is commutative, so

$$\begin{aligned} f + g &= \sum a_t t + \sum b_t t \\ &= \sum (a_t + b_t)\, t \\ &= \sum (b_t + a_t)\, t \\ &= \sum b_t t + \sum a_t t \\ &= g + f. \end{aligned}$$

(R2) Applying the definitions of polynomial and term multiplication, and recalling that integral domains are commutative rings, we have

$$\begin{aligned} f g &= \sum_{t \in T} \left[(a_t t) \sum_{u \in T} b_u u \right] \\ &= \sum_{t \in T} \left[\sum_{u \in T} ((a_t t)\, (b_u u)) \right] \\ &= \sum_{t \in T} \left[\sum_{u \in T} (a_t b_u)\, (t u) \right]. \end{aligned}$$

Since R is closed under multiplication, each $(a_t b_u)(tu)$ is a term. Thus fg is a sum of sums of terms, or a sum of terms. In other words, $fg \in R[x_1, \ldots, x_n]$.

(R3) We start by applying the form of a product that we derived in (R2):

$$\begin{aligned}(fg)h &= \left[\sum_{t\in T}\left[\sum_{u\in T}(a_t b_u)(tu)\right]\right]\cdot\sum_{v\in T}c_v v \\ &= \sum_{t\in T}\left[\sum_{u\in T}\left[\sum_{v\in T}[(a_t b_u)c_v][(tu)v]\right]\right].\end{aligned}$$

Now apply the associative property of multiplication in R and the associative property of addition in $\mathbb{Z}$:

$$(fg)h = \sum_{t\in T}\left[\sum_{u\in T}\left[\sum_{v\in T}[a_t(b_u c_v)][t(uv)]\right]\right].$$

Now unapply the form of a product that we derived in (R2):

$$\begin{aligned}(fg)h &= \sum_{t\in T}\left[\sum_{u\in T}\left[\sum_{v\in T}[a_t(b_u c_v)][t(uv)]\right]\right] \\ &= \sum_{t\in T}a_t t\cdot\left[\sum_{u\in T}\left[\sum_{v\in T}(b_u c_v)(uv)\right]\right] \\ &= f(gh).\end{aligned}$$

(R4) To analyze $f(g+h)$, first apply addition, then multiplication:

$$\begin{aligned}f(g+h) &= \sum_{t\in T}a_t t\cdot\left(\sum_{u\in T}b_u u+\sum_{u\in T}c_u u\right) \\ &= \sum_{t\in T}a_t t\cdot\sum_{u\in T}(b_u+c_u)u \\ &= \sum_{t\in T}\left[\sum_{u\in T}[a_t(b_u+c_u)](tu)\right].\end{aligned}$$

Now apply the distributive property in the ring, and unapply the addition and multi-

plication:

$$\begin{aligned} f(g+h) &= \sum_{t\in T}\left[\sum_{u\in T}(a_t b_u + a_t c_u)(tu)\right] \\ &= \sum_{t\in T}\left[\sum_{u\in T}[(a_t b_u)(tu) + (a_t c_u)(tu)]\right] \\ &= \sum_{t\in T}\left[\sum_{u\in T}(a_t b_u)(tu) + \sum_{u\in T}(a_t c_u)(tu)\right] \\ &= \sum_{t\in T}\left[\sum_{u\in T}(a_t b_u)(tu)\right] + \sum_{t\in T}\left[\sum_{u\in T}(a_t c_u)(tu)\right] \\ &= fg + fh. \end{aligned}$$

□

Exercises.

Exercise 7.33: Let $f(x) = x$ and $g(x) = x+1$ in $\mathbb{Z}_2[x]$.
(a) Show that f and g are not zero polynomials.
(b) Compute the polynomial $p = fg$.
(c) Show that $p(x)$ is a zero polynomial.
(d) Explain why this does *not* contradict Proposition 7.30.

Exercise 7.34: Pick at random a degree 5 polynomial f in $\mathbb{Z}[x]$. Then pick at random an integer a.
(a) Find $q \in \mathbb{Z}[x]$ and $r \in \mathbb{Z}$ such that $f(x) = q(x)\cdot(x-a)+r$.
(b) Explain why you *cannot* pick a nonzero integer b at random and expect willy-nilly to find $q \in \mathbb{Z}[x]$ and $r \in \mathbb{Z}$ such that $f(x) = q(x)\cdot(bx-a)+r$.
(c) Explain why you *can* pick a nonzero integer b at random and expect willy-nilly to find $q \in \mathbb{Z}[x]$ and $r, s \in \mathbb{Z}$ such that $s\cdot f(x) = q(x)\cdot(bx-a)+r$. (Neat, huh?)
(d) If the requirements of (b) were changed to finding $q \in \mathbb{Q}[x]$ and $r \in \mathbb{Q}$, would you then be able to carry out (b)? Why or why not?

Exercise 7.35: Let R be an integral domain, $f \in R[x]$, and $a \in R$. Show that there exists $q \in R[x]$ and $r \in R$ such that $f(x) = q(x)\cdot(x-a)+r$.

Exercise 7.36: Let R be an integral domain.
(a) Show that $R[x]$ is also an integral domain.
(b) How does this not contradict Exercise (7.33)? After all, $\mathbb{Z}_2$ is a field, and thus an integral domain!

Exercise 7.37: Let R be a ring, and $f, g \in R[x]$. Show that $\deg(f+g) \leq \max(\deg f, \deg g)$.

Exercise 7.38: Let R be a ring and define

$$R(x) = \text{Frac}(R[x]);$$

for example,

$$\mathbb{Z}(x) = \text{Frac}(\mathbb{Z}[x]) = \left\{ \frac{p}{q} : \ p, q \in \mathbb{Z}[x] \right\}.$$

Is $R(x)$ a ring? is it a field?

7.4: Euclidean domains

In this section we consider an important similarity between the ring of integers and the ring of polynomials. This similarity will motivate us to define a new kind of ring. We will then show that all rings of this type allow us to perform important operations that we find both useful and necessary. What is the similarity? The ability to *divide with remainder*.

Theorem 7.39: *Let R be one of the rings $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, and consider the polynomial ring $R[x]$. Let $f, g \in R[x]$ with $f \neq 0$. There exist unique $q, r \in R[x]$ satisfying (D1) and (D2) where*
(D1) $g = qf + r$;
(D2) $r = 0$ *or* $\deg r < \deg f$.
We call g the ***dividend****, f the* ***divisor****, q the* ***quotient****, and r the* ***remainder****.*

PROOF: The proof is essentially the procedure of long division of polynomials.

If $\deg g < \deg f$, let $r = g$ and $q = 0$. Then $g = qf + r$ and $\deg r < \deg f$. Otherwise, $\deg g \geq \deg f$. Let $\deg f = m$ and $n = \deg g - \deg f$. We proceed by induction on n.

For the *inductive base* $n = 0$, notice that $\deg g = \deg f = m$. Choose $a_m, \ldots, a_1, b_m, \ldots, b_1 \in R$ such that

$$g = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$
$$f = b_m x_m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0.$$

Let $q = \frac{a_m}{b_m}$ and $r = g - qf$. We have $g = qf + r$, but is $\deg r < \deg f$? Apply substitution,

distribution, and polynomial addition to obtain

$$\begin{aligned} r &= g - qf \\ &= \left(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0\right) - \frac{a_m}{b_m}\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0\right) \\ &= \left(a_m - \frac{a_m}{b_m}\cdot b_m\right)x^m + \left(a_{m-1} - \frac{a_m}{b_m}\cdot b_{m-1}\right)x^{m-1} + \cdots + \left(a_0 - \frac{a_m}{b_m}\cdot b_0\right) \\ &= 0x^m + \left(a_{m-1} - \frac{a_m}{b_m}\cdot b_{m-1}\right)x^{m-1} + \cdots + \left(a_0 - \frac{a_m}{b_m}\cdot b_0\right). \end{aligned}$$

Notice that if $r \neq 0$, then $\deg r < \deg f$.

For the *inductive hypothesis*, assume that for all $i < n$ there exist $q, r \in R[x]$ such that $g = qf + r$ and $r = 0$ or $\deg r < \deg f$.

For the *inductive step,* let $\ell = \deg g$. Choose $a_m, \ldots, a_0, b_\ell, \ldots, b_0 \in R$ such that

$$\begin{aligned} f &= a_m x^m + \cdots + a_0 \\ g &= b_\ell x^\ell + \cdots + b_0. \end{aligned}$$

Let $q = \frac{a_m}{b_\ell}\cdot x^n$ and $r = g - qf$. Apply substitution and distribution to obtain

$$\begin{aligned} g' &= g - qf \\ &= \left(b_\ell x^\ell + \cdots + b_0\right) - \frac{b_\ell}{a_m}\cdot x^n\left(a_m x^m + \cdots + a_0\right) \\ &= \left(b_\ell x^\ell + \cdots + b_0\right) - \left(b_\ell x^{m+n} + \frac{b_\ell a_{m-1}}{a_m}\cdot x^{m-1+n} + \cdots + \frac{b_\ell a_0}{a_m}\cdot x^n\right). \end{aligned}$$

Recall that $n = \deg g - \deg f = \ell - m$, so $\ell = m + n > n$. Apply substitution and polynomial addition to obtain

$$\begin{aligned} g' = g - qf &= \left(b_\ell x^\ell + \cdots + b_0\right) - \left(b_\ell x^\ell + \frac{b_\ell a_{m-1}}{a_m}\cdot x^{\ell-1} + \cdots + \frac{b_\ell a_0}{a_m}\cdot x^n\right) \\ &= 0x^\ell + \left(b_{\ell-1} - \frac{b_\ell a_{m-1}}{a_m}\right)x^{\ell-1} + \cdots + \left(b_n - \frac{b_\ell a_0}{a_m}\right)x^n + b_{n-1}x^{n-1}\cdots + b_0. \end{aligned}$$

Observe that $\deg g' < \ell = \deg g$, so $\deg g' - \deg f < n$. Apply the inductive hypothesis to find $q', r \in R[x]$ such that $g' = q'f + r$ and $r = 0$ or $\deg r < \deg f$. Then

$$\begin{aligned} g = qf + g' &= qf + (q'f + r) \\ &= (q + q')f + r. \end{aligned}$$

Since $R[x]$ is a ring, $q + q' \in R[x]$, and we have shown the existence of a quotient and remainder.

For uniqueness, assume that there exist $q_1, q_2, r_1, r_2 \in R[x]$ such that $g = q_1 f + r_1 = q_2 f + r_2$ and $\deg r_1, \deg r_2 < \deg f$. Then

$$\begin{aligned} q_1 f + r_1 &= q_2 f + r_2 \\ 0 &= (q_2 - q_1) f + (r_2 - r_1). \end{aligned} \tag{19}$$

If $q_2 - q_1 \neq 0$, then every term of $(q_2 - q_1)\operatorname{lm}(f)$ has degree no smaller than $\deg f$. Since every term of $r_2 - r_1$ has degree smaller than $\deg f$, there are no like terms between the two. Thus, there can be no cancellation between $(q_2 - q_1)\operatorname{lm}(f)$ and $r_2 - r_1$, and for similar reasons there can be no cancellation between $(q_2 - q_1)\operatorname{lm}(f)$ and lower-degree terms of $(q_2 - q_1) f$. However, the coefficients of the terms of $(q_2 - q_1)\operatorname{lm}(f)$ are all 0 on the left hand side, so they must likewise be all zero on the right hand side. That implies $(q_2 - q_1)\operatorname{lm}(f)$ is equal to the constant polynomial 0. We are working in an integral domain (Exercise 7.36), and $\operatorname{lm}(f) \neq 0$, so it mus tbe that $q_2 - q_1 = 0$. In other words, $q_1 = q_2$.

In addition, since $q_2 - q_1 = 0$, substitution into (19) implies that $0 = r_2 - r_1$. Immediately we have $r_1 = r_2$. We have shown that q and r are unique. □

We did *not* list $\mathbb{Z}$ as one of the rings of the theorem. Exercise 7.34 explains why. That's a shame: for some integral domains, we can perform a division on the corresponding polynomial ring, but for others we cannot. We will classify the ones in which we can perform some kind of division; you will see that we generalize the notion of remainder to something special here.

Definition 7.40: Let R be an integral domain and v a function mapping the nonzero elements of R to $\mathbb{N}^+$. We say that R is a **Euclidean Domain** with respect to the **valuation function** v if it satisfies (E1) and (E2) where

(E1) $v(r) \leq v(rs)$ for all nonzero $r, s \in R$.

(E2) For all nonzero $f \in R$ and for all $g \in R$, there exist $q, r \in R$ such that
- $g = qf + r$, and
- $r = 0$ or $v(r) < v(f)$.

If $f, g \in R$ are such that $f \neq 0$ and $g = qf$ for some $q \in R$, then we say that f **divides** g.

Example 7.41: Both $\mathbb{Z}$ and $R[x]$ of Theorem 7.39 are Euclidean domains.
- In $\mathbb{Z}$, the valuation function is $v(r) = |r|$.
- In $R[x]$ above, the valuation function is $v(r) = \deg r$.

On the other hand, $\mathbb{Z}[x]$ is *not* a Euclidean domain with the valuation function $v(r) = \deg r$. If $f = 2$ and $g = x$, we cannot find $q, r \in \mathbb{Z}[x]$ such that $g = qf + r$ and $\deg r < \deg f$. The best we can do is $x = 0 \cdot 2 + x$, but $\deg x > \deg 2$.

Theorem 7.42: *Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a Euclidean domain.*

PROOF: You do it! See Exercise 7.50. □

Since we can perform division with remainder in Euclidean rings, we can compute the greatest common divisor using the Euclidean algorithm. Unlike integers, however, we have to relax our expectation of uniqueness for the greatest common divisor.

Definition 7.43: Let R be a Euclidean domain with respect to v, and let $a, b \in R$. If there exists $d \in R$ such that $d \mid a$ and $d \mid b$, then we call d a **common divisor** of a and b. If in addition all other common divisors d' of a and b divide d, then d is a **greatest common divisor** of a and b.

Notice that the definition refers to *a* greatest common divisor, not *the* greatest common divisor. *There can be many greatest common divisors!*

Example 7.44: Consider $x^2-1, x^2+2x+1 \in \mathbb{Q}[x]$. Recall from Theorem 7.39 and Definition 7.40 that $\mathbb{Q}[x]$ is a Euclidean domain with respect to the valuation function $v(p) = \deg p$. Both of the given polynomials factor:

$$x^2-1 = (x+1)(x-1) \quad \text{and} \quad x^2+2x+1 = (x+1)^2,$$

so we see that $x+1$ is a divisor of both. In fact, it is a greatest common divisor, since no polynomial of degree two divides both x^2-1 and x^2+2x+1.

However, $x+1$ is not the *only* greatest common divisor. Another greatest common divisor is $2x+2$. It may not be obvious that $2x+2$ divides both x^2-1 and x^2+2x+1, but it does:

$$x^2-1 = (2x+2)\left(\frac{x}{2}-\frac{1}{2}\right) \quad \text{and} \quad x^2+2x+1 = (2x+2)\left(\frac{x}{2}+\frac{1}{2}\right).$$

Notice that $2x+2$ divides $x+1$ and vice-versa; also that $\deg(2x+2) = \deg(x+1)$.

Likewise, $\frac{x+1}{3}$ is also a greatest common divisor of x^2-1 and x^2+2x+1.

In fact, notice that in this new definition, there exists more than one greatest common divisor in $\mathbb{Z}$. For example, for $a = 8$ and $b = 12$, both 4 *and* -4 are greatest common divisors! This happens because each divides the other, emphasizing that for us, the notion of a "greatest" common divisor is relative to divisibility, not to other orderings.

That said, all greatest common divisors have something in common.

Proposition 7.45: *Let R be a Euclidean domain with respect to v, and $a, b \in R$. Suppose that d is a greatest common divisor of a and b. If d' is a common divisor of a and b, then $v(d') \leq v(d)$. If d' is another greatest common divisor of a and b, then $v(d) = v(d')$.*

PROOF: Since d is a greatest common divisor of a and b, and d' is a common divisor, the definition of a greatest common divisor tells us that d divides d'. Thus there exists $q \in R$ such that $qd' = d$. From property (E1) of the valuation function,

$$v(d') \leq v(qd') = v(d).$$

On the other hand, if d' is also a greatest common divisor of a and b, an argument similar to the one above shows that

$$v(d) \leq v(d') \leq v(d).$$

Hence $v(d) = v(d')$. □

Finally we come to the point of a Euclidean domain: we can use the Euclidean algorithm to compute a gcd of any two elements! Essentially we transcribe the Euclidean Algorithm for integers (Theorem 6.4 on page 130 of Section 6.1).

Theorem 7.46 (The Euclidean Algorithm for Euclidean domains): *Let R be a Euclidean domain with valuation v and $m, n \in R \setminus \{0\}$. One can compute a greatest common divisor of m, n in the following way:*

1. *Let $s = m$ and $t = n$.*
2. *Repeat the following steps until $t = 0$:*
   (a) *Let q be the quotient and r the remainder after dividing s by t.*
   (b) *Assign s the current value of t.*
   (c) *Assign t the current value of r.*

The final value of s is a greatest common divisor of m and n.

PROOF: You do it! See Exercise 7.51. □

Just as we could adapt the Euclidean Algorithm for integers to the Extended Euclidean Algorithm in order to compute $a, b \in \mathbb{Z}$ such that

$$am + bn = \gcd(m, n),$$

we can do the same thing in Euclidean domains, using exactly the same technique. In fact, you will need this for Exercise 7.46

Exercises.

Exercise 7.47: Let $f = x^2 + 1$ and $g = x^3 - 1$.

(a) Show that 1 is a greatest common divisor of f and g in $\mathbb{Q}[x]$, and find $a, b \in \mathbb{Q}[x]$ such that $1 = af + bg$.

(b) Recall that $\mathbb{Z}_5$ is a field. Show that 1 is a greatest common divisor of f and g in $\mathbb{Z}_5[x]$, and find $a, b \in \mathbb{Z}_5[x]$ such that $1 = af + bg$.

(c) Recall that $\mathbb{Z}[x]$ is not a Euclidean domain. Explain why the result of part (a) cannot be used to show that 1 is a greatest common divisor of f and g in $\mathbb{Z}[x]$. What would you get if you used the Euclidean algorithm on f and g in $\mathbb{Z}[x]$?

Exercise 7.48: Let $f = x^4 + 9x^3 + 27x^2 + 31x + 12$ and $g = x^4 + 13x^3 + 62x^2 + 128x + 96$.

(a) Compute a greatest common divisor of f and g in $\mathbb{Q}[x]$.

(b) Recall that $\mathbb{Z}_{31}$ is a field. Compute a greatest common divisor of f and g in $\mathbb{Z}_{31}[x]$.
(c) Recall that $\mathbb{Z}_3$ is a field. Compute a greatest common divisor of f and g in $\mathbb{Z}_3[x]$.
(d) Even though $\mathbb{Z}[x]$ is not a Euclidean domain, it still has greatest common divisors. What's more, we can compute the greatest common divisors using the Euclidean algorithm! How?

Exercise 7.49: Show that every field is a Euclidean domain.

Exercise 7.50: Prove Theorem 7.42.

Exercise 7.51: Prove Theorem 7.46, the Euclidean Algorithm for Euclidean domains.

Exercise 7.52: A famous Euclidean domain is the ring of *Gaussian integers*

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

where $i^2 = -1$. The valuation function is

$$v(a + bi) = a^2 + b^2.$$

To find any quotient and remainder, you must use the fact that the smallest distance between $a + bi$ and other complex number is at most $\frac{1}{2}\sqrt{2\left(a^2 + b^2\right)}$.

(a) Assuming the facts given about v, divide:
  (i) 11 by 3;
  (ii) 11 by $3i$;
  (iii) $2 + 3i$ by $1 + 2i$.
(b) Show that v is, in fact, a valuation function suitable for a Euclidean domain.
(c) Give a general method for dividing Gaussian integers.

Chapter 8:
Ideals

This chapter fills two roles. Some sections describe ring analogues to structures that we introduced in group theory:

- Section 8.1 introduces the *ideal*, an analogue to a normal subgroup;
- Section 8.4 provides an analogue of quotient groups; and
- Section 8.6 decribes ring homomorphisms.

The remaining sections use these ring structures to introduce new kinds of ring structures:

- Section 8.3 highlights an important class of ideals;
- Section 8.5 brings us to finite fields, which are important for computation in polynomial rings; and
- Section 8.7 describes a fundamental relationship between ideals and the zeros of polynomials.

8.1: Ideals

Just as groups have subgroups, rings have subrings:

Definition 8.1: Let R be a ring, and S a nonempty subset of R. If S is also a ring under the same operations as R, then S is a subring of R.

Example 8.2: Recall from Exercise 7.9 that $2\mathbb{Z}$ is a ring; since $2\mathbb{Z} \subsetneq \mathbb{Z}$, it is a subring of $\mathbb{Z}$.

To show that a subset of a ring is a subring, do we have to show all four ring properties? No: as with subgroups, we can simplify the characterization to two properties:

Theorem 8.3 (The Subring Theorem): *Let R be a ring and S be a nonempty subset of R. The following are equivalent:*

(A) *S is a subring of R.*

(B) *S is closed under subtraction and multiplication. That is, for all $a, b \in S$*

(S1) *$a - b \in S$, and*

(S2) *$ab \in S$.*

PROOF: That (A) implies (B) is clear, so assume (B). From (B) we know that for any $a, b \in S$ we have (S1) and (S2). Now (S1) is essentially the Subgroup Theorem, so S is an additive subgroup of the additive group R. On the other hand, (S2) only tells us that S satisfies property $(R2)$ of a ring, but any elements of S are elements of R, so the associative and distributive properties follow from inheritance. Thus S is a ring in its own right, which makes it a subring of R. □

You might think that, just as we moved from subgroups to quotient groups via cosets, we will move from subrings to "quotient rings" via the ring analogue of normal subgroups. While this is true, the analogue may not have quite the form you expect.

Definition 8.4: Let A be a subring of R that satisfies the **absorption property**:

$$\forall r \in R \; \forall a \in A \quad ra \in A.$$

Then A is an **ideal subring** of R, or simply, an **ideal**, and we write $A \triangleleft R$. An ideal A is **proper** if $\{0\} \neq A \neq R$.

Recall that our rings are assumed to be commutative, so if $ra \in A$ then $ar \in A$, also.

Example 8.5: Recall the subring $2\mathbb{Z}$ of the ring $\mathbb{Z}$. We show that $2\mathbb{Z} \triangleleft \mathbb{Z}$: let $r \in \mathbb{Z}$, and $a \in 2\mathbb{Z}$. By definition of $2\mathbb{Z}$, there exists $d \in \mathbb{Z}$ such that $a = 2d$. Substitution gives us

$$ra = r \cdot 2d = 2(rd) \in 2\mathbb{Z},$$

so $2\mathbb{Z}$ "absorbs" multiplication by $\mathbb{Z}$. This makes $2\mathbb{Z}$ an ideal of $\mathbb{Z}$.

Naturally, we can generalize this proof to arbitrary $n \in \mathbb{Z}$: see Exercises 8.16 and 8.17.

Ideals in the ring of integers have a nice property that we will use in future examples.

Lemma 8.6: *Let $a, b \in \mathbb{Z}$. The following are equivalent:*
(A) $a \mid b$;
(B) $b\mathbb{Z} \subseteq a\mathbb{Z}$.

PROOF: You do it! See Exercise 8.18. □

Example 8.7: Certainly $3 \mid 6$ since $3 \cdot 2 = 6$. Look at the ideals generated by 3 and 6:

$$3\mathbb{Z} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$
$$6\mathbb{Z} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}.$$

Inspection suggests that $6\mathbb{Z} \subseteq 3\mathbb{Z}$. Is it? Let $x \in 6\mathbb{Z}$. By definition, $x = 6q$ for some $q \in \mathbb{Z}$. By substitution, $x = (3 \cdot 2)q = 3(2 \cdot q) \in 3\mathbb{Z}$. Since x was arbitrary in $6\mathbb{Z}$, we have $6\mathbb{Z} \subseteq 3\mathbb{Z}$.

The absorption property makes ideals useful for studying roots of polynomials.

Example 8.8: You showed in Exercise 7.3 that $\mathbb{C}[x, y]$ is a ring. Let $f = x^2 + y^2 - 4$, $g = xy - 1$. Define $A = \{hf + kg : h, k \in \mathbb{C}[x, y]\}$. We claim that A is an ideal:

- For any $a, b \in A$, we can write $a = h_a f + k_a g$ and $b = h_b f + k_b g$ for some $h_a, h_b, k_a, k_b \in \mathbb{C}[x, y]$. Thus

$$\begin{aligned} a - b &= (h_a f + k_a g) - (h_b f + k_b g) \\ &= (h_a - h_b) f + (k_a - k_b) g \in A. \end{aligned}$$

  It takes a little more work to show that $ab \in A$:

$$\begin{aligned} ab &= (h_a f + k_a g)(h_b f + k_b g) \\ &= h_a h_b f^2 + h_a k_b f g + h_b k_a f g + k_a k_b g^2 \\ &= (h_a h_b f + h_a k_b g + h_b k_a g) f + (k_a k_b g) g. \end{aligned}$$

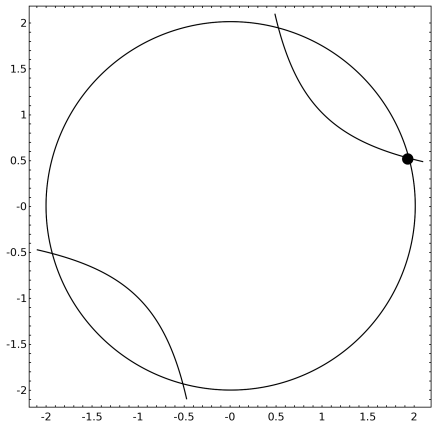


Figure 8.1. A common root of x^2+y^2-4 and $xy-1$

Let

$$h' = h_a h_b f + h_a k_b g + h_b k_a g \quad \text{and} \quad k' = k_a k_b g;$$

then $ab = h'f + k'g$, so $ab \in A$, as well. By the Subring Theorem, A is a subring of $\mathbb{C}[x,y]$.

- For any $a \in A$, $r \in \mathbb{C}[x,y]$, write a as before; then

$$ra = r(h_a f + k_a g) = r(h_a f) + r(k_a g) = (rh_a) f + (rk_a) g \in A.$$

Thus, A satisfies the absorption property.

We have shown that A satisfies the subring and absorption properties; thus, $A \triangleleft \mathbb{C}[x,y]$.

What's interesting about A is the following algebraic fact: *the common roots of f and g are roots of any element of A.* To see this, let (α,β) be a common root of f and g; that is, $f(\alpha,\beta) = g(\alpha,\beta) = 0$. Let $p \in A$; by definition, we can write $p = hf + kg$ for some $h,k \in \mathbb{C}[x,y]$. By substitution,

$$\begin{aligned} p(\alpha,\beta) &= (hf+kg)(\alpha,\beta) \\ &= h(\alpha,\beta)\cdot f(\alpha,\beta) + k(\alpha,\beta)\cdot g(\alpha,\beta) \\ &= h(\alpha,\beta)\cdot 0 + k(\alpha,\beta)\cdot 0 \\ &= 0; \end{aligned}$$

that is, (α,β) is a root of p.

Figure 8.1 depicts the root $(\alpha,\beta) = \left(\sqrt{2+\sqrt{3}}, 2\sqrt{2+\sqrt{3}} - \sqrt{6+3\sqrt{3}}\right)$. It is also a root of every element of A.

You will show in Exercise 8.25 that the ideal of Example 8.8 can be generalized to other rings and larger numbers of variables.

Remark 8.9: Recall from linear algebra that *vector spaces* are an important tool for the study of systems of linear equations: finding a *triangular basis* of the vector space spanned by a system of linear polynomials allows us to analyze the solutions of the system. Example 8.8 illustrates why ideals are an important tool for the study of non-linear polynomial equations. If one can compute a "triangular basis" of a polynomial ideal, then one can analyze the solutions of the system that generates the ideal in a method very similar to methods for linear systems. We take up this task in Chapter 10.

Since ideals are fundamental, we would like an analogue of the Subring Theorem to decide whether a subset of a ring is an ideal.

Theorem 8.10 (The Ideal Theorem): *Let R be a ring and $A \subset R$. The following are equivalent:*

(A) *A is an ideal subring of R.*

(B) *A is closed under subtraction and absorption. That is,*

(I1) *for all $a, b \in A$, $a - b \in A$; and*

(I2) *for all $a \in A$ and $r \in R$, we have $ar, ra \in A$.*

PROOF: You do it! See Exercise 8.20. □

We conclude by defining a special kind of ideal, with a notation similar to that of cyclic subgroups, but with a different meaning.

Notation 8.11: Let R be a ring with unity and $r_1, r_2, \ldots, r_m \in R$. Define the set $\langle r_1, r_2, \ldots, r_m \rangle$ as the intersection of all the ideals of R that contain all of $r_1, r_2, \ldots, r_m$.

Proposition 8.12: *Let R be a ring with unity. For all $r_1, \ldots, r_m \in R$, $\langle r_1, \ldots, r_m \rangle$ is an ideal.*

PROOF: Let $a, b \in \langle r_1, \ldots, r_m \rangle$. Let I be any ideal that contains all of $r_1, \ldots, r_m$. By definition of $\langle r_1, \ldots, r_m \rangle$, $a, b \in I$. By the Ideal Theorem, $a - b \in I$ and for all $r \in R$, $ar, ra \in I$. Since I was an arbitrary ideal containing all of $r_1, \ldots, r_m$, *every* such ideal contains $a - b$ and ra. Thus $a - b, ra \in \langle r_1, \ldots, r_m \rangle$. By the Ideal Theorem, $\langle r_1, \ldots, r_m \rangle$ is an ideal. □

Definition 8.13: In a ring with unity, we call $\langle r_1, r_2, \ldots, r_m \rangle$ the **ideal generated by** $r_1, r_2, \ldots, r_m$, and $\{r_1, r_2, \ldots, r_m\}$ a **basis** of $\langle r_1, r_2, \ldots, r_m \rangle$.

Proposition 8.14: *The ideal $\langle r_1, r_2, \ldots, r_m \rangle$ is precisely the set*

$$I = \{h_1 r_1 + h_2 r_2 + \cdots + h_m r_m : h_i \in R\}.$$

PROOF: First, we show that $I \subseteq \langle r_1, \ldots, r_m \rangle$. Let $p \in I$; by definition, there exist $h_1, \ldots, h_m \in R$ such that $p = \sum_{i=1}^{m} h_i r_i$. Let J be any ideal that contains all of $r_1, \ldots, r_m$. By definition, $r_i \in J$ for each i. By absorption, $h_i r_i \in J$ for each i. By closure, $p = \sum_{i=1}^{m} h_i r_i \in J$. Since J was an

arbitrary ideal containing all of $r_1,\ldots,r_m$, we infer that all the ideals containing all of $r_1,\ldots,r_m$ contain p. Since p is an arbitrary element of I, I is a subset of all the ideals containing all of $r_1,\ldots,r_m$. By definition, $I \subseteq \langle r_1,\ldots,r_m\rangle$.

To complete the proof, we must show that $I \supseteq \langle r_1,\ldots,r_m\rangle$. To that end, we claim first that I is an ideal. Absorption is obvious; as for the closure of subtraction, let $x,y \in I$; then choose $h_i, p_i \in R$ such that

$$\begin{aligned} x &= h_1 r_1 + \cdots + h_m r_m \text{ and} \\ y &= p_1 r_1 + \cdots + p_m r_m. \end{aligned}$$

Using the associative property, the commutative property of addition, the commutative property of multiplication, distribution, and the closure of subtraction in R, we see that

$$\begin{aligned} x - y &= (f_1 r_1 + \cdots + f_m r_m) - (p_1 r_1 + \cdots + p_m r_m) \\ &= (f_1 r_1 - p_1 r_1) + \cdots + (f_m r_m - p_m r_m) \\ &= (f_1 - p_1)\, r_1 + \cdots + (f_m - p_m)\, r_m. \end{aligned}$$

Hence $x - y \in I$, and by the Ideal Theorem, I is an ideal. Moreover, it is easy to see that $r_i \in I$ for each $i = 1,2,\ldots,m$ since

$$r_i = 1 \cdot r_i + \sum_{j \neq i} 0 \cdot r_j \in I.$$

Hence I is an ideal containing all of $r_1, r_2, \ldots, r_m$. By definition of $\langle r_1,\ldots,r_m\rangle$, $I \supseteq \langle r_1,\ldots,r_m\rangle$.

We have shown that $I \subseteq \langle r_1,\ldots,r_m\rangle \subseteq I$. Hence $I = \langle r_1,\ldots,r_m\rangle$ as claimed. □

We conclude with an example that shows how an ideal can have more than one basis.

Example 8.15: Consider the ring $\mathbb{Z}$, and let $I = \langle 4,6\rangle$. Proposition 8.14 claims that

$$I = \{4m + 6n : \ m,n \in \mathbb{Z}\}.$$

Choosing concrete values of m and n, we see that

$$\begin{aligned} 4 &= 4\cdot 1 + 6\cdot 0 \in I \\ 0 &= 4\cdot 0 + 6\cdot 0 \in I \\ -12 &= 4\cdot(-3) + 6\cdot 0 \in I \\ -12 &= 4\cdot 0 + 6\cdot(-2) \in I. \end{aligned}$$

Notice that for some elements of I, we can provide representations in terms of 4 and 6 in more than one way.

While we're at it, we claim that we can simplify I as $I = 2\mathbb{Z}$. Why? For starters, $2 = 4\cdot(-1) + 6\cdot 1$, so $2 \in I$. Now that we have $2 \in I$, let $x \in 2\mathbb{Z}$; then $x = 2q$ for some $q \in \mathbb{Z}$. Then

$$x = 2q = [4\cdot(-1) + 6\cdot 1]\cdot q = 4\cdot(-q) + 6\cdot q \in I.$$

Since x was arbitrary, $I \supseteq 2\mathbb{Z}$. On the other hand, let $x \in I$; there exist $m, n \in \mathbb{Z}$ such that

$$x = 4m + 6n = 2(2m + 3n) \in 2\mathbb{Z}.$$

Since x was arbitrary, $I \subseteq 2\mathbb{Z}$. Hence $I = 2\mathbb{Z}$.

So $I = \langle 4, 6\rangle = \langle 2\rangle = 2\mathbb{Z}$. If we think of $r_1, \ldots, r_m$ as a "basis" for $\langle r_1, \ldots, r_m\rangle$, then the example above shows that any given ideal can have bases of different sizes.

You might wonder if every ideal can be written as $\langle a\rangle$. As you will see in Section 8.2, the answer is, "Not always." However, the statement is true for the ring $\mathbb{Z}$ (and a number of other rings as well). You will explore this in Exercise 8.19, and Section 8.2.

Exercises.

Exercise 8.16: Show that for any $n \in \mathbb{N}$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Exercise 8.17: Show that every ideal of $\mathbb{Z}$ has the form $n\mathbb{Z}$, for some $n \in \mathbb{N}$.

Exercise 8.18:

(a) Prove Lemma 8.6.

(b) Explain why part (a) asked you to show that, in $\mathbb{Z}$, $a \mid b$ if and only if $\langle b\rangle \subseteq \langle a\rangle$.

(c) More generally, prove that in *any* ring with unity, $a \mid b$ if and only if $\langle b\rangle \subseteq \langle a\rangle$.

Exercise 8.19: In this exercise, we explore how $\langle r_1, r_2, \ldots, r_m\rangle$ behaves in $\mathbb{Z}$. Keep in mind that the results do not necessarily generalize to other rings.

(a) For the following values of $a, b \in \mathbb{Z}$, show that $\langle a, b\rangle = \langle c\rangle$ for a certain $c \in \mathbb{Z}$.
   (i) $a = 3$, $b = 5$
   (ii) $a = 3$, $b = 6$
   (iii) $a = 4$, $b = 6$

(b) What is the relationship between a, b, and c in part (a)?

(c) Prove the conjecture you formed in part (b).

Exercise 8.20: Prove Theorem 8.10 (the Ideal Theorem).

Exercise 8.21: Suppose R is a ring with unity, and A an ideal. Show that if $1_R \in A$, then $A = R$.

Exercise 8.22: Show that in any field $\mathbb{F}$, the only two distinct ideals are the zero ideal and $\mathbb{F}$ itself.

Exercise 8.23: Let R be a ring and A and I two ideals of R. Decide whether the following subsets of R are also ideals, and explain your reasoning:

(a) $A \cap I$

(b) $A \cup I$

(c) $A + I = \{x + y : x \in A, y \in I\}$

(d) $A \cdot I = \{xy : x \in A, y \in I\}$

(e) $AI = \left\{\sum_{i=1}^{n} x_i y_i : n \in \mathbb{N}, x_i \in A, y_i \in I\right\}$

Exercise 8.24: Let A, B be two ideals of a ring R. Observe the definition of AB in Exercise 8.23

(a) Show that $AB \subseteq A \cap B$.

(b) Show that sometimes $AB \neq A \cap B$; that is, find a ring R and ideals A, B such that $AB \neq A \cap B$.

Exercise 8.25: Let R be a ring with unity. Recall the polynomial ring $R[x_1, x_2, \ldots, x_n]$, whose ground ring is R (Section 7.3). Let

$$\langle f_1, f_2, \ldots, f_m \rangle = \{h_1 f_1 + h_2 f_2 + \cdots + h_m f_m : h_1, h_2, \ldots, h_m \in R[x_1, x_2, \ldots, x_n]\}.$$

Example 8.8 showed that the set $A = \langle x^2 + y^2 - 4, xy - 1 \rangle$ was an ideal; Proposition 8.14 generalizes this to show that $\langle f_1, f_2, \ldots, f_m \rangle$ is an ideal of $R[x_1, x_2, \ldots, x_n]$. Show that the common roots of $f_1, f_2, \ldots, f_m$ are common roots of all polynomials in the ideal I.

Exercise 8.26: Let A be an ideal of a ring R. Define its **radical** to be

$$\sqrt{A} = \{r \in R : r^n \in A \; \exists r \in \mathbb{N}^+\}.$$

Show that $\sqrt{A}$ is an ideal.

8.2: Principal Ideal Domains and the Ascending Chain Condition

In the previous section, we described ideals for commutative rings with identity that are generated by a finite set of elements, denoting them by $\langle r_1, \ldots, r_m \rangle$. An important subclass of these ideals consists of ideals generated by only one element.

Definition 8.27: Let A be an ideal of a ring R. If $A = \langle a \rangle$ for some $a \in R$, then A is a **principal ideal**.

Many ideals can be rewritten as principal ideals. For example, the zero ideal $\{0\} = \langle 0 \rangle$. If R has unity, we can write $R = \langle 1 \rangle$. On the other hand, not all ideals are principal. For example, if $A = \langle x, y \rangle$ in the ring $\mathbb{C}[x, y]$, there is no $f \in \mathbb{C}[x, y]$ such that $A = \langle f \rangle$.

The following property of principal ideals is extremely useful.

Lemma 8.28: *Let $a, b \in R$. There exists $q \in R$ such that $qa = b$ if and only if $\langle b \rangle \subseteq \langle a \rangle$. In addition, if R is an integral domain, q has a multiplicative inverse if and only if $\langle b \rangle = \langle a \rangle$.*

PROOF: The first assertion is precisely Exercise 8.18(b). For the second, assume that R is an integral domain and that $qa = b$. The first assertion gives us $\langle b \rangle \subseteq \langle a \rangle$. By definition, q has a multiplicative inverse r iff $rq = 1_R$. By substitution, $rb = r(qa) = a$. By absorption, $a \in \langle b \rangle$. Hence $\langle b \rangle \supseteq \langle a \rangle$. Since we already had $\langle b \rangle \subseteq \langle a \rangle$, we conclude that $\langle b \rangle = \langle a \rangle$. □

Outside an integral domain, a could divide b with an element that has no multiplicative inverse, yet $\langle b \rangle = \langle a \rangle$. For example, in $\mathbb{Z}_6$, we have $[2] \cdot [2] = [4]$, but $\langle [2] \rangle = \{[0], [2], [4]\} = \langle [4] \rangle$.

There are rings in which all ideals are principal.

Definition 8.29: A **principal ideal domain** is a ring where every ideal can be written as a principal ideal.

Example 8.30: We claim that $\mathbb{Z}$ is a principal ideal domain, and we can prove this using a careful application of Exercise 8.19. Let A be any ideal of $\mathbb{Z}$. The zero ideal is $\langle 0 \rangle$, so assume that $A \neq \{0\}$. That is, contains at least one non-zero element; call it a_1. Without loss of generality, we may assume that $a_1 \in \mathbb{N}^+$ (if not, we could take $-a_1$ instead, since the definition of an ideal requires $-a_1 \in A$ as well).

Is $A = \langle a_1 \rangle$? If not, we can choose $b_1 \in A \setminus \langle a_1 \rangle$. Let $q_1, r_1 \in \mathbb{Z}$ be the quotient and remainder from division of b_1 by a_1; notice that $r_1 = b_1 - q_1 a_1 \in A$. Let $a_2 = \gcd(a_1, r_1)$. By the Extended Euclidean Algorithm, we can find $x, y \in \mathbb{Z}$ such that $xa_1 + yr_1 = a_2$, and since $a_1, r_1 \in A$, absorption and closure give us $a_2 \in A$. Notice $0 < a_2 \leq r_1 < a_1$.

Is $A = \langle a_1, a_2 \rangle$? If not, we can repeat the procedure to find $b_2 \in A \setminus \langle a_1, a_2 \rangle$, $r_2 \in A$ the remainder of division of b_2 by a_2, and $a_3 = \gcd(a_2, r_2)$, so that $0 < a_3 < a_2$. Indeed, as long as $A \neq \langle a_1, a_2, \ldots, a_i \rangle$, we can find $b_i \in A \setminus \langle a_1, \ldots, a_i \rangle$, $r_i \in A$ the remainder of division of b_i by a_i, and $a_{i+1} = \gcd(a_i, r_i)$, with $0 < a_{i+1} < a_i$. This gives us a strictly decreasing chain of integers $a_1 > a_2 > \cdots > a_i > 0$. Let S be the set of all a_i that we can generate in this way; by the well-ordering of $\mathbb{N}$, S must have a least element, d. Since d is the smallest element of S, it must be the last a_i that we computed, implying that we cannot compute anymore. That implies $A = \langle d \rangle$.

Before moving on, let's take a moment to look at how the ideals are related, as well. Let $B_1 = \langle a_1 \rangle$, and $B_2 = \langle a_1, r_1 \rangle$. Exercise 8.19 tells us that, in fact, $B_2 = \langle a_2 \rangle$. Lemma 8.28 implies that $B_1 \subsetneq B_2$. When we choose, $b_3 \in A \setminus \langle a_1, a_2 \rangle$, we are actually choosing $b_3 \in A \setminus \langle a_2 \rangle$. Likewise, if we set $B_3 = \langle a_2, r_2 \rangle = \langle a_3 \rangle$, then $B_2 \subsetneq B_3$. In fact, as long as $A \neq \langle a_i \rangle$, we can generate an ascending sequence of ideals $B_1 \subsetneq B_2 \subsetneq \cdots$. In other words, another way of looking at this proof is that it *tries to expand the principal ideal B_i until $B_i = A$*, basically by adding elements not in B_i. Rather amazingly, the argument above implies that this ascending chain of ideals must stabilize, at least in $\mathbb{Z}$.

This property that an ascending chain of ideals must stabilize is one that some rings satisfy, but not all; we return to it in a moment.

We can extend the argument of Example 8.30 to more general rings.

Theorem 8.31: *Every Euclidean domain is a principal ideal domain.*

PROOF: Let R be a Euclidean domain with respect to v, and let A be any non-zero ideal of R. Let $a_1 \in A$. As long as $A \neq \langle a_i \rangle$, do the following:

- find $b_i \in A \setminus \langle a_i \rangle$;
- let r_i be the remainder of dividing b_i by a_i;
  - notice $v(r_i) < v(a_i)$;
- compute a gcd a_{i+1} of a_i and r_i;
  - notice $v(a_{i+1}) \leq v(r_i) < v(a_i)$;
- this means $\langle a_i \rangle \subsetneq \langle a_{i+1} \rangle$; after all,

- as a gcd, $a_{i+1} \mid a_i$, but
- $a_i \nmid a_{i+1}$, lest $a_i \mid a_{i+1}$ imply $v(a_i) \leq v(a_{i+1}) < v(a_i)$

- hence, $\langle a_i \rangle \subsetneq \langle a_{i+1} \rangle$ and $v(a_{i+1}) < v(a_i)$.

Let T be the set of all the a_i that we can generate in this way, and let $S = \{v(t) : t \in T\}$. By the well-ordering of $\mathbb{N}$, S must have a least element, d. By definition, there exists $t \in T$ such that $d = v(t)$, and $t = a_i$ for some i. Since $d = v(a_i)$, d is minimal, and computing an a_{i+1} using the procedure above would give us $v(a_{i+1}) < v(a_i)$, it must not be possible to compute any more a_i. If $A \neq \langle a_i \rangle$, however, we could certainly compute another one. Thus, $A = \langle a_i \rangle$. □

Not all integral domains are principal ideal domains; you will show in the exercises that for any field $\mathbb{F}$ and its polynomial ring $\mathbb{F}[x,y]$, the ideal $\langle x, y \rangle$ is not principal. For now, though, we will turn to a phenomenon that appeared in Example 8.30 and Theorem 8.31. In each case, we built a chain of ideals

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \cdots$$

and were able to show that the procedure we used to find the a_i must eventually terminate.

As we mentioned above, this property is very useful for a ring. In both Example 8.30 and Theorem 8.31, we relied on the well-ordering of $\mathbb{N}$, but that is not always available to us. So the property might be useful in other settings, even in cases where ideals aren't guaranteed to be principal. For example, eventually we will show that $\mathbb{F}[x,y]$ satisfies this property.

Definition 8.32: Let R be a ring. If for every **ascending chain of ideals** $A_1 \subseteq A_2 \subseteq \cdots$ we can find an integer k such that $A_k = A_{k+1} = \cdots$, then R satisfies the **Ascending Chain Condition**.

Remark 8.33: Another name for a ring that satisfies the Ascending Chain Condition is a **Noetherian ring**, after Emmy Noether.

Theorem 8.34: *Each of the following holds.*

(A) *Every principal ideal domain satisfies the Ascending Chain Condition.*

(B) *Any field $\mathbb{F}$ satisfies the Ascending Chain Condition.*

(C) *If a ring R satisfies the Ascending Chain Condition, so does $R[x]$.*

(D) *If a ring R satisfies the Ascending Chain Condition, so does $R[x_1, x_2, \ldots, x_n]$.*

PROOF: (A) Let R be a principal ideal domain, and let $A_1 \subseteq A_2 \subseteq \cdots$ be an ascending chain of ideals in R. Let $B = \bigcup_{i=1}^{\infty} A_i$. By Exercise 8.39, B is an ideal. Since R is a principal ideal domain, $B = \langle b \rangle$ for some $b \in R$. By definition of a union, $b \in A_i$ for some $i \in \mathbb{N}$. The definition of an ideal now implies that $rb \in A_i$ for all $r \in R$; so $\langle b \rangle \subseteq A_i$. By substitution, $B \subseteq A_i$. By definition of B, we also have $A_i \subseteq B$. Hence $A_i = B$, and a similar argument shows that $A_j = B$ for all $j \geq i$. Hence the chain of ideals stabilizes at A_i. Since the chain was arbitrary, every ascending chain of ideals in R stabilizes, so R satisfies the ascending chain condition.

(B) By Exercise 7.49, any field $\mathbb{F}$ is a Euclidean domain, so this follows from (A) and Theorem 8.31. However, it's instructive to look at it from the point of view of a field as well.

Recall from Exercise 8.22 that a field has only two distinct ideals: the zero ideal, and the field itself. Hence, any ascending chain of ideals stabilizes either at the zero ideal or at $\mathbb{F}$ itself.

(C) Assume that R satisfies the Ascending Chain Condition. If every ideal of $R[x]$ is finitely generated, then we are done, since for any ascending chain $I_1 \subseteq I_2 \subseteq \cdots$ the set $I = \cup_{i=1}^{\infty} I_i$ is also an ideal (Exercise 8.39), and is finitely generated, say $I = \langle f_1, \ldots, f_m \rangle$, which implies that the chain stabilizes at I_j where $f_1, \ldots, f_m \in I_j$.

So if we show that every ideal of $R[x]$ is finitely generated, then we are done. Let I be any ideal of $R[x]$, and choose $f_1, f_2, \ldots \in I$ in the following way:

- Let $J_0 = \{0\}$, and $k = 0$.
- While $I \neq \langle J_k \rangle$:
  - Let $S_k = \{\deg f : f \in I \setminus \langle J_k \rangle\}$. Since $S_k \subseteq \mathbb{N}$, it has a least element; call it d_k.
  - Let $f_k \in I \setminus J_k$ be any polynomial of degree d_k. Notice that $f_k \in I \setminus J_k$ implies that $J_k \subsetneq \langle J_k \cup \{f_k\} \rangle$.
  - Let $J_{k+1} = J_k \cup \{f_k\}$, and increment k by 1.

Does this process terminate? By construction, $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \cdots$ is an ascending chain of ideals. Denote the leading coefficient of f_i by a_i and let $K_i = \langle a_1, a_2, \ldots, a_i \rangle$. Since R satisfies the Ascending Chain Condition, the ascending chain of ideals $K_1 \subseteq K_2 \subseteq \cdots$ stabilizes for some $m \in \mathbb{N}$.

By way of contradiction, suppose we can find f_{m+1} of minimal degree in $I \setminus \langle f_1, \ldots, f_m \rangle$. Since $K_m = K_{m+1}$ of necessity, $a_{m+1} = b_1 a_1 + \cdots + b_m a_m$ for some $b_1, \ldots, b_m \in \mathbb{F}$. Write $d_i = \deg_x f_i$, and consider

$$p = b_1 f_1 x^{d_{m+1} - d_1} + \cdots + b_m f_m x^{d_{m+1} - d_m}.$$

Choosing the f_i's to be of minimal degree implies that for each i, $d_i \leq d_{m+1}$, so $d_{m+1} - d_i \in \mathbb{N}$. Moreover, we have set up the sum and products so that the leading term of p is

$$(b_1 a_1 + \cdots + b_m a_m) x^{d_{m+1}} = a_{m+1} x^{d_{m+1}}.$$

Let $g = f_{m+1} - p$. Since $\mathrm{lt}(f_{m+1}) = \mathrm{lt}(p)$ and $\mathrm{lc}(f_{m+1}) = \mathrm{lc}(p)$, their leading terms cancel in the subtraction. Thus, $\deg g < \deg f_{m+1}$. By construction, $p \in \langle f_1, f_2, \ldots, f_m \rangle$. If $f_{m+1} \notin \langle f_1, f_2, \ldots, f_m \rangle$, then $g \notin \langle f_1, f_2, \ldots, f_m \rangle$; otherwise, $f = g + p \in \langle f_1, f_2, \ldots, f_m \rangle$. That means $g \in I \setminus \langle f_1, f_2, \ldots, f_m \rangle$. This contradicts the choice of f_{m+1}, which was supposed to have minimal degree in $I \setminus \langle f_1, \ldots, f_m \rangle$.

Thus, the process must terminate. Since it does not terminate unless $I = \langle J_k \rangle$, we conclude that eventually $I = \langle J_k \rangle = \langle f_1, \ldots, f_k \rangle$. In other words, I is finitely generated. As explained above, this implies that $R[x]$ satisfies the ascending chain condition.

(D) follows from (C) by induction on the number of variables n: use R to show $R[x_1]$ satisfies the Ascending Chain Condition; use $R[x_1]$ to show that $R[x_1, x_2] = (R[x_1])[x_2]$ satisfies the Ascending Chain Condition; etc. □

Corollary 8.35 (Hilbert Basis Theorem): *For any field* $\mathbb{F}$, $\mathbb{F}[x_1, x_2, \ldots, x_n]$ *satisfies the Ascending Chain Condition. Thus, for any ideal* I *of* $\mathbb{F}[x_1, \ldots, x_n]$, *we can find* $f_1, \ldots, f_m \in I$ *such that* $I = \langle f_1, \ldots, f_m \rangle$.

PROOF: Apply (B) and (D) of Theorem 8.34. □

Exercises

Exercise 8.36: Let q be an element of a ring with unity. Show that q has a multiplicative inverse if and only if $\langle q \rangle = \langle 1 \rangle$.

Exercise 8.37: Is $\mathbb{F}[x]$ a principal ideal domain for every field $\mathbb{F}$? What about $R[x]$ for every ring R?

Exercise 8.38: Let $\mathbb{F}$ be any field, and consider the polynomial ring $\mathbb{F}[x, y]$. Explain why $\langle x, y \rangle$ cannot be principal.

Exercise 8.39: Let R be a ring and $I_1 \subseteq I_2 \subseteq \cdots$ an ascending chain of ideals. Show that $\mathcal{I} = \bigcup_{i=1}^{\infty} I_i$ is itself an ideal.

8.3: Prime and maximal ideals

Two important classes of ideals are *prime* and *maximal* ideals. Let R be a ring.

Definition 8.40: A proper ideal A of R is a **maximal ideal** if no other proper ideal of R contains A.

Another way of expressing that A is maximal is the following: for any other ideal I of R, $A \subseteq I$ implies that $A = I$ or $I = R$.

Example 8.41: In Exercise 8.17 you showed that all ideals of $\mathbb{Z}$ have the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Are any of these (or all of them) maximal ideals?

Let $n \in \mathbb{Z}$ and suppose that $n\mathbb{Z}$ is maximal. Certainly $n \neq 0$, since $2\mathbb{Z} \nsubseteq \{0\}$. We claim that n is irreducible; that is, n is divisible only by $\pm 1, \pm n$. To see this, recall Lemma 8.6: $m \in \mathbb{Z}$ is a divisor of n iff $n\mathbb{Z} \subseteq m\mathbb{Z}$. Since $n\mathbb{Z}$ is maximal, either $m\mathbb{Z} = \mathbb{Z}$ or $m\mathbb{Z} = n\mathbb{Z}$. In the first case, $m = \pm 1$; in the second case, $m = \pm n$. Hence n is irreducible.

For prime ideals, you need to recall from Exercise 8.23 that for any two ideals A, B of R, AB is also an ideal.

Definition 8.42: A proper ideal P of R is a **prime ideal** if for every two ideals A, B of R we know that

$$\text{if } AB \subseteq P \text{ then } A \subseteq P \text{ or } B \subseteq P.$$

Definition 8.42 might remind you of our definition of prime integers from page 6.29. Indeed, the two are connected.

Example 8.43: Let $n \in \mathbb{Z}$ be a prime integer. Let $a, b \in \mathbb{Z}$ such that $p \mid ab$. Hence $p \mid a$ or $p \mid b$. Suppose that $p \mid a$.

Let's turn our attention to the corresponding ideals. Since $p \mid ab$, Lemma 8.6 tells us that $(ab)\mathbb{Z} \subseteq p\mathbb{Z}$. It is routine to show that $(ab)\mathbb{Z} = (a\mathbb{Z})(b\mathbb{Z})$. Put $A = a\mathbb{Z}$, $B = b\mathbb{Z}$, and $P = p\mathbb{Z}$; thus $AB \subseteq P$.

Recall that $p \mid a$; applying Lemma 8.6 again, we have $A = a\mathbb{Z} \subseteq p\mathbb{Z} = P$.

Conversely, if n is not prime, $n\mathbb{Z}$ is not a prime ideal: for example, $6\mathbb{Z}$ is not a prime ideal because $(2\mathbb{Z})(3\mathbb{Z}) \subseteq 6\mathbb{Z}$ but by Lemma 8.18 neither $2\mathbb{Z} \subseteq 6\mathbb{Z}$ nor $3\mathbb{Z} \subseteq 6\mathbb{Z}$. This can be generalized easily to all integers that are not prime: see Exercise 8.47.

You might wonder if the relationship found in Example 8.41 works the other way. That is: we found in Example 8.41 that an ideal in $\mathbb{Z}$ is maximal iff it is generated by a prime integer, and in Example 8.43 we argued that an ideal is prime iff it is generated by a prime integer. We can see that in the integers, at least, an ideal is maximal if and only if it is prime.

What about other rings?

Theorem 8.44: *If R is a ring with unity, then every maximal ideal is prime.*

PROOF: Let M be a maximal ideal of R. Let A, B be any two ideals of R such that $AB \subseteq M$. We claim that $A \subseteq M$ or $B \subseteq M$.

Assume that $A \nsubseteq M$; we claim that $B \subseteq M$. Recall from Exercise 8.23 that $A + M$ is also an ideal. Since M is maximal, $A + M = M$ or $A + M = R$. Since $A \nsubseteq M$, $A + M \neq M$; thus $A + M = R$. Since R has unity, $1_R \in A + M$, so there exist $a \in A$, $m \in M$ such that

$$1_R = a + m. \tag{20}$$

Let $b \in B$ and multiply both sides of (20) on the right by b; we have

$$\begin{aligned} 1_R \cdot b &= (a + m)\, b \\ b &= ab + mb. \end{aligned}$$

Recall that $AB \subseteq M$; since $ab \in AB$, $ab \in M$. Likewise, since M is an ideal, $mb \in M$. Ideals are subrings, hence closed under addition, so $ab + mb \in M$. Substitution implies that $b \in M$. Since b was arbitrary in B, $B \subseteq M$.

We assumed that $AB \subseteq M$, and found that $A \subseteq M$ or $B \subseteq M$. Thus, M is prime. □

Theorem 8.45: *If R is a ring without unity, then maximal ideals might not be prime.*

PROOF: The proof is by counterexample: Clearly $2\mathbb{Z}$ is a ring without unity. (If this isn't clear, reread the previous section.) We claim that $4\mathbb{Z}$ is an ideal of $R = 2\mathbb{Z}$:

subring: Let $x, y \in 4\mathbb{Z}$. By definition of $4\mathbb{Z}$, $x = 4a$ and $y = 4b$ for some $a, b \in \mathbb{Z}$. Using the distributive property and substitution, we have $x - y = 4a - 4b = 4(a-b) \in 4\mathbb{Z}$.

absorption: Let $x \in 4\mathbb{Z}$ and $r \in 2\mathbb{Z}$. By definition of $4\mathbb{Z}$, $x = 4q$ for some $q \in \mathbb{Z}$. By subtitution, the associative property, and the commutative property of integer multiplication, $rx = 4(rq) \in 4\mathbb{Z}$.

Having shown that $4\mathbb{Z}$ is an ideal, we now show that it is a maximal ideal. Let A be any ideal of $2\mathbb{Z}$ such that $4\mathbb{Z} \subsetneq A$. Let $x \in A \backslash 4\mathbb{Z}$; by the Division Theorem, $x = 4q + r$ such that $0 < r < 4$. Since $x \in 2\mathbb{Z}$, we can write $x = 2d$ for some $d \in \mathbb{Z}$. Thus $r = x - 4q = 2(d - 2q) \in 2\mathbb{Z}$. But $0 < r < 4$ and $r \in 2\mathbb{Z}$ implies that $r = 2$.

Now $4q \in 4\mathbb{Z}$ and thus in A, so $x - 4q \in A$. By substitution, $x - 4q = (4q+2) - 4q = 2$; since A is an ideal, $2 \in A$. By absorption, $2n \in A$ for all $n \in \mathbb{Z}$. Thus $2\mathbb{Z} \subseteq A$. But A is an ideal of $2\mathbb{Z}$, so $2\mathbb{Z} \subseteq A \subseteq 2\mathbb{Z}$, which implies that $A = 2\mathbb{Z}$. Since A is an arbitrary ideal of $2\mathbb{Z}$ that contains $4\mathbb{Z}$ properly, $4\mathbb{Z}$ is maximal in $2\mathbb{Z}$.

Finally, we show that $4\mathbb{Z}$ is not prime. This is easy: $(2\mathbb{Z})(2\mathbb{Z}) \subseteq 4\mathbb{Z}$, but $2\mathbb{Z} \nsubseteq 4\mathbb{Z}$. □

Theorem 8.46: *A prime ideal is not necessarily maximal, even in a ring with unity.*

PROOF: Recall that $R = \mathbb{C}[x, y]$ is a ring with unity, and that $I = \langle x \rangle$ is an ideal of R.

We claim that I is a prime ideal of R. Let A, B be ideals of R such that $AB \subseteq I$. Suppose that $A \nsubseteq I$; let $a \in A \backslash I$. For any $b \in B$, $ab \in AB \subseteq I = \langle x \rangle$, so $ab \in \langle x \rangle$. This implies that $x \mid ab$; let $q \in R$ such that $qx = ab$. Write $a = f \cdot x + a'$ and $b = g \cdot x + b'$ where $a', b' \in R \backslash I$; that is, a' and b' are polynomials with *no* terms that are multiples of x. By substitution,

$$\begin{aligned} ab &= (f \cdot x + a')(g \cdot x + b') \\ qx &= (f \cdot x) \cdot (g \cdot x) + a' \cdot (g \cdot x) + b' \cdot (f \cdot x) + a' \cdot b' \\ (q - fg - a'g - b'f)\, x &= a'b'. \end{aligned}$$

Hence $a'b' \in \langle x \rangle$. However, no term of a' or b' is a multiple of x, so no term of $a'b'$ is a multiple of x. The only element of $\langle x \rangle$ that satisfies this property is 0. Hence $a'b' = 0$, which by the zero product property of complex numbers implies that $a' = 0$ or $b' = 0$.

Which is it? If $a' = 0$, then $a = f \cdot x + 0 \in \langle x \rangle = I$, which contradicts the assumption that $a \in A \backslash I$. Hence $a' \neq 0$, implying that $b' = 0$, so $b = gx + 0 \in \langle x \rangle = I$. Since b is arbitrary, this holds for all $b \in B$; that is, $B \subseteq I$.

We took two arbitrary ideals such that $AB \subseteq I$ and showed that $A \subseteq I$ or $B \subseteq I$; hence $I = \langle x \rangle$ is prime. However, I is not maximal, since

- $y \notin \langle x \rangle$, implying that $\langle x \rangle \subsetneq \langle x, y \rangle$; and
- $1 \notin \langle x, y \rangle$, implying that $\langle x, y \rangle \nsubseteq \mathbb{C}[x, y]$.

□

So prime and maximal ideals need not be equivalent. In Chapter 9, we will find conditions on a ring that ensure that prime and maximal ideals are equivalent.

Chapter Exercises.

Exercise 8.47: Let $n \in \mathbb{Z}$ be an integer that is not prime. Show that $n\mathbb{Z}$ is not a prime ideal.

Exercise 8.48: Show that $\{[0],[4]\}$ is a proper ideal of $\mathbb{Z}_8$, but that it is not maximal. Then find a maximal ideal of $\mathbb{Z}_8$.

Exercise 8.49: Find all the maximal ideals of $\mathbb{Z}_{12}$. Are they prime? How do you know?

Exercise 8.50: Let $\mathbb{F}$ be a field, and $a_1, a_2 \ldots, a_n \in \mathbb{F}$.

(a) Show that the ideal $\langle x_1 - a_1, x_2 - a_1, \ldots, x_n - a_n \rangle$ is both a prime ideal and a maximal ideal of $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

(b) Use Exercise 8.25 to describe the common root(s) of this ideal.

8.4: Quotient Rings

We now generalize the notion of *quotient groups* to rings, and prove some interesting properties of certain quotient groups that help explain various phenomena we observed in both group theory and ring theory.

Theorem 8.51: *Let R be a ring and A an ideal of R. For every $r \in R$, denote*

$$r + A := \{r + a : a \in A\},$$

called a ***class****. Then define*

$$R/A := \{r + A : r \in R\}$$

and define addition and multiplication for this set in the "natural" way: for all $X, Y \in R/A$ denoted as $x + A, y + A$ for some $x, y \in R$,

$$X + Y = (x + y) + A$$
$$XY = (xy) + A.$$

The set R/A is a ring under these operations, called the ***quotient ring****.*

Notation 8.52: When we consider elements of $X \in R/A$, we will refer to the "usual representation" of X as $x + A$ for appropriate $x \in R$; that is, "big" X is represented by "little" x.

In most cases, there are many representations of any class in R/A. As with quotient groups, we have to show that the operations are themselves well-defined. Thus the structure of the proof of Theorem 8.51 considers:

- whether the operations are well-defined;
- whether R/A is an additive group; and
- whether R/A is a ring.

You may remember that when working in quotient rings we made heavy use of Lemma 3.29 on page 62; before proving Theorem 8.51 we need a similar property for the classes $x+A$ of R/A.

Lemma 8.53: *Let $X, Y \in R/A$ with representations $X = x+A$ and $Y = y+A$ for appropriate $x, y \in R$. Then (A) and (B) hold where*
(A) *$X = Y$ if and only if $x-y \in A$.*
(B) *$X = A$ if and only if $x \in A$.*

PROOF: You do it! See Exercise 8.59. □

We now turn to the proof of Theorem 8.51.

PROOF OF THEOREM 8.51: First we show that the operations are well-defined. Let $X, Y \in R/A$ and consider two representations $w+A$ and $x+A$ of X (so $x+A = w+A = X$) and two representations $y+A$ and $z+A$ of Y, for appropriate $w, x, y, z \in R$.

Is addition well-defined? Observe that $X+Y = (x+y)+A$ and $X+Y = (w+z)+A$. By the hypothesis that $x+A = w+A$ and $y+A = z+A$, Lemma 8.53 implies that $x-w \in A$ and $y-z \in A$. By closure, $(x-w)+(y-z) \in A$. Using the properties of a ring,

$$(x+y)-(w+z) = (x-w)+(y-z) \in A.$$

Again from Lemma 8.53 $(x+y)+A = (w+z)+A$, and by definition

$$(x+A)+(y+A) = (x+y)+A = (w+z)+A = (w+A)+(z+A).$$

It does not matter, therefore, what representation we use for X; the sum $X+Y$ has the same value, so addition in R/A is well-defined.

Is multiplication well-defined? Observe that $XY = (x+A)(y+A) = xy+A$. As explained above, $x-w \in A$ and $y-z \in A$. Let $a, \widehat{a} \in A$ such that $x-w = a$ and $y-z = \widehat{a}$; from the absorption property of an ideal, $ay \in A$, so

$$xy-wz = (xy-xz)+(xz-wz) = x(y-z)+(x-w)z = x\widehat{a}+az \in A.$$

Again from Lemma 8.53, $xy+A = wz+A$, and by definition

$$(x+A)(y+A) = xy+A = wz+A = (w+A)(z+A).$$

It does not matter, therefore, what representation we use for X; the product XY has the same value, so multiplication in R/A is well-defined.

Having shown that addition and multiplication in R/A is well-defined, we turn to showing that R/A is a ring. First we show the properties of an additive group:

closure: Let $X, Y \in R/A$, with the usual representation. By substitution, $X+Y = (x+y)+A$. Since R, a ring, is closed under addition, $x+y \in R$. Thus $X+Y \in R/A$.

associative: Let $X, Y, Z \in R/A$, with the usual representation. Applying substitution and the associative property of R, we have

$$\begin{aligned}(X+Y)+Z &= ((x+y)+A)+(z+A)\\ &= ((x+y)+z)+A\\ &= (x+(y+z))+A\\ &= (x+A)+((y+z)+A)\\ &= X+(Y+Z).\end{aligned}$$

identity: We claim that $A = 0+A$ is itself the identity of R/A; that is, $A = 0_{R/A}$. Let $X \in R/A$ with the usual representation. Indeed, substitution and the additive identity of R demonstrate this:

$$\begin{aligned}X+A &= (x+A)+(0+A)\\ &= (x+0)+A\\ &= x+A\\ &= X.\end{aligned}$$

inverse: Let $X \in R/A$ with the usual representation. We claim that $-x+A$ is the additive inverse of X. Indeed,

$$\begin{aligned}X+(-x+A) &= (x+(-x))+A\\ &= 0+A\\ &= A\\ &= 0_{R/A}.\end{aligned}$$

Hence $-x+A$ is the additive inverse of X.

Now we show that R/A satisfies the ring properties. Each property falls back on the corresponding property of R.

closure: Let $X, Y \in R/A$ with the usual representation. By definition and closure in R,

$$\begin{aligned}XY &= (x+A)(y+A)\\ &= (xy)+A\\ &\in R/A.\end{aligned}$$

associative: Let $X, Y, Z \in R/A$ with the usual representation. By definition and the associa-

tive property in R,

$$\begin{aligned}(XY)Z &= ((xy)+A)(z+A)\\ &= ((xy)z)+A\\ &= (x(yz))+A\\ &= (x+A)((yz)+A)\\ &= X(YZ).\end{aligned}$$

distributive: Let $X, Y, Z \in R/A$ with the usual representation. By definition and the distributive property in R,

$$\begin{aligned}X(Y+Z) &= (x+A)((y+z)+A)\\ &= (x(y+z))+A\\ &= (xy+xz)+A\\ &= ((xy)+A)+((xz)+A)\\ &= XY+XZ.\end{aligned}$$

Hence R/A is a ring. □

Proposition 8.54: *If R is a ring with unity, then R/A is also a ring with unity. The multiplicative identity of R/A is $1_R + A$.*

PROOF: You do it! See Exercise 8.60. □

In Section 3.5 we showed that one could define a group using the quotient group $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z}$ is a ring and $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ by Exercise 8.16, it follows that $\mathbb{Z}_n$ is also a ring. Of course, you had already argued this in Exercise 7.10.

We can say more. You found in Exercise 7.22 that $\mathbb{Z}_n$ is not, in general, an integral domain, let alone a field. The relationship between maximal ideals and prime ideals that we studied in Section 8.3 helps explain this.

Theorem 8.55: *If R is a ring with unity and M is a maximal ideal of R, then R/M is a field. The converse is also true.*

PROOF: ($\Rightarrow$) Assume that R is a ring with unity and M is a maximal ideal of R. Let $X \in R/M$ and assume that $X \neq M$; that is, X is non-zero. Since $X \neq M$, $X = x + M$ for some $x \notin M$. Since M is a maximal ideal, the ideal $\langle x \rangle + M$ satisfies $M \subsetneq \langle x \rangle + M = R$ (see Exercise 8.23, Definition 8.13, and Proposition 8.14). By Exercise 8.21, $1 \notin M$. Thus $\langle 1 \rangle + M$ also satisfies $\langle 1 \rangle + M = R$. In other words, $\langle x \rangle + M = \langle 1 \rangle + M$. Since $1 = 1 + 0 \in \langle 1 \rangle + M$, we see that $1 \in \langle x \rangle + M$, so there exist $h \in R$, $m \in M$ such that $1 = hx + m$. Thus $1 - hx = m \in M$, and by Lemma 8.53

$$1 + M = hx + M = (h + M)(x + M).$$

This shows that $h+M$ is a multiplicative inverse of $X = x+M$ in R/M. Since X was an arbitrary non-zero element of R/M, every element of R/M has a multiplicative inverse, and R/M is a field.

($\Leftarrow$) For the converse, assume that R/M is a field. Let N be any ideal of R such that $M \subsetneq N \subseteq R$. Let $x \in N \backslash M$; then $x+M \neq M$, and since R/M is a field, $x+M$ has a multiplicative inverse; call it Y with the usual representation. Thus

$$(xy)+M = (x+M)(y+M) = 1+M,$$

which by Lemma 8.53 implies that $xy-1 \in M$. Let $m \in M$ such that $xy-1 = m$; then $1 = xy-m$. Now, $x \in N$ implies by absorption that $xy \in N$, and $m \in M \subsetneq N$ implies by inclusion that $m \in N$. Closure of the subring N implies that $1 \in N$, and Exercise 8.21 implies that $N = R$. Since N was an arbitrary ideal that contained M properly, M is maximal. □

A similar property holds true for prime ideals.

Theorem 8.56: *If R is a ring with unity and P is a prime ideal of R, then R/P is an integral domain. The converse is also true.*

PROOF: ($\Rightarrow$) Assume that R is a ring with unity and P is a prime ideal of R. Let $X, Y \in R/P$ with the usual representation, and assume that $XY = 0_{R/P} = P$. By definition of the operation, $XY = (xy)+P$; by Lemma 8.53 $xy \in P$. We claim that this implies that $x \in P$ or $y \in P$.

Assume to the contrary that $x, y \notin P$. For any $z \in \langle x \rangle \langle y \rangle$, we have $z = \sum_{k=1}^{m} (h_k x)(q_k y)$ for appropriate $h_k, q_k \in R$. Recall that R is commutative and P absorbs multiplication, which means that $z = [\sum (h_k q_k)](xy) \in P$. Since z was arbitrary in $\langle x \rangle \langle y \rangle$, we conclude that $\langle x \rangle \langle y \rangle \subseteq P$. Now P is a prime ideal, so $\langle x \rangle \subseteq P$ or $\langle y \rangle \subseteq P$; without loss of generality, $\langle x \rangle \subseteq P$, so that $x \in \langle x \rangle \subseteq P$.

Since $x \in P$, Lemma 8.53 implies that $x+P = P$. Thus $X = 0_{R/P}$.

We took two arbitrary elements of R/P, and showed that if their product was the zero element of R/P, then one of those elements had to be P, the zero element of R/P. That is, R/P is an integral domain.

($\Leftarrow$) For the converse, assume that R/P is an integral domain. Let A, B be two ideals of R, and assume that $AB \subseteq P$. Assume that $A \nsubseteq P$ and let $a \in A \backslash P$; we have however $ab \in AB \subseteq P$ for all $b \in P$. Thus

$$(a+P)(b+P) = (ab)+P = P \quad \forall b \in B.$$

Since R/P is an integral domain, $b+P = P$ for all $b \in B$; by Lemma 8.53 $b \in P$ for all $b \in B$. Hence $B \subseteq P$. We took two arbitrary ideals of R, and showed that if their product was a subset of P, then one of them had to be a subset of P. Thus P is a prime ideal. □

A corollary gives us an alternate proof of Theorem .8.44.

Corollary 8.57: *In a ring with unity, every maximal ideal is prime, but the converse is not necessarily true.*

PROOF: Let R be a ring with unity, and M a maximal ideal. By Theorem 8.55, R/M is a field. By Theorem 7.20, R/M is an integral domain. By Theorem 8.56, M is prime.

The converse is not necessarily true because not every integral domain is a field. □

Exercises.

Exercise 8.58: Let $R = \mathbb{Z}_5[x]$ and $I = \langle x^2 + 2x + 2 \rangle$.

(a) Explain why $(x^2 + x + 3) + I = (4x + 1) + I$.

(b) Find a factorization of $x^2 + 2x + 2$ in R.

(c) Explain why R/I is, therefore, not a field.

(d) Find two non-zero elements of R/I whose product is the zero element of R/I.

Exercise 8.59: Prove Lemma 8.53.

Exercise 8.60: Prove Proposition 8.54.

Exercise 8.61: Consider the ideal $I = \langle x^2 + 1 \rangle$ in $R = \mathbb{R}[x]$. The purpose of this exercise is to show that I is maximal.

(a) Explain why $x^2 + x + I = x - 1 + I$.

(b) Explain why every $f \in R/I$ has the form $r + I$ for some $r \in R$ such that $\deg r < 2$.

(c) Part (a) implies that every element of R/I can be written in the form $f = (ax + b) + I$ where $a, b \in \mathbb{C}$. Show that if $f + I$ is a nonzero element of R/I, then $a^2 + b^2 \neq 0$.

(d) Let $f + I \in R/I$ be nonzero, and find $g + I \in R/I$ such that $g + I = (f + I)^{-1}$; that is, $(fg) + I = 1_{R/I}$.

(e) Explain why part (c) shows that I is maximal.

(f) Explain why, if $R = \mathbb{C}[x]$, $\langle x^2 + 1 \rangle$ is not even prime, let alone maximal. Show further that this is because the observation in part (b) is false in $\mathbb{C}$.

Exercise 8.62: Let $\mathbb{F}$ be a field, and $f \in \mathbb{F}[x]$ be any polynomial that does not factor in $\mathbb{F}[x]$. Show that $\mathbb{F}[x] / \langle f \rangle$ is a field.

Exercise 8.63: Recall the ideal $I = \langle x^2 + y^2 - 4, xy - 1 \rangle$ of Exercise 8.8. We want to know whether this ideal is maximal. The purpose of this exercise is to show that it is not so easy to accomplish this as it was in Exercise 8.61.

(a) Explain why someone might think naïvely that every $f \in R/I$ has the form $r + I$ where $r \in R$ and $r = bx + p(y)$, for appropriate $b \in \mathbb{C}$ and $p \in \mathbb{C}[y]$; in the same way, someone might think naïvely that every distinct polynomial r of that form represents a distinct element of R/I.

(b) Show that, to the contrary, $1 + I = (y^3 - 4y + x + 1) + I$.

Exercise 8.64: Determine necessary and sufficient conditions on a ring R such that in $R[x, y]$:

(a) the ideal $I = \langle x \rangle$ is prime;

(b) the ideal $I = \langle x, y \rangle$ is maximal.

8.5: Finite Fields I

Most of the fields you have studied in the past have been infinite: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc. Some fields have not been; in Exercise 7.23 on page 169 you found that $\mathbb{Z}_n^*$ is not, in general, a field. You showed in Exercise 7.22 that if n is irreducible, then $\mathbb{Z}_n$ is not only an integral domain, but a field. However, that does not characterize all finite fields. In this section we will explore finite fields; in particular we will construct some finite fields and show that any finite field has p^n elements where $p, n \in \mathbb{N}$ and p is irreducible.[26]

Before we proceed, we will need the following definition.

Definition 8.65: Let R be a ring.

- If there exists $r \in R$ such that $\{nr : n \in \mathbb{N}\}$ is infinite, then R has **characteristic zero**.
- Otherwise, there exists a smallest positive integer c such that $cr = 0_R$ for all nonzero $r \in R$. In this case, R has **characteristic** c.

Example 8.66: The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic zero, since

$$\{n \cdot 1 : n \in \mathbb{N}\} = \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

The ring $\mathbb{Z}_8$ has characteristic 8, since $8 \cdot [1] = [0]$ and no smaller positive integer multiple of $[1]$ is $[0]$. Let p be an irreducible integer. By Exercise 7.23, $\mathbb{Z}_p$ is a field. Its characteristic is p. ◿

Given these examples, you might expect the characteristic of a finite ring to be the number of elements in the ring. This is not always the case.

Example 8.67: Let $R = \mathbb{Z}_2 \times \mathbb{Z}_4 = \{(a, b) : a \in \mathbb{Z}_2, b \in \mathbb{Z}_4\}$, with addition and multiplication defined in the natural way:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac, bd).$$

It is not hard to show that R is a ring; we leave it to Exercise 8.72. It has eight elements,

$$R = \{([0]_2, [0]_4), ([0]_2, [1]_4), ([0]_2, [2]_4), ([0]_2, [3]_4), ([1]_2, [0]_4), ([1]_2, [1]_4), ([1]_2, [2]_4), ([1]_2, [3]_4)\}.$$

However, the characteristic of R is not eight, but four:

- for any $a \in \mathbb{Z}_2$, we know that $2a = [0]_2$, so $4a = 2[0]_2 = [0]_2$; and
- for any $b \in \mathbb{Z}_4$, we know that $4b = [0]_4$; thus
- for any $(a, b) \in R$, we see that $4(a, b) = (4a, 4b) = ([0]_2, [0]_4) = 0_R$. ◿

[26] The converse to this statement is that if $p, n \in \mathbb{N}$ and p is irreducible, then there exists a finite field with p^n elements. It turns out that this is true, but proving it is beyond the scope of this chapter (or, given current plans, the scope of these notes.)

That said, we can make the following observation.

Proposition 8.68: *In a ring R with multiplicative identity 1_R, the characteristic of a ring is determined by the multiplicative identity. That is, if c is the smallest positive integer such that $c \cdot 1_R = 0_R$, then c is the characteristic of the ring.*

PROOF: You do it! See Exercise 8.73. □

In case you are wondering why we have dedicated this much time to Definition 8.65 and Proposition 8.68, which are about *rings*, whereas this section is supposedly about fields, don't forget that a field is a commutative ring with a multiplicative identity and a little more. Thus we *have* been talking about fields, but we have also been talking about other kinds of rings as well. This is one of the nice things about abstraction: later, when we talk about other kinds of rings that are not fields but are commutative and have a multiplicative identity, we can still apply Proposition 8.68.

At any rate, it is time to get down into the dirt of building finite fields. The standard method of building a finite field is different from what we will do here, but the method used here is an interesting application of quotient rings.

Notation 8.69: Our notation for a finite field with n elements is $\mathbb{F}_n$. However, we cannot yet say that $\mathbb{F}_p = \mathbb{Z}_p$ whenever p is prime.

Example 8.70: We will build finite fields with four and sixteen elements. In the exercises, you will use the same technique to build fields of nine and twenty-seven elements.

Case 1. $\mathbb{F}_4$

Start with the polynomial ring $\mathbb{Z}_2[x]$. We claim that $f(x) = x^2 + x + 1$ does not factor in $\mathbb{Z}_2[x]$. If it did, it would have to factor as a product of linear polynomials; that is,

$$f(x) = (x + a)(x + b)$$

where $a, b \in \mathbb{Z}_2$. This implies that a is a root of f (remember that in $\mathbb{Z}_2$, $a = -a$), but f has no zeroes:

$$f(0) = 0^2 + 0 + 1 = 1 \text{ and}$$
$$f(1) = 1^2 + 1 + 1 = 1.$$

Thus f does not factor. By Exercise 8.62, $I = \langle f \rangle$ is a maximal ideal in $R = \mathbb{Z}_2[x]$, and by Theorem 8.55, R/I is a field.

How many elements does this field have? Let $X \in R/I$; choose a representation $g + I$ of X where $g \in R$. We assume that $\deg g < 2$. Why? If $\deg g \geq 2$ then we can subtract multiples of f; since $f + I$ is the zero element of R/I, this does not affect X.

Given that $\deg g < 2$, there must be two terms in g: x^1 and x^0. Each of these terms can have one of two coefficients: 0 or 1. This gives us $2 \times 2 = 4$ distinct possibilities for the representation of X; thus there are 4 elements of R/I. We can write them as

$$I, \quad 1 + I, \quad x + I, \quad x + 1 + I.$$

Case 1. $\mathbb{F}_{16}$

Start with the polynomial ring $\mathbb{Z}_2[x]$. We claim that $f(x) = x^4 + x + 1$ does not factor in $\mathbb{Z}_2[x]$; if it did, it would have to factor as a product of either a linear and cubic polynomial, or as a product of two quadratic polynomials. The former is impossible, since neither 0 nor 1 is a zero of f. As for the second, suppose that $f = \left(x^2 + ax + b\right)\left(x^2 + cx + d\right)$, where $a, b, c, d \in \mathbb{Z}_2$. Let's consider this possibility: If

$$x^4 + x + 1 = x^4 + (a+c)\,x^3 + (ac + b + d)\,x^2 + (ad + bc)\,x + db,$$

and since (from linear algebra) equal polynomials must have the same coefficients for like terms, we have the system of linear equations

$$\begin{aligned} a + c &= 0 \\ ac + b + d &= 0 \\ ad + bc &= 1 \\ bd &= 1. \end{aligned} \tag{21}$$

From (21) we conclude that $a = -c$, but in $\mathbb{Z}_2$ this implies that $a = c$. The system now simplifies to

$$a^2 + b + d = 0 \tag{22}$$
$$a(b + d) = 1 \tag{23}$$
$$bd = 1. \tag{24}$$

Again, in $\mathbb{Z}_2$ we know that $a^2 = a$ regardless of the value of a, so (22) implies $a = -(b + d) = b + d$. Substituting this into (23), we have $a^2 = 1$, which implies that $a = 1$. Hence $b + d = 1$, which implies that one of b and d is 1, while the other is 0. This implies that $bd = 0$, contradicting (24).

Thus f does not factor. By Exercise 8.62, $I = \langle f \rangle$ is a maximal ideal in $R = \mathbb{Z}_2[x]$, and by Theorem 8.55, R/I is a field.

How many elements does this field have? Let $X \in R/I$; choose a representation $g + I$ of X where $g \in R$. Without loss of generality, we can assume that $\deg g < 4$, since if $\deg g \geq 4$ then we can subtract multiples of f; since $f + I$ is the zero element of R/I, this does not affect X.

Since $\deg g < 4$, there are four terms in g: x^3, x^2, x^1, and x^0. Each of these terms can have one of two coefficients: $[0]$ or $[1]$. This gives us $2^4 = 16$ distinct possibilities for the representation of X; thus there are 16 elements of R/I. We can write them as

$$\begin{array}{cccc} I, & 1+I, & x+I, & x+1+I, \\ x^2+I & x^2+1+I, & x^2+x+I, & x^2+x+1+I, \\ x^3+I, & x^3+1+I, & x^3+x+I, & x^3+x+1+I, \\ x^3+x^2+I, & x^3+x^2+1+I, & x^3+x^2+x+I, & x^3+x^2+x+1+I. \end{array} \quad \triangle$$

You may have noticed that in each case we ended up with p^n elements where $p = 2$. Since we started with $\mathbb{Z}_p$, you might wonder if the generalization of this to arbitrary finite fields starts with $\mathbb{Z}_p[x]$, finds a polynomial that does not factor in that ring, then builds the quotient ring. Yes and no. One does start with $\mathbb{Z}_p$, and if we could find an irreducible polynomial of degree n over $\mathbb{Z}_p$, then we would be finished. Unfortunately, finding an irreducible polynomial of $\mathbb{Z}_p$ is not easy.

Instead, one considers $f(x) = x^{p^n} - x$; from Euler's Theorem (Theorem 6.45) we deduce (via induction) that $f(a) = 0$ for all $a \in \mathbb{Z}_p$. One can then use *field extensions* from *Galois Theory* to construct p^n roots of f, so that f factors into linear polynomials. Extend $\mathbb{Z}_p$ by those roots; the resulting field has p^n elements. However, this is beyond the scope of this section. We settle instead for the following.

Theorem 8.71: *Suppose that $\mathbb{F}_n$ is a finite field with n elements. Then n is a power of an irreducible integer p, and the characteristic of $\mathbb{F}_n$ is p.*

PROOF: The proof has three steps.[27]

First, we show that $\mathbb{F}_n$ has characteristic p, where p is an irreducible integer. Let p be the characteristic of $\mathbb{F}_n$, and suppose that $p = ab$ for some positive integers a, b. Now

$$0_{\mathbb{F}_n} = p \cdot 1_{\mathbb{F}_n} = (ab) \cdot 1_{\mathbb{F}_n} = \left(a \cdot 1_{\mathbb{F}_n}\right)\left(b \cdot 1_{\mathbb{F}_n}\right).$$

Recall that a field is an integral domain; by definition, it has no zero divisors. Hence $a \cdot 1_{\mathbb{F}_n} = 0_{\mathbb{F}_n}$ or $b \cdot 1_{\mathbb{F}_n} = 0_{\mathbb{F}_n}$; without loss of generality, $a \cdot 1_{\mathbb{F}_n} = 0_{\mathbb{F}_n}$. By Proposition 8.68, p is the smallest positive integer c such that $c \cdot 1_{\mathbb{F}_n} = 0_{\mathbb{F}_n}$; thus $p \leq a$. However, a divides p, so $a \leq p$. This implies that $a = p$ and $b = 1$; since $p = ab$ was an arbitrary factorization of p, p is irreducible.

Second, we claim that for any irreducible $q \in \mathbb{N}$ that divides $n = |\mathbb{F}_n|$, we can find $x \in \mathbb{F}_n$ such that $q \cdot x = 0_{\mathbb{F}_n}$. Let $q \in \mathbb{N}$ such that q is irreducible and q divides $n = |\mathbb{F}_n|$. Consider the additive group of $\mathbb{F}_n$. Let

$$\mathcal{L} = \left\{ \left(a_1, a_2, \ldots, a_q\right) \in \mathbb{F}_n^q : \sum_{i=1}^{q} a_i = 0 \right\};$$

that is, $\mathcal{L}$ is the set of all lists of q elements of $\mathbb{F}_n$ such that the sum of those elements is the additive identity. For example,

$$q \cdot 0_{\mathbb{F}_n} = 0_{\mathbb{F}_n} + 0_{\mathbb{F}_n} + \cdots + 0_{\mathbb{F}_n} = 0_{\mathbb{F}_n},$$

so $\left(0_{\mathbb{F}_n}, 0_{\mathbb{F}_n}, \ldots, 0_{\mathbb{F}_n}\right) \in \mathcal{L}$.

For any $\sigma \in S_q$, the commutative property of addition implies that $\sigma\left(a_1, a_2, \ldots, a_q\right) \in \mathcal{L}$. In particular, if $\sigma \in \langle (\ 1\ \ 2\ \ \cdots\ \ q\ ) \rangle$ then $\sigma\left(a_1, a_2, \ldots, a_q\right) \in \mathcal{L}$. In fact, when we permute any element $A \in \mathcal{L}$ by some $\sigma \in \langle (\ 1\ \ 2\ \ \cdots\ \ q\ ) \rangle$, then $\sigma(A) \neq A$ implies that $\sigma \neq (\ 1\ )$ and A has

[27] Adapted from the proofs of Theorems 31.5, 42.4, and 46.1 in [AF05].

at least two distinct elements. Assume that $\sigma \neq \begin{pmatrix} 1 \end{pmatrix}$; if $\sigma(A) \neq A$, then all the permutations of $\left\langle \begin{pmatrix} 1 & 2 & \cdots & q \end{pmatrix} \right\rangle$ generate q different lists. Let

- $\mathcal{M}_1$ be the subset of $\mathcal{L}$ such that $A \in \mathcal{L}$ and $\sigma(A) = A$ for all $\sigma \in S_q$ implies that $A \in \mathcal{M}_1$; and
- $\mathcal{M}_2$ be the subset of $\mathcal{L}$ such that $A \in \mathcal{L}$ and $\sigma(A) \neq A$ implies that exactly one permutation of A is in $\mathcal{M}_2$, though perhaps not A itself.

Notice that $\sigma\left(0_{\mathbb{F}_n}, 0_{\mathbb{F}_n}, \ldots, 0_{\mathbb{F}_n}\right) = \left(0_{\mathbb{F}_n}, 0_{\mathbb{F}_n}, \ldots, 0_{\mathbb{F}_n}\right)$, so $\left(0_{\mathbb{F}_n}, 0_{\mathbb{F}_n}, \ldots, 0_{\mathbb{F}_n}\right) \in \mathcal{M}_1$ without question. In fact, the elements of $\mathcal{M}_1$ are those tuples whose entries are identical; that is, $\left(a_1, \ldots, a_q\right) \in \mathcal{M}_1$ iff $a_1 = \cdots = a_q$. On the other hand, if we let $\mathcal{M}_3 = \mathcal{L} \backslash \mathcal{M}_1$, then for any $A \in \mathcal{M}_3$ we can find $B \in \mathcal{M}_2$ such that $\sigma(A) = B$.

Let $|\mathcal{M}_1| = r$ and $|\mathcal{M}_2| = s$; then

$$|\mathcal{L}| = |\mathcal{M}_1| + q! \cdot |\mathcal{M}_2| = r + q! \cdot s.$$

In addition, when constructing $\mathcal{L}$ we can choose any elements from $\mathbb{F}_n$ that we want for the first $q-1$ elements; the final, qth element is determined to be $-\left(a_1 + a_2 + \cdots + a_{q-1}\right)$, so

$$|\mathcal{L}| = |\mathbb{F}_n|^{q-1} = n^{q-1}.$$

By substitution,

$$n^{q-1} = r + q! \cdot s.$$

Recall that $q \mid n$, say $n = qd$ for $d \in \mathbb{N}$, so

$$\begin{aligned} (qd)^{q-1} &= r + q! \cdot s \\ q\left[d\,(qd)^{q-2} - (q-1)! \cdot s\right] &= r, \end{aligned}$$

so $q \mid r$. Since $\left(0_{\mathbb{F}_n}, 0_{\mathbb{F}_n}, \ldots, 0_{\mathbb{F}_n}\right) \in \mathcal{L}$, we know that $r \geq 1$. Since $q \mid r$, some non-zero $x \in \mathbb{F}_n$ is in $\mathcal{M}_1$, implying that

$$q \cdot x = 0_{\mathbb{F}_n}.$$

Third, we claim that for any irreducible $q \in \mathbb{Z}$ that divides n, $q = p$. Let q be an irreducible integer that divides n. Using the second claim, choose $x \in \mathbb{F}_n$ such that $q \cdot x = 0_{\mathbb{F}_n}$. Since the characteristic of $\mathbb{F}_n$ is p, we also have $px = 0$. Consider the additive cyclic group $\langle x \rangle$; by Exercise 2.60 on page 47, $\operatorname{ord}(x) \mid p$, but p is irreducible, so $\operatorname{ord}(x) = 1$ or $\operatorname{ord}(x) = p$. Since $x \neq 0_{\mathbb{F}_n}$, $\operatorname{ord}(x) \neq 1$; thus $\operatorname{ord}(x) = p$. Likewise, $p \mid q$, and since both p and q are irreducible this implies that $q = p$.

We have shown that if $q \mid n$, then $q = p$. Thus all the irreducible divisors of n are p, so n is a power of p. □

A natural question to ask is whether $\mathbb{F}_{p^n}$ exists for every irreducible p and every $n \in \mathbb{N}^+$. You might think that the answer is yes; after all, it suffices to find an polynomial of degree n that is irreducible over $\mathbb{F}_p$. However, it is not obvious that such polynomials exist for every possible p and n. That is the subject of Section 9.3.

Exercises.

Exercise 8.72: Recall $R = \mathbb{Z}_2 \times \mathbb{Z}_4$ from Example 8.67.

(a) Show that R is a ring, but not an integral domain.

(b) Show that for any two rings R_1 and R_2, $R_1 \times R_2$ is a ring with addition and multiplication defined in the natural way.

(c) Show that even if the rings R_1 and R_2 are fields, $R_1 \times R_2$ is not even an integral domain, let alone a field. Observe that this argument holds true even for infinite fields, since the rings R_1 and R_2 are arbitrary.

(d) Show that for any n rings $R_1, R_2, \ldots, R_n$, $R_1 \times R_2 \times \cdots \times R_n$ is a ring with addition and multiplication defined in the natural way.

Exercise 8.73: Prove Proposition 8.68.

Exercise 8.74: Build the addition and multiplication tables of the field of four elements that we constructed in Example 8.70 on page 203.

Exercise 8.75: Construct a field with 9 elements, and list them all.

Exercise 8.76: Construct a field with 27 elements, and list them all.

Exercise 8.77: Does every infinite field have characteristic 0?

8.6: Ring isomorphisms

Just as we found with groups, it is often useful to show that two rings are essentially the same, as far as ring theory is concerned. With groups, we defined a special mapping called a *group homomorphism* that measured whether the group operation behaved similarly. We would like to do the same thing with rings. Rings have two operations rather than merely one, so we have to measure whether both ring operations behave similarly.

Definition 8.78: Let R and S be rings. A function $f : R \to S$ is a **ring homomorphism** if for all $a, b \in R$

$$f(a+b) = f(a) + f(b) \quad \text{and} \quad f(ab) = f(a)f(b).$$

If, in addition, f is one-to-one and onto, we call it a **ring isomorphism**.

Example 8.79: Let $f : \mathbb{Z} \to \mathbb{Z}_2$ by $f(x) = [x]$. The homomorphism properties are satisfied:

$$f(x+y) = [x+y] = [x] + [y] = f(x) + f(y)$$

and f is onto, but f is certainly not one-to-one, inasmuch as $f(0) = f(2)$. ◿

On the other hand, consider Example 8.80.

Example 8.80: Let $f : \mathbb{Z} \to 2\mathbb{Z}$ by $f(x) = 4x$. In Example 4.3 on page 82 we showed that this was a homomorphism of groups. However, it is *not* a homomorphism of rings, because it does not preserve multiplication:

$$f(xy) = 4xy \quad \text{but} \quad f(x)f(y) = (4x)(4y) = 16xy \neq f(xy). \triangle$$

Example 8.80 drives home the point that rings are more complicated than groups on account of having two operations. It is harder to show that two rings are homomorphic, and therefore harder to show that they are isomorphic. This is especially interesting in this example, since we had shown earlier that $\mathbb{Z} \cong n\mathbb{Z}$ *as groups* for all nonzero n. If this is the case with rings, then we have to find some other function between the two. Theorem (8.81) shows that this is not possible, in a way that should not surprise you.

Theorem 8.81: *Let R be a ring with unity. If there exists an onto homomorphism between R and another ring S, then S is also a ring with unity.*

PROOF: Let S be a ring such that there exists a homomorphism f between R and S. We claim that $f(1_R)$ is an identity for S.

Let $y \in S$; the fact that R is onto implies that $f(x) = y$ for some $x \in R$. Applying the homomorphism property,

$$y = f(x) = f(x \cdot 1_R) = f(x)f(1_R) = y \cdot f(1_R).$$

A similar argument shows that $y = f(1_R) \cdot y$. Since y was arbitrary in S, $f(1_R)$ is an identity for S. □

We can deduce from this that $\mathbb{Z}$ and $n\mathbb{Z}$ are not isomorphic as rings whenever $n \neq 1$:

- to be isomorphic, there would have to exist an onto function from $\mathbb{Z}$ to $n\mathbb{Z}$;
- $\mathbb{Z}$ has a multiplicative identity;
- by Theorem 8.81, $n\mathbb{Z}$ would also have to have a multiplicative identity;
- but $n\mathbb{Z}$ does not have a multiplicative identity when $n \neq 1$.

We should also identify some other properties of a ring homomorphism.

Theorem 8.82: *Let R and S be rings, and f a ring homomorphism from R to S. Each of the following holds:*
(A) $f(0_R) = 0_S$;
(B) *for all $x \in R$, $f(-x) = -f(x)$;*
(C) *for all $x \in R$, if x has a multiplicative inverse and f is onto, then $f(x)$ has a multiplicative inverse, and $f(x^{-1}) = f(x)^{-1}$.*

PROOF: You do it! See Exercise 8.87 on page 212. □

We have not yet encountered an example of a ring isomorphism, so let's consider one.

Example 8.83: Let $p = ax + b \in \mathbb{Q}[x]$, where $a \neq 0$. Recall from Exercise 8.62 that $\langle p \rangle$ is maximal in $\mathbb{Q}[x]$. Let $R = \mathbb{Q}[x]$ and $I = \langle p \rangle$; by Theorem 8.55, R/I is a field.

Recall that $\mathbb{Q}$ is also a field; are $\mathbb{Q}$ and R/I isomorphic? Let $f : \mathbb{Q} \to R/I$ in the following way: let $f(c) = x + I$ for every $c \in \mathbb{Q}$. Is f a homomorphism?

Homomorphism property? Let $c, d \in \mathbb{Q}$; using the definition of f and the properties of coset addition,

$$f(c+d) = (c+d) + I = (c+I) + (d+I) = f(c) + f(d).$$

Likewise,

$$f(cd) = (cd) + I = (c+I)(d+I) = f(c) f(d).$$

One-to-one? Let $c, d \in \mathbb{Q}$ and suppose that $f(c) = f(d)$. Then $c + I = d + I$, which implies that $c - d \in I$. By the closure of $\mathbb{Q}$, $c - d$ is a rational number, while $I = \langle ax + b \rangle$ is the set of all multiples of $ax + b$. Since $a \neq 0$, the only rational number in I is 0, which implies that $c - d = 0$, so $c = d$.

Onto? Let $X \in R/I$; choose a representation $X = p + I$ where $p \in \mathbb{Q}[x]$. Divide p by $ax + b$ to obtain

$$p = q(ax + b) + r$$

where $q, r \in \mathbb{Q}[x]$ and $\deg r < \deg(ax + b) = 1$. Hence

$$p + I = [q(ax + b) + r] + I = [q(ax + b) + I] + (r + I) = I + (r + I)$$

Now $\deg r < 1$ implies that $\deg r = 0$, or in other words that r is a constant. The constants of $\mathbb{Q}[x]$ are elements of $\mathbb{Q}$, so $r \in \mathbb{Q}$. Hence

$$f(r) = r + I = p + I,$$

and f is onto.

We have shown that there exists a one-to-one, onto ring homomorphism from $\mathbb{Q}$ to $\mathbb{Q}[x]$; as a consequence, $\mathbb{Q}$ and $\mathbb{Q}[x]$ are isomorphic as rings. ◿

We conclude with an important result. First, we need to revisit the definition of a kernel.

Definition 8.84: Let R and S be rings, and $f : R \to S$ a homomorphism of rings. The **kernel** of f, denoted $\ker f$, is the set of all elements of R that map to 0_S. That is,

$$\ker f = \{x \in R : f(x) = 0_S\}.$$

You will show in Exercise 8.88 that $\ker f$ is an ideal of R, and that the function $g : R \to R/\ker f$ by $g(x) = x + \ker f$ is a homomorphism of rings.

Theorem 8.85: *Let R, S be rings, and $f : R \to S$ an onto homomorphism. Let $g : R \to R/\ker f$ be the natural homomorphism $g(r) = r + \ker f$. There exists an isomorphism $h : R/\ker f \to S$ such that $f = h \circ g$.*

PROOF: Define h by $h(X) = f(x)$ where $X = x + \ker f$. Is f an isomorphism? Since its domain consists of cosets, we must show first that it's well-defined:

well-defined? Let $X \in R/\ker f$ and consider two representations $X = x + \ker f$ and $X = y + \ker f$. We must show that $h(X)$ has the same value regardless of which representation we use. Now $x + \ker f = X = y + \ker f$, so by properties of cosets $x - y \in \ker f$. From the definition of the kernel, $f(x - y) = 0_S$. We can apply Theorem 8.82 to see that

$$\begin{aligned} 0_S &= f(x-y) \\ &= f(x+(-y)) \\ &= f(x) + f(-y) \\ &= f(x) + [-f(y)], \end{aligned}$$

so $h(y + \ker f) = f(y) = f(x) = h(x + \ker f)$. In other words, the representation of X does not affect the value of h, and h is well-defined.

homomorphism property? Let $X, Y \in R/\ker f$ and consider the representations $X = x + \ker f$ and $Y = y + \ker f$. Since f is a ring homomorphism,

$$\begin{aligned} h(X+Y) &= h((x+\ker f) + (y+\ker f)) \\ &= h((x+y) + \ker f) \\ &= f(x+y) \\ &= f(x) + f(y) \\ &= h(x+\ker f) + f(y+\ker f) \\ &= h(X) + h(Y) \end{aligned}$$

and similarly

$$\begin{aligned} h(XY) &= h((x+\ker f)\cdot(y+\ker f)) \\ &= h((xy) + \ker f) \\ &= f(xy) \\ &= f(x)f(y) \\ &= h(x+\ker f)\cdot f(y+\ker f) \\ &= h(X)\cdot h(Y). \end{aligned}$$

Thus h is a ring homomorphism.

one-to-one? Let $X, Y \in R/\ker f$ and suppose that $h(X) = h(Y)$. By the definition of h, $f(x) = f(y)$ where $X = x + \ker f$ and $Y = y + \ker y$ for appropriate $x, y \in R$. Applying Theorem 8.82, we see that

$$\begin{aligned} f(x) = f(y) &\Longrightarrow f(x) - f(y) = 0_S \\ &\Longrightarrow f(x-y) = 0_S \\ &\Longrightarrow x - y \in \ker f \\ &\Longrightarrow x + \ker f = y + \ker f, \end{aligned}$$

so $X = Y$. Thus h is one-to-one.

onto? Let $y \in S$. Since f is onto, there exists $x \in R$ such that $f(x) = y$. Then $h(x + \ker f) = f(x) = y$, so h is onto.

We have shown that h is a well-defined, one-to-one, onto homomorphism of rings. Thus h is an isomorphism from $R/\ker f$ to S. □

Example 8.86: Let $f : \mathbb{Q}[x] \to \mathbb{Q}$ by $f(p) = p(2)$ for any polynomial $p \in \mathbb{Q}[x]$. That is, f maps any polynomial to the value that polynomial gives for $x = 2$. For example, if $p = 3x^3 - 1$, then $p(2) = 3(2)^3 - 1 = 23$, so $f\left(3x^3 - 1\right) = 23$.

Is f a homomorphism? For any polynomials $p, q \in \mathbb{Q}[x]$ we have

$$f(p+q) = (p+q)(2);$$

applying a property of polynomial addition we have

$$f(p+q) = (p+q)(2) = p(2) + q(2) = f(p) + f(q).$$

A similarly property of polynomial multiplication gives

$$f(pq) = (pq)(2) = p(2) \cdot q(2) = f(p) f(q),$$

so f is a homomorphism.

Is f onto? Let $a \in \mathbb{Q}$; we need a polynomial $p \in \mathbb{Q}[x]$ such that $p(2) = a$. The easiest way to do this is use a linear polynomial, and $p = x + (a-2)$ will work, since

$$f(p) = p(2) = 2 + (a-2) = a.$$

Hence f is onto.

Is f one-to-one? The answer is *no*. We already saw that $f\left(3x^3 - 1\right) = 23$, and from our work showing that f is onto, we deduce that $f(x+21) = 23$, so f is not one-to-one.

Let's apply Theorem 8.85 to obtain an isomorphism. First, identify $\ker f$: it consists of all the polynomials $p \in \mathbb{Q}[x]$ such that $p(2) = 0$. The Factor Theorem (Theorem 7.31 on

page 172) implies that $x-2$ must be a factor of any such polynomial. In other words,

$$\ker f = \{p \in \mathbb{Q}[x] : (x-2) \text{ divides } p\} = \langle x-2 \rangle .$$

Since $\ker f = \langle x-2 \rangle$, Theorem 8.85 tells us that there exists an isomorphism between the quotient ring $\mathbb{Q}[x] / \langle x-2 \rangle$ and $\mathbb{Q}$.

Notice, as in Example 8.83, that $x-2$ is a linear polynomial. Linear polynomials do not factor. By Exercise 8.62, $\langle x-2 \rangle$ is a maximal ideal; so $\mathbb{Q}[x] / \langle x-2 \rangle$ must be a field—as is $\mathbb{Q}$. ⊿

Exercises.

Exercise 8.87: Prove Theorem 8.82.

Exercise 8.88: Let R and S be rings, and $f : R \to S$ a homomorphism of rings.

(a) Show that $\ker f$ is an ideal of R.

(b) Show that the function $g : R \to R/\ker f$ by $g(x) = x + \ker f$ is a homomorphism of rings.

Exercise 8.89: Let R be a ring and $a \in R$. The **evaluation map with respect to** a is $\varphi_a : R[x] \to R$ by $\varphi_a(f) = f(a)$; that is, φ_a maps a polynomial to its value at a.

(a) If $R = \mathbb{Q}[x]$ and $a = 2/3$, find $\varphi_a\left(2x^2-1\right)$ and $\varphi_a(3x-2)$.

(b) Show that the evaluation map is a ring homomorphism.

(c) Recall from Example8.83 that $\mathbb{Q}$ is isomorphic to the quotient ring $\mathbb{Q}[x] / \langle ax+b \rangle$ where $ax+b \in \mathbb{Q}[x]$ is non-zero. Use Theorem 8.85 to show this a different way.

Exercise 8.90: Use Theorem 8.85 to show that $\mathbb{Q}[x] / \left\langle x^2 \right\rangle$ is isomorphic to

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \right\} \subset \mathbb{Q}^{2\times 2}.$$

Exercise 8.91: In this exercise we show that $\mathbb{R}$ is not isomorphic to $\mathbb{Q}$ as rings, and $\mathbb{C}$ is not isomorphic to $\mathbb{R}$ as rings.

(a) Assume to the contrary that there exists an isomorphism f from $\mathbb{R}$ to $\mathbb{Q}$.

  (i) Use the properties of a homomorphism to find $f(1)$.

  (ii) Use the result of (i) to find $f(2)$.

  (iii) Use the properties of a homomorphism to find $f\left(\sqrt{2}\right)$. This should contradict your answer for (ii).

(b) Find a similar proof that $\mathbb{C}$ and $\mathbb{R}$ are not isomorphic.

Exercise 8.92: Let $p \in \mathbb{Z}$ be irreducible, and $R = \mathbb{Z}_p[x]$. Show that $\varphi : R \to R$ by $\varphi(f) = f^p$ is an automorphism. This is called the **Frobenius automorphism**.

Exercise 8.93: Show that if R is an integral domain, then $\text{Frac}(R)$ is isomorphic to the intersection of all fields containing R as a subring.

8.7: Nullstellensatz

In this section,

- $\mathbb{F}$ is an *algebraically closed* field—that is, all polynomials over $\mathbb{F}$ have their roots in $\mathbb{F}$;
- $\mathcal{R} = \mathbb{F}[x_1, x_2, \ldots, x_n]$ is a polynomial ring;
- $F \subset \mathcal{R}$;
- $V_F \subset \mathbb{F}^n$ is the set of common roots of elements of F;[28]
- $I = \langle F \rangle$; and
- $G = (g_1, g_2, \ldots, g_m)$ is a Gröbner basis of I with respect to an admissible ordering.

Note that $\mathbb{C}$ is algebraically closed, but $\mathbb{R}$ is not, since the roots of $x^2 + 1 \in \mathbb{R}[x]$ are not in $\mathbb{R}$.

Lemma 8.94: *$\mathbb{F}$ is infinite.*

PROOF: I need this. □

Theorem 8.95: *If $V_F = \emptyset$, then $I = \mathcal{R}$.*

PROOF: We proceed by induction on n, the number of variables.

Inductive base: Let $n = 1$. Recall that in this case, $\mathcal{R}$ is a Euclidean domain, and hence a principal ideal domain. Thus $I = \langle f \rangle$ for some $f \in \mathcal{R}$. If $V_F = \emptyset$, then f has no roots in $\mathbb{F}$. However, $\mathbb{F}$ is algebraically closed, so f must have no roots in *any* field. This is possible only if f is constant.[29]

Inductive hypothesis: Let $k \in \mathbb{N}^+$, and suppose that in any polynomial ring over a closed field with $n = k$ variables, $V_F = \emptyset$ implies $I = \mathcal{R}$.

Inductive step: Let $n = k + 1$. Assume $V_F = \emptyset$. If f_1 is constant, then we are done; thus, assume f_1 is constant. Let d be the maximum degree of a term of f_1. Rewrite f_1 by substituting

$$\begin{aligned} x_1 &= y_1, \\ x_2 &= y_2 + a_2 y_1, \\ &\vdots \\ x_n &= y_n + a_n y_1, \end{aligned}$$

for some $a_1, \ldots, a_n \in \mathbb{F}$. After this substitution,

$$f_1 = c y_1^d + g(y_1, \ldots, y_n)$$

where $c \in \mathbb{F}$ and $\deg_y g < d$. Since $\mathbb{F}$ is infinite, we can choose $a_2, \ldots, a_n$ such that $c \neq 0$.

Let $\varphi : \mathcal{R} \longrightarrow \mathbb{F}[y_1, \ldots, y_n]$ by

$$\varphi(f(x_1, \ldots, x_n)) = f(y_1, y_2 + a_2 y_1, \ldots, y_n + a_n y_1);$$

[28] The notation V_F comes from the term **variety** in algebraic geometry.

[29] This requires Kronecker's Theorem. We have to see if we can work it in here, or later, and subsequently move this theorem to a more appropriate location.

that is, φ substitutes *every* element of $\mathcal{R}$ with the values that we obtained so that f_1 would have the special form above. This is a ring isomomorphism (Exercise 8.97), so that in this case, $J = \varphi(I)$ is an ideal of $\mathbb{F}[y_1,\ldots,y_n]$. Note that if $V_J \neq \emptyset$, then any $b \in V_J$ can be transformed into an element of V_F (see Exercise 8.98); hence $V_J = \emptyset$ as well.

Now let $\eta : \mathbb{F}[y_1,\ldots,y_n] \longrightarrow \mathbb{F}[y_2,\ldots,y_n]$ by $\eta(g) = g(0, y_2,\ldots,y_n)$. Again, $K = \eta(J)$ is an ideal, though the proof is different (Exercise 8.100). We claim that if $V_K \neq \emptyset$, then likewise $V_J \neq \emptyset$. To see why, let $h \in \eta(\mathbb{F}[y_1,\ldots,y_n])$, and suppose $b \in \mathbb{F}^{n-1}$ satisfies $h(b) = 0$. Let g be any element of $\mathbb{F}[y_1,\ldots,y_n]$ such that $\eta(g) = h$; then

$$g(0, b_1,\ldots,b_{n-1}) = h(b_1,\ldots,b_{n-1}) = 0,$$

so that we can prepend 0 to any element of V_K and obtain an element of V_J. Since $V_J = \emptyset$, this is impossible, so $V_K = \emptyset$.

Since $V_K = \emptyset$ and $K \subseteq \mathbb{F}[y_2,\ldots,y_n]$, the inductive hypothesis finally helps us see that $K = \mathbb{F}[y_2,\ldots,y_n]$. In other words, $1 \in K$. Since $K \subset J$ (see Exercise), $1 \in J$. Since $\varphi(f) \in \mathbb{F}$ if and only if $f \in \mathbb{F}$ (Exercise 8.99), there exists some $f \in \langle F \rangle$ such that $f \in \mathbb{F}$. □

Exercises

Exercise 8.96: Show that the intersection of two radical ideals is also radical.

Exercise 8.97: Show that φ in the proof of Theorem 8.95 is a ring isomomorphism.

Exercise 8.98: Show that for φ in the proof of Theorem 8.95, any $b \in V_{\varphi(F)}$ can be rewritten to obtain an element of V_F. *Hint:* Reverse the translation that defines φ.

Exercise 8.99: Show that for φ in the proof of Theorem 8.95, $\varphi(f) \in \mathbb{F}$ if and only if $f \in \mathbb{F}$.

Exercise 8.100: Show that for η in the proof of Theorem 8.95, if J is an ideal of $\mathbb{F}[y_1,\ldots,y_n]$, then $\eta(J)$ is an ideal of $\mathbb{F}[y_2,\ldots,y_n]$. *Hint:* $\mathbb{F}[y_2,\ldots,y_n] \subsetneq \mathbb{F}[y_1,\ldots,y_n]$ and $\eta(J) = J \cap \mathbb{F}[x_2,\ldots,y_n]$ is an ideal of $\mathbb{F}[y_2,\ldots,y_n]$.

Chapter 9:
Rings and polynomial factorization

In this chapter we begin a turn toward applications of ring theory. In particular, here we will build up some basic algorithms for factoring polynomials. To do this, we will revisit the Chinese Remainder Theorem that we studied in Chapter 6, study more precisely the rings that factor, then delve into the algorithms themselves.

In this chapter, every ring is an integral domain, unless otherwise specified.

9.1: The link between factoring and ideals

We start with two important problems for factorization: the link between factoring and ideals, and the distinction between irreducible and prime elements of a ring.

As for the latter, we mentioned in Chapter 6 that although irreducible integers are prime and vice-versa, the same would not hold true later. Here we want to explore the question,

When is a prime element of a ring irreducible, and vice-versa?

Before answering that question, we should first define what are meant by the two terms. In fact, their definitions are identical to the definitions in Chapter 6. Compare the definitions below to Definitions 6.26 and 6.29.

Definition 9.1: Let R be a commutative ring with unity, and $a, b, c \in R \setminus \{0\}$. We say that

- a is a **unit** if a has a multiplicative inverse;
- a and b are **associates** if $a = bc$ and c is a unit;
- a is **irreducible** if a is not a unit and for every factorization $a = bc$, one of b or c is a unit; and
- a is **prime** if a is not a unit and whenever $a \mid bc$, we can conclude that $a \mid b$ or $a \mid c$.

Example 9.2: Consider the ring $\mathbb{Q}[x]$.

- The only units are the rational numbers, since no polynomial has a multiplicative inverse.
- $4x^2+6$ and $6x^2+9$ are associates, since $4x^2+6 = \frac{2}{3}(6x^2+9)$. Notice that they are *not* associates in $\mathbb{Z}[x]$, however.
- $x+q$ is irreducible for every $q \in \mathbb{Q}$. x^2+q is also irreducible for every $q \in \mathbb{Q}$ such that $q > 0$. ◿

The link between divisibility and principal ideals (Exercise 8.18(b)) implies that we can rewrite Definition 9.1 in terms of ideals.

Theorem 9.3: *Let R be an integral domain, and let $a, b \in R$.*

(A) *a is a unit if and only if $\langle a \rangle = R$.*

(B) *a and b are associates if and only if $\langle a \rangle = \langle b \rangle$.*

(C) *In a principal ideal domain, a is irreducible if and only if $\langle a \rangle$ is maximal.*

(D) *In a principal ideal domain, a is prime if and only if $\langle a \rangle$ is prime.*

PROOF: We show (A) and (C), and leave (B) and (D) to the exercises.

(A) This is a straightforward chain: a is a unit if and only if there exists $b \in R$ such that $ab = 1_R$ if and only if $1_R \in \langle a \rangle$ if and only if $R = \langle a \rangle$.

(C) Assume that R is a principal ideal domain, and suppose first that a is irreducible. Let B be an ideal of R such that $\langle a \rangle \subseteq B \subseteq R$. Since R is a principal ideal domain, $B = \langle b \rangle$ for some $b \in R$. Since $a \in B = \langle b \rangle$, $a = rb$ for some $r \in R$. By definition of irreducible, r or b is a unit. If r is a unit, then by definition, a and b are associates, and by part (B) $\langle a \rangle = \langle b \rangle = B$. Otherwise, b is a unit, and by part (A) $B = \langle b \rangle = R$. Since $\langle a \rangle \subseteq B \subseteq R$ implies $\langle a \rangle = B$ or $B = R$, we can conclude that $\langle a \rangle$ is maximal.

For the converse, we show the contrapositive. Assume that a is not irreducible; then there exist $r, b \in R$ such that $a = rb$ and neither r nor b is a unit. Thus $a \in \langle b \rangle$ and by Lemma 8.28 and part (B) of this lemma, $\langle a \rangle \subsetneq \langle b \rangle \subsetneq R$. In other words, $\langle a \rangle$ is not maximal. By the contrapositive, then, if $\langle a \rangle$ is maximal, then a is irreducible. □

Remark 9.4: In the proof, we did *not* need the assumption that R be a principal ideal domain to show that if $\langle a \rangle$ is maximal, then a is irreducible. So in fact this remains true even when R is not a principal ideal domain.

On the other hand, if R is not a principal ideal domain, then it can happen that a is irreducible, but $\langle a \rangle$ is not maximal. Returning to the example $\mathbb{C}[x, y]$ that we exploited in Theorem 8.46 on page 195, x is irreducible, but $\langle x \rangle \subsetneq \langle x, y \rangle \subsetneq \mathbb{C}[x, y]$.

In a similar way, the proof you develop of part (D) should show that if $\langle a \rangle$ is prime, then a is prime even if R is not a principal ideal domain. The converse, however, might not be true. In any case, we have the following result.

We *do* need R to be an integral domain to show (B). For a counterexample, consider $R = \mathbb{Z}_6$; we have $\langle 2 \rangle = \langle 4 \rangle$, but $2 \cdot 2 = 4$ and $4 \cdot 2 = 2$. Neither 2 nor 4 is a unit, so 2 and 4 are not associates.

Theorem 9.5: *Let R be an integral domain, and let $p \in R$. If $\langle p \rangle$ is maximal, then p is irreducible, and if $\langle p \rangle$ is prime, then p is prime.*

It is now easy to answer part of the question that we posed at the beginning of the section.

Corollary 9.6: *In a principal ideal domain, if an element p is irreducible, then it is prime.*

PROOF: You do it! See Exercise 9.11. □

The converse is true even if we are not in a principal ideal domain.

Theorem 9.7: *If R is an integral domain and $p \in R$ is prime, then p is irreducible.*

PROOF: Let R be a ring with unity, and $p \in R$. Assume that p is prime. Suppose that there exist $a, b \in R$ such that p factors as $p = ab$. Since $p \cdot 1 = ab$, the definition of prime implies that $p \mid a$ or $p \mid b$. Without loss of generality, there exists $q \in R$ such that $pq = a$. By substition,

$p = ab = (pq)\,b$. Since we are in an integral domain, it follows that $1_R = qb$; that is, b is a unit.

We took an arbitrary prime p that factored, and found that one of its factors is a unit. By definition, then, p is irreducible. □

To resolve the question completely, we must still decide whether:

1. an irreducible element is prime even when the ring is not a principal ideal domain; or
2. a prime element is irreducible even when the ring is not an integral domain.

The answer to both question is, "only sometimes". We can actually get there with a more sophisticated structure, but we don't have the information yet.

Example 9.8: Let

$$\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}.$$

You will show in the exercises that this is a ring. It is also not a principal ideal domain. Rather than show this directly, consider the fact that

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right).$$

It is not hard to see that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible in this ring. The above equation implies that they cannot be prime, either, since (for example) 2 divides the product $\left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$ but neither of the factors. We know from Corollary 9.6 that irreducibles are prime in a principal ideal domain; hence, $\mathbb{Z}\left[\sqrt{-5}\right]$ must not be a principal ideal domain.

Example 9.9: Consider the ring $\mathbb{Z}_{18}$. It is not hard to verify that 2 is a prime element of $\mathbb{Z}_{18}$. However, 2 is not irreducible, since $2 = 72 = 12 \cdot 6$, neither of which is a unit.

We have now answered the question posed at the beginning of the chapter:

- If R is an integral domain, then prime elements are irreducible.
- If R is a principal ideal domain, then irreducible elements are prime.

Because we are generally interested in factoring only for integral domains, many authors restrict the definition of *prime* so that it is defined only in an integral domain. In this case, a prime element is always irreducible, although the converse might not be true, since not all integral domains are principal ideal domains. We went beyond this in order to show, as we did above, *why* it is defined in this way. Since we maintain throughout most of this chapter the assumption that all rings are integral domains, one could shorten this (as many authors do) to,

A prime element is always irreducible, but an irreducible element is not always prime.

Exercises.

Exercise 9.10: Prove parts (B) and (D) of Theorem 9.3.

Exercise 9.11: Prove Corollary 9.6.

Exercise 9.12: Prove that $\mathbb{Z}\left[\sqrt{-5}\right]$ is a ring.

Exercise 9.13: Show that in an integral domain, factorization terminates iff every ascending sequence of principal ideals $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \cdots$ is eventually stationary; that is, for some $n \in \mathbb{N}^+$, $\langle a_i\rangle = \langle a_{i+1}\rangle$ for all $i \geq n$.

Exercise 9.14: Show that in a principal ideal domain R, a greatest common divisor d of $a, b \in R$ always exists, and:
(a) $\langle d\rangle = \langle a, b\rangle$; and
(b) there exist $r, s \in R$ such that $d = ra + sb$.

9.2: Unique Factorization domains

An important fact about the integers is that every integer factors *uniquely* into a product of irreducible elements. We saw this in Chapter 6 with the Fundamental Theorem of Arithmetic (Theorem 6.32 on page 143). This is not true in every ring. For example, consider $\mathbb{Z}\left[-\sqrt{5}\right]$; here $6 = 2\cdot 3$, but $6 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$. In this ring, 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$ are all irreducible, so 6 factors two different ways as a product of irreducibles. We are interested in unique factorization, so we will start with a definition:

Definition 9.15: An integral domain is a **unique factorization domain** if every $r \in R$ factors into irreducibles $r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, and if this factorization is unique up to order and associates.

Obviously $\mathbb{Z}$ is a unique factorization domain. What are some others?

Example 9.16: $\mathbb{Z}[x]$ is a unique factorization domain. To see this takes two major steps. Let $f \in \mathbb{Z}[x]$. If the terms of f have a common divisor, we can factor that out easily; for example, $2x^2+4x = 2x(x+2)$. So we may assume, without loss of generality, that the terms of f have no common factor. If f is not irreducible, then we claim it must factor as two polynomials of smaller degree. Otherwise, f would factor as ag where $\deg a = 0$, which implies $a \in \mathbb{Z}$, which implies that a is a common factor of the terms of f, contradicting the hypothesis. Since the degrees of the factors of f are integers, and they decrease each time we factor a polynomial further, the well-ordering property of $\mathbb{Z}$ implies that this process must eventually end with irreducibles; that is, $f = p_1 p_1 \cdots p_n$, where $i \neq j$ does *not* imply that $p_i \neq p_j$.

Suppose that we can also factor f into irreducibles by $f = q_1 \cdots q_n$. Consider f as an element of $\mathbb{Q}[x]$, which by Exercise 8.37 on page 193 is a principal ideal domain. Corollary 9.6 tells us that irreducible elements of $\mathbb{Q}[x]$ are prime. Hence p_1 divides q_j for some $j = 1, \ldots, m$. Without loss of generality, $p_1 \mid q_1$. Since q_1 is also irreducible, p_1 and q_1 are associates; say $p_1 = a_1 q_1$ for some unit a_1. The units of $\mathbb{Q}[x]$ are the nonzero elements of $\mathbb{Q}$, so $a_1 \in \mathbb{Q}\setminus\{0\}$. And so forth; each p_i is an associate of a unique q_j in the product.

Right now we have p_i and q_j as associates in $\mathbb{Q}[x]$. If we can show that each $a_i = \pm 1$, then we will have shown that the corresponding p_i and q_j are associates in $\mathbb{Z}[x]$ as well, so we will have shown that $\mathbb{Z}[x]$ is a unique factorization domain. Write $a_1 = \frac{b}{c}$ where $\gcd(b,c) = 1$; we have $p_1 = \frac{b}{c}\cdot q_1$. We can rewrite this as $c\,p_1 = b\,q_1$. Lemma 6.15 on page 135 implies both

that $c \mid q_1$ and that $b \mid p_1$. However, if the greatest common divisor of the coefficients of p_1 is not 1, then p_1 would not be irreducible in $\mathbb{Z}[x]$! So $b, c = \pm 1$, which implies that $a_1 = \pm 1$. Hence p_1 and q_1 are associates in $\mathbb{Z}[x]$.

The same argument can be applied to the remaining irreducible factors. Thus, the factorization of f was unique up to order and associates. ◿

Example 9.17: The ring $6\mathbb{Z}$ is not a unique factorization domain. Its irreducible elements include ± 6 and ± 12, but $72 = 6 \cdot 12 = (-6) \cdot (-12)$. Notice that here 6 and -6 are *not* associates, because $-1 \notin 6\mathbb{Z}$. On the other hand, notice that $6\mathbb{Z}$ is also not an integral domain, because it does not have unity, so of course it cannot be a unique factorization domain. ◿

Now we consider some facts about unique factorization domains.

Theorem 9.18: *Every principal ideal domain is a unique factorization domain.*

PROOF: Let R be a principal ideal domain, and $f \in R$.

First we show that f has a factorization. Suppose f is not irreducible; then there exist $p_1, p_2 \in R$ such that $f = p_1 p_2$ and f is not an associate of either. By Theorem 9.3, $\langle f \rangle \subsetneq \langle p_1 \rangle$ and $\langle f \rangle \subsetneq \langle p_2 \rangle$. If p_1 is not irreducible, then there exist $p_3, p_4 \in R$ such that $p_1 = p_3 p_4$ and p_1 is not an associate of either. Again, $\langle p_1 \rangle \subsetneq \langle p_3 \rangle$ and $\langle p_1 \rangle \subsetneq \langle p_4 \rangle$. Continuing in this fashion, we obtain an ascending chain of ideals

$$\langle f \rangle \subsetneq \langle p_1 \rangle \subsetneq \langle p_3 \rangle \subsetneq \cdots .$$

By Theorem 8.34 on page 191, a principal ideal domain satisfies the ascending chain condition; thus, this chain must terminate eventually. It can terminate only if we reach an irreducible polynomial. This holds for each chain, so they must all terminate with irreducible polynomials. Combining the results, we obtain $f = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ where each p_i is irreducible.

Now we show the factorization is unique. Suppose that $f = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ and $f = q_1^{\beta_1} \cdots q_n^{\beta_n}$ where $m \leq n$ and the p_i and q_j are irreducible. Recall that irreducible elements are prime in a principal ideal domain (Corollary 9.6). Hence p_1 divides one of the q_i; without loss of generality, $p_1 \mid q_1$. However, q_1 is irreducible, so p_1 and q_1 must be associates; say $p_1 = a_1 q_1$ for some unit $a_1 \in R$. Since we are in an integral domain, we can cancel p_1 and q_1 from $f = f$, obtaining

$$p_2^{\alpha_2} \cdots p_m^{\alpha_m} = a_1^{-1} q_1^{\beta_1 - \alpha_1} q_2^{\beta_2} \cdots q_n^{\beta_n}.$$

Since p_2 is irreducible, hence prime, we can continue this process until we conclude with $1_R = a_1^{-1} \cdots a_m^{-1} q_1^{\gamma_1} \cdots q_n^{\gamma_n}$. By definition, irreducible elements are not units, so $\gamma_1, \ldots, \gamma_n$ are all zero. Thus the factorization is unique up to ordering and associates.

We chose an arbitrary element of an arbitrary principal ideal domain R, and showed that it had only one factorization into irreducibles. Thus every principal ideal domain is a unique factorization domain. □

Corollary 9.19: *Every Euclidean domain is a unique factorization domain.*

PROOF: This is a consequence of Theorem 9.18 and Theorem 8.31 on page 190. □

The converse is false; see Example 7.41 on page 179. However, the definition of a greatest common divisor that we introduced with Euclidean domains certainly generalizes to unique factorization domains.

We can likewise extend a result from a previous section.

Theorem 9.20: *In a unique factorization domain, irreducible elements are prime.*

PROOF: You do it! See Exercise 9.24. □

Corollary 9.21: *In a unique factorization domain:*
- *an element is irreducible iff it is prime; and*
- *an ideal is maximal iff it is prime.*

In addition, we can say the following:

Theorem 9.22: *In a unique factorization domain, greatest common divisors are unique up to associates.*

PROOF: Let R be a unique factorization domain, and let $f, g \in R$. Let $d, \widehat{d}$ be two gcds of f, g. Let $d = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ be an irreducible factorization of d, and $\widehat{d} = q_1^{\beta_1} \cdots q_n^{\beta_n}$ be a unique factorization of $\widehat{d}$. Since d and $\widehat{d}$ are both gcds, $d \mid \widehat{d}$ and $\widehat{d} \mid d$. So $p_1 \mid \widehat{d}$. By Theorem 9.20, irreducible elements are prime in a unique factorization domain, so $p_1 \mid q_i$ for some $i = 1, \ldots, n$. Without loss of generality, $p_1 \mid q_1$. Since q_1 is irreducible, p_1 and q_1 must be associates.

We can continue this argument with $\frac{d}{p_1}$ and $\frac{\widehat{d}}{p_1}$, so that $d = a\widehat{d}$ for some unit $a \in R$. Since d and $\widehat{d}$ are unique up to associates, greatest common divisors are unique up to associates. □

Exercises.

Exercise 9.23: Use $\mathbb{Z}[x]$ to show that even if R a unique factorization domain but not a principal ideal domain, then we cannot write always find $r, s \in R$ such that $\gcd(a, b) = ra + sb$ for every $a, b \in R$.

Exercise 9.24: Prove Theorem 9.20.

Exercise 9.25: Consider the ideal $\langle 180 \rangle \subset \mathbb{Z}$. Use unique factorization to build a chain of ideals $\langle 180 \rangle = \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots \subsetneq \langle a_n \rangle = \mathbb{Z}$ such that there are no ideals between $\langle a_i \rangle$ and $\langle a_{i+1} \rangle$. Identify $a_1, a_2, \ldots$ clearly.

Exercise 9.26: We showed in Theorem 9.22 that gcds are unique up to associate for in every unique factorization domain. Suppose that $P = \mathbb{F}[x]$ for some field $\mathbb{F}$. Since P is a Euclidean domain (Exercise 7.50 on page 182), it is a unique factorization domain, and gcds are unique up to associates (Theorem 9.22 on the previous page). The fact that the base ring is a field allows us some leeway that we do not have in an ordinary unique factorization domain. For any two $f, g \in P$, use the properties of a field to describe a method to define a "canonical" gcd $\gcd(f, g)$, and show that this canonical gcd is unique.

Exercise 9.27: Generalize the argument of Example 9.16 to show that for any unique factorization domain R, the polynomial ring $R[x]$ is a unique factorization domain. Explain why this shows that for any unique factorization domain R, the polynomial ring $R[x_1, \ldots, x_n]$ is a unique factorization domain. On the other hand, give an example that shows that if R is not a unique factorization domain, then neither is $R[x]$.

9.3: Finite fields II

We saw in Section 8.5 that *if* a field is finite, then its size is p^n for some $n \in \mathbb{N}^+$ and some irreducible integer p. In this section, we show the converse: for every irreducible integer p and for every $n \in \mathbb{N}^+$, there exists a field with p^n elements. In this section, we show that for any polynomial $f \in \mathbb{F}[x]$,

- there exists a field $\mathbb{E}$ containing *one* root of f;
- there exists a field $\mathbb{E}$ where f factors into linear polynomials; and
- we can use this fact to build a finite field with p^n elements for any irreducible integer p, and for any $n \in \mathbb{N}^+$.

Theorem 9.28: *Suppose $f \in \mathbb{F}[x]$ is irreducible.*
(A) $\mathbb{E} = \mathbb{F}[x] / \langle f \rangle$ *is a field.*
(B) $\mathbb{F}$ *is isomorphic to a subfield $\mathbb{F}'$ of $\mathbb{E}$.*
(C) *Let $\widehat{f} \in \mathbb{E}[x]$ such that the coefficient of x^i is $a_i + \langle f \rangle$, where a_i is the coefficient of x^i in f. There exists $\alpha \in \mathbb{E}$ such that $\widehat{f}(\alpha) = 0$.*
In other words, $\mathbb{E}$ contains a root of $\widehat{f}$.

PROOF: Denote $I = \langle f \rangle$.

(A) Let $\mathbb{E} = \mathbb{F}[x] / I$. In Exercise 8.62, you showed that if f is irreducible in $\mathbb{F}[x]$, then I is maximal in $\mathbb{F}[x]$. By Theorem 8.55, the quotient ring $\mathbb{E} = \mathbb{F}[x] / I$ is a field.

(B) To see that $\mathbb{F}$ is isomorophic to

$$\mathbb{F}' = \{a + I : a \in \mathbb{F}\} \subsetneq \mathbb{E},$$

use the function $\varphi : \mathbb{F} \to \mathbb{F}'$ by $\varphi(a) = a + I$. You will show in the exercises that φ is a ring isomorphism.

(C) Let $\alpha = x + I$. Let $a_0, a_1, \ldots, a_n \in \mathbb{F}$ such that

$$f = a_0 + a_1 x + \cdots + a_n x^n.$$

As defined in this Theorem,

$$\widehat{f}(\alpha) = (a_0 + I) + (a_1 + I)\alpha + \cdots + (a_n + I)\alpha^n.$$

By substitution and the arithmetic of ideals,

$$\begin{aligned}\widehat{f}(\alpha) &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\ &= (a_0 + I) + (a_1 x + I) + \cdots + (a_n x^n + I) \\ &= (a_0 + a_1 x + \cdots + a_n x^n) + I \\ &= f + I.\end{aligned}$$

By Theorem 8.53, $f + I = I$, so $\widehat{f}(\alpha) = I$. Recall that $\mathbb{E} = \mathbb{F}[x]/I$; it follows that $\widehat{f}(\alpha) = 0_{\mathbb{E}}$. □

The isomorphism between $\mathbb{F}$ and $\mathbb{F}'$ implies that we can *always* assume that an irreducible polynomial over a field $\mathbb{F}$ has a root in another field containing $\mathbb{F}$. We will, in the future, think of $\mathbb{E}$ as a field containing $\mathbb{F}$, rather than containing a field isomorphic to $\mathbb{F}$.

Corollary 9.29 (Kronecker's Theorem): *Let $f \in \mathbb{F}[x]$ and $n = \deg f$. There exists a field $\mathbb{E}$ such that $\mathbb{F} \subseteq \mathbb{E}$, and f factors into linear polynomials in $\mathbb{E}$.*

PROOF: We proceed by induction on $\deg f$.

Inductive base: If $\deg f = 1$, then $f = ax + b$ for some $a, b \in \mathbb{F}$ with $a \neq 0$. In this case, let $\mathbb{E} = \mathbb{F}$; then $-a^{-1}b \in \mathbb{E}$ is a root of f.

Inductive hypothesis: Assume that for any polynomial of degree n, there exists a field $\mathbb{E}$ such that $\mathbb{F} \subseteq \mathbb{E}$, and f factors into linear polynomials in $\mathbb{E}$.

Inductive step: Assume $\deg f = n + 1$. By Exercise 9.27, $\mathbb{F}[x]$ is a unique factorization domain, so let p be an irreducible factor of f. Let $g \in \mathbb{F}[x]$ such that $f = pg$. By Theorem 9.28, there exists a field $\mathbb{E}'$ such that $\mathbb{F} \subsetneq \mathbb{E}'$ and $\mathbb{E}'$ contains a root α of p. Of course, if α is a root of p, then it is a root of f: $f(\alpha) = p(\alpha)g(\alpha) = 0 \cdot g(\alpha) = 0$. By the Factor Theorem, we can write $f = (x - \alpha)q(x) \in \mathbb{E}'[x]$. We now have $\deg q = \deg f - 1 = n$. By the inductive hypothesis, there exists a field $\mathbb{D}$ such that $\mathbb{E}' \subseteq \mathbb{E}$, and q factors into linear polynomials in $\mathbb{E}$. But then $\mathbb{F} \subsetneq \mathbb{E}' \subseteq \mathbb{E}$, and f factors into linear polynomials in $\mathbb{E}$. □

Example 9.30: Let $f(x) = x^4 + 1 \in \mathbb{Q}[x]$. We can construct a field $\mathbb{E}'$ with a root α of f; using the proofs above,

$$\mathbb{E}' = \mathbb{Q}[x]/\langle f \rangle \qquad \text{and} \qquad \alpha = x + \langle f \rangle.$$

Notice that $-\alpha$ is also a root of f, so in fact, $\mathbb{E}'$ contains two roots of f. If we repeat the procedure, we obtain two more roots of f in a field $\mathbb{E}$. ◿

Before we proceed to the third topic of this section, we need a concept that we borrow from Calculus.

Definition 9.31: Let $f \in \mathbb{F}[x]$, and write $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$. The **formal derivative of** f is

$$f' = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Proposition 9.32 (The product rule): *Let $f \in \mathbb{F}[x]$, and suppose f factors as $f = pq$. Then $f' = p'q + pq'$.*

PROOF: Write $p = \sum_{i=0}^{m} a_i x^i$ and $q = \sum_{j=0}^{n} b_j x^j$. First we write f in terms of the coefficints of p and q. By Definition 7.29 on page 171 and the distributive property,

$$f = pq = \sum_{i=0}^{m} \left[a_i x^i \sum_{j=0}^{n} b_j x^j \right] = \sum_{i=0}^{m} \left[\sum_{j=0}^{n} \left(a_i b_j \right) x^{i+j} \right].$$

If we collect like terms, we can rewrite this as

$$f = \sum_{k=0}^{m+n} \left[\left(\sum_{i+j=k} a_i b_j \right) x^k \right].$$

We can now examine the claim. By definition,

$$f' = \sum_{k=1}^{m+n} \left[k \left(\sum_{i+j=k} a_i b_j \right) x^{k-1} \right].$$

On the other hand,

$$\begin{aligned}
p'q + pq' &= \left(\sum_{i=1}^{m} i a_i x^{i-1} \right) \left(\sum_{j=0}^{n} b_j x^j \right) + \left(\sum_{i=0}^{m} a_i x^i \right) \left(\sum_{j=1}^{n} j b_j x^{j-1} \right) \\
&= \sum_{k=1}^{m+n} \left[\left(\sum_{i+j=k} i a_i b_j \right) x^{k-1} \right] + \sum_{k=1}^{m+n} \left[\left(\sum_{i+j=k} j a_i b_j \right) x^{k-1} \right] \\
&= \sum_{k=1}^{m+n} \left[\left(\sum_{i+j=k} (i+j) a_i b_j \right) x^{k-1} \right] \\
&= \sum_{k=1}^{m+n} \left[\left(\sum_{i+j=k} k a_i b_j \right) x^{k-1} \right] \\
&= f'.
\end{aligned}$$

□

We can now prove the final assertion of this section.

Theorem 9.33: *For any irreducible integer p, and for any $n \in \mathbb{N}^+$, there exists a field with p^n elements.*

PROOF: Let $f = x^{p^n} - x \in \mathbb{Z}_p[x]$. By Kronecker's Theorem, there exists a field $\mathbb{E}$ such that $\mathbb{Z}_p \subseteq \mathbb{E}'$, and f factors into linear polynomials in $\mathbb{E}'$. Let $\mathbb{E} = \{\alpha \in \mathbb{E}' : f(\alpha) = 0\}$. We claim that $\mathbb{E}$ has p^n elements, and that $\mathbb{E}$ is a field.

To see that $\mathbb{E}$ has p^n elements, it suffices to show that f has no repeated linear factors. Suppose to the contrary that it does; say

$$f = (x-a)^2 \cdot g$$

for some $g \in \mathbb{E}[x]$. By Proposition 9.32,

$$f' = 2(x-a) \cdot g + (x-a)^2 \cdot g' = (x-a) \cdot \left(2g + (x-a)\, g'\right).$$

That is, $x-a$ divides f'. To the contrary, the definition of a formal derivative tells us that

$$f' = p^n x^{p^n - 1} - 1.$$

In $\mathbb{Z}_p$, $p^n = 0$, so we can simplify f' as

$$f' = 0 - 1 = -1.$$

It is clear that $x-a$ does not divide f'; we have a contradiction, so f has no repeated linear factors.

We now show that $\mathbb{E}$ is a field. Since $\mathbb{E} \subseteq \mathbb{E}'$, we can accomplish this using the Subring Theorem to show it is a ring, and then finding an inverse for any nonzero element of $\mathbb{E}$.

For the Subring Theorem, let $a, b \in \mathbb{E}$. We must show that ab and $a-b$ are both roots of f; they would then be elements of $\mathbb{E}$ by definition of the latter. You will show in Exercise 9.35(a) that ab is a root of f. For subtraction, we claim that

$$(a-b)^{p^n} = a^{p^n} - b^{p^n}.$$

We proceed by induction.

Inductive base: Observe that

$$(a-b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p.$$

By assumption, p is an irreducible integer, so its only divisors in $\mathbb{N}$ are itself and 1. For any

$i \in \mathbb{N}^+$, then, the integer

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$$

can be factored into the two integers

$$\binom{p}{i} = p \cdot \frac{(p-1)!}{i!\,(p-i)!};$$

the fraction $\frac{(p-1)!}{i!(p-i)!}$ is an integer precisely because no element of the denominator can divide p. Using Exercise 9.35(b), we can rewrite $(a-b)^p$ as

$$\begin{aligned}(a-b)^p &= a^p + \sum_{i=1}^{p-1} \frac{p!}{i!\,(p-i)!} a^i b^{p-i} + b^p \\ &= a^p + p \cdot \sum_{i=1}^{p-1} \frac{(p-1)!}{i!\,(p-i)!} a^i b^{p-i} + b^p \\ &= a^p + 0 + b^p \\ &= a^p + b^p.\end{aligned}$$

Inductive hypothesis: Assume that $(a-b)^{p^n} = a^{p^n} - b^{p^n}$.

Inductive step: Applying the properties of exponents,

$$(a-b)^{p^{n+1}} = \left[(a-b)^{p^n}\right]^p = \left(a^{p^n} - b^{p^n}\right)^p = a^{p^{n+1}} - b^{p^{n+1}},$$

where the final step uses the base case. Thus

$$(a-b)^{p^n} - (a-b) = \left(a^{p^n} - b^{p^n}\right) - (a-b).$$

Again, a and b are roots of f, so $a^{p^n} = a$ and $b^{p^n} = b$, so

$$(a-b)^{p^n} - (a-b) = (a-b) - (a-b) = 0.$$

We see that $a-b$ is a root of f, and therefore $a-b \in \mathbb{E}$.

Finally, we show that every nonzero element of $\mathbb{E}$ has an inverse in $\mathbb{E}$. Let $a \in \mathbb{E} \setminus \{0\}$; by definition, $a \in \mathbb{E}'$. Since $\mathbb{E}'$ is a field, there exists an inverse of a in $\mathbb{E}'$; call it b. By definition of $\mathbb{E}$, a is a root of f; that is, $a^{p^n} - a = 0$. Multiply both sides of this equation by b^2, and rewrite

to obtain $a^{p^n-2} = b$. Using the substitutions $b = a^{p^n-2}$ and $a^{p^n} = a$ in $f(b)$ shows that:

$$\begin{aligned} f(b) &= b^{p^n} - b \\ &= \left(a^{p^n-2}\right)^{p^n} - a^{p^n-2} \\ &= \left(a^{p^n} \cdot a^{-2}\right)^{p^n} - a^{p^n-2} \\ &= \left(a^{p^n}\right)^{p^n} \left(a^{p^n}\right)^{-2} - a^{p^n-2} \\ &= a^{p^n} \cdot a^{-2} - a^{p^n-2} \\ &= a^{p^n-2} - a^{p^n-2} \\ &= 0. \end{aligned}$$

We have shown that b is a root of f. By definition, $b \in \mathbb{E}$. Since $b = a^{-1}$ and a was an arbitrary element of $\mathbb{E} \setminus \{0\}$, *every* nonzero element of $\mathbb{E}$ has its inverse in $\mathbb{E}$.

We have shown that

- $\mathbb{E}$ has p^n elements;
- it is a ring, since it is closed under multiplication and subtraction; and
- it is a field, since every nonzero element has a multiplicative inverse in $\mathbb{E}$.

In other words, $\mathbb{E}$ is a field with p^n elements. □

Exercises.

Exercise 9.34: Show that the function φ defined in part (B) of the proof of Theorem 9.28 is an isomorphism between $\mathbb{F}$ and $\mathbb{F}'$.

Exercise 9.35: Let p be an irreducible integer and $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Define $\mathbb{E} = \mathbb{Z}_p[x] / \langle f \rangle$.

(a) Show that $pa = 0$ for all $a \in \mathbb{E}$.

(b) Show that if $f(a) = f(b) = 0$, then $f(ab) = 0$.

9.4: Polynomial factorization in finite fields

We now turn to the question of factoring polynomials in $R[x]$. This material comes primarily from [vzGG99].

Suppose that $f \in R[x]$; factorization requires the following steps.

- **Squarefree factorization** is the process of removing multiples of factors p of f; that is, if $p^a \mid f$, then we want to work with $\frac{f}{p^{a-1}}$, for which only p is a factor.
- **Distinct degree factorization** is the process of factoring a squarefree polynomial f into polynomials $p_1, \ldots, p_m$ such that if a p_i factors as $p_i = q_1 \cdots q_n$, then $\deg q_1 = \cdots \deg q_n$.
- **Equal degree factorization** is the process of factoring each distinct degree factor p_i into its equal degree factors $q_1, \ldots, q_n$.

- The algorithms we develop in this chapter only work in finite fields. To factor a polynomial in $\mathbb{Z}[x]$, we will first factor over several finite fields $\mathbb{Z}_p[x]$, then use the Chinese Remainder Theorem to recover a factorization in $\mathbb{Z}[x]$. We discuss this in Section 9.5.

The goal of this section is merely to show you how the ideas studied so far combine into this problem. The algorithm we will study is not an inefficient algorithm, but more efficient ones exist.

For the rest of this section, we assume that $p \in \mathbb{N}$ is irreducible and $f \in \mathbb{Z}_p[x]$.

Distinct degree factorization.

Distinct-degree factorization can be accomplished using a generalization of Euler's Theorem (Theorem 6.45 on page 149).

Theorem 9.36 (Fermat's Little Theorem): *For all $a \in \mathbb{Z}_p$, $a^p = a$. In $\mathbb{Z}_p[x]$, we have*

$$x^p - x = \prod_{a \in \mathbb{Z}_p} (x - a).$$

PROOF: Euler's Theorem tells us that $a^p = a$ for all $a \in \mathbb{Z}_p$. Thus every $a \in \mathbb{Z}_p$ is a root of $x^p - x$. The Factor Theorem (Theorem 7.31 on page 172) implies that $x - a$ divides $x^p - x$ for every $a \in \mathbb{Z}_p$. But $x^p - x$ can have at most p factors, so $x^p - x = (x - 0)(x - 1) \cdots (x - (p - 1)) = \prod_{a \in \mathbb{Z}_p} (x - a)$. □

Example 9.37: Suppose $p = 5$. You already know from basic algebra that

$$\begin{aligned} x^5 - x &= x\left(x^4 - 1\right) \\ &= x\left(x^2 - 1\right)\left(x^2 + 1\right) \\ &= x(x - 1)(x + 1)\left(x^2 + 1\right). \end{aligned}$$

We are working in $\mathbb{Z}_5$, so $1 = -4$. Thus $x + 1 = x - 4$, and $(x - 2)(x - 3) = \left(x^2 - 5x + 6\right) = \left(x^2 + 1\right)$. This means that we can write

$$x^5 - x = x(x - 1)(x - 2)(x - 3)(x - 4) = \prod_{a \in \mathbb{Z}_5} (x - a),$$

as claimed. ◿

We can generalize this to the following.

Theorem 9.38: *For any $d \geq 1$, $x^{p^d} - x$ is the product of all monic irreducible polynomials in $\mathbb{Z}_p[x]$ whose degree divides d.*

Algorithm 4. Distinct degree factorization

inputs
  $f \in \mathbb{Z}_p[x]$, squarefree and monic, of degree $n > 0$
outputs
  $p_1, \ldots, p_m \in \mathbb{Z}_p[x]$, a distinct-degree factorization of f
do
  Let $h_0 = x$
  Let $f_0 = f$
  Let $i = 0$
  repeat while $f_i \neq 1$
    Increment i
    Let h_i be the remainder of division of h_{i-1}^p by f
    Let $p_i = \gcd(h_i - x, f_{i-1})$
    Let $f_i = \frac{f_{i-1}}{p_i}$
  Let $m = i$
return $p_1, \ldots, p_m$

However, proving Theorem 9.38 on the previous page is beyond the scope of this course. For now, it suffices to know what it is. In addition, it suggests an "easy" algorithm to compute the distinct degree factorization of $f \in \mathbb{Z}_p[x]$. See Algorithm 4.

Theorem 9.39: *Algorithm 4 terminates with each p_i the product of the factors of f that are all of degree i.*

PROOF: Note that the second and third steps of the loop are an optimization of the computation of $\gcd\left(x^{p^i} - x, f\right)$; you can see this by thinking about how the Euclidean algorithm would compute the gcd. So termination is guaranteed by the fact that eventually $\deg h_i^p > \deg f_i$: Theorem 9.38 implies that at this point, all distinct degree factors of f have been removed. Correctness is guaranteed by the fact that in each step we are computing $\gcd\left(x^{p^i} - x, f\right)$. □

Example 9.40: Returning to $\mathbb{Z}_5[x]$, let's look at $f = x(x+3)(x^3+4)$. Notice that *we do not know* whether this factorization is into irreducible elements. Expanded, $f = x^5 + 3x^4 + 4x^2 + 2x$. When we plug it into Algorithm 4, the following occurs:

- For $i = 1$,
  - the remainder of division of $h_0^5 = x^5$ by f is $h_1 = 2x^4 + x^2 + 3x$;
  - $p_1 = x^3 + 2x^2 + 2x$;
  - $f_1 = x^2 + x + 1$.
- For $i = 2$,
  - the remainder of division of $h_1^5 = 2x^{20} + x^{10} + 3x^5$ by f is $h_2 = x$;
  - $p_2 = \gcd(0, f_1) = f_1$;

- $f_2 = 1$.

Thus the distinct degree factorization of f is $f = \left(x^3 + 2x^2 + 2x\right)\left(x^2 + x + 1\right)$. This demonstrates that the original factorization was not into irreducible elements, since $x\,(x+3)$ is not equal to either of the two new factors, so that $x^3 + 4$ must have a linear factor as well. ◿

Equal degree factorization

Once we have a distinct degree factorization $f = p_1 \cdots p_m \in \mathbb{Z}_p[x]$ where each p_i is the product of the factors of degree i of a squarefree polynomial f, we need to factor each p_i into its irreducible factors. Here we consider the case that p is an odd prime; the case where $p = 2$ requires different methods.

Take any p_i, and let its factorization into irreducible polynomials of degree i be $p_i = q_1 \cdots q_n$. Suppose that we select at random some $h \in \mathbb{Z}_p[x]$ with $\deg h < n$. If $\gcd(p_i, h) \neq 1$, then we have found a factor of p_i. Otherwise, we will try the following. Since each q_j is irreducible and of degree i, $\left\langle q_j \right\rangle$ is a maximal ideal in $\mathbb{Z}_p[x]$, so $\mathbb{Z}_p[x] / \left\langle q_j \right\rangle$ is a field with p^i elements. Denote it by $\mathbb{F}$.

Lemma 9.41: *Let G be the set of nonzero elements of $\mathbb{F}$; that is, $G = \mathbb{F} \setminus \{0\}$. Let $a = \frac{p^i - 1}{2}$, and let $\varphi : G \to G$ by $\varphi(g) = g^e$.*
(A) φ is a group homomorphism of G.
(B) Its image, $\varphi(G)$, consists of the square roots of unity.
(C) $|\ker \varphi| = a$.

PROOF: From the definition of a field, G is an abelian group under multiplication.

(A) Let $g, h \in G$. Since G is abelian,

$$\varphi(gh) = (gh)^a = \underbrace{(gh)(gh)\cdots(gh)}_{e \text{ copies}} = \underbrace{(g \cdot g \cdots g)}_{e \text{ copies}} \cdot \underbrace{(h \cdot h \cdots h)}_{e \text{ copies}} = g^a h^a = \varphi(g)\,\varphi(h).$$

(B) Let $y \in \varphi(G)$; by definition, there exists $g \in G$ such that

$$y = \varphi(g) = g^a.$$

Corollary 3.46 to Lagrange's Theorem, with the fact that $|G| = p^i - 1$, implies that

$$y^2 = (g^a)^2 = \left(g^{\frac{p^i - 1}{2}}\right)^2 = g^{p^i - 1} = 1.$$

We see that y is a square root of unity. We chose $y \in \varphi(G)$ arbitrarily, so *every* element of $\varphi(G)$ is a square root of unity.

(C) Observe that $g \in \ker \varphi$ implies $g^a = 1$, or $g^a - 1 = 0$. That makes g an ath root of unity. Since $g \in \ker \varphi$ was chosen arbitrarily, $\ker \varphi$ consists of ath roots of unity. By Theorem 7.31 on page 172, each $g \in \ker \varphi$ corresponds to a linear factor $x - g$ of $x^a - 1$. There can

Algorithm 5. Equal-degree factorization

inputs
  $f \in \mathbb{Z}_p[x]$, where p is irreducible and odd, f is squarefree, $n = \deg f$, and all factors of f are of degree d
outputs
  a factor q_i of f
do
  Let $q = 1$
  repeat while $q = 1$
    Let $h \in \mathbb{Z}_p[x] \setminus \mathbb{Z}_p$, with $\deg h < n$
    Let $q = \gcd(h, f)$
    if $q = 1$
      Let h be the remainder from division of $h^{\frac{p^d-1}{2}}$ by f
      Let $q = \gcd(h-1, f)$
  return q

be at most a such factors, so there can be at most a distinct elements of $\ker\varphi$; that is, $|\ker\varphi| \le a$. Since $\varphi(G)$ consists of the square roots of unity, similar reasoning implies that there are at most two elements in $\varphi(G)$. Since G has $p^i - 1$ elements, Exercise 4.26 on page 86 gives us

$$p^i - 1 = |G| = |\ker\varphi|\,|\varphi(G)| \le a \cdot 2 = \frac{p^i - 1}{2} \cdot 2 = p^i - 1.$$

The inequality is actually an equality, forcing $|\ker\varphi| = a$. □

To see how Lemma 9.41 is useful, denote the coset of h in $\mathbb{F}$ by

$$[h] = h + \langle q_j \rangle \in \mathbb{F}.$$

Since $\gcd(h, q) = 1$, $h \notin \langle q_j \rangle$, so $[h] \neq 0_{\mathbb{F}}$, so $[h] \in G$. Raising $[h]$ to the ath power gives us an element of $\varphi(G)$. Part (B) of the lemma tells us that $\varphi(G)$ consists of the square roots of unity in G, so $[h]^a$ is a square root of $1_{\mathbb{F}}$, either $1_{\mathbb{F}}$ or $-1_{\mathbb{F}}$. If $[h]^a = 1_{\mathbb{F}}$, then $[h]^a - 1_{\mathbb{F}} = 0_{\mathbb{F}}$. Recall that $\mathbb{F}$ is a quotient ring, and $[h] = h + \langle q_j \rangle$. Thus

$$(h^a - 1) + \langle q_j \rangle = [h]^a - 1_{\mathbb{F}} = 0_{\mathbb{F}} = \langle q_j \rangle.$$

This is a phenomenal consequence! Equality of cosets implies that $h^a - 1 \in \langle q_j \rangle$, so q_j divides $h^a - 1$. This means that $h^a - 1$ has at least q_j in common with p_i! Taking the greatest common divisor of $h^a - 1$ and p_i extracts the greatest common factor, which may be a multiple of q_j. This leads us to Algorithm 5. Note that there we have written f instead of p_i and d instead of i.

Algorithm 5 is a little different from previous algorithms, in that it requires us to select a random element. Not all choices of h have either a common factor with p_i, or an

image $\varphi([h]) = 1_{\mathbb{F}}$. So to get $q \neq 1$, we have to be "lucky". If we're extraordinarily unlucky, Algorithm 5 might never terminate. But this is highly unlikely, for two reasons. First, Lemma 9.41(C) implies that the number of elements $g \in G$ such that $\varphi(g) = 1$ is a. We have to have $\gcd(h, p_i) = 1$ to be unlucky, so $[h] \in G$. Observe that

$$a = \frac{p^i - 1}{2} = \frac{|G|}{2},$$

so we have less than 50% probability of being unlucky, and the cumulative probability decreases with each iteration. In addition, we can (in theory) keep track of which polynomials we have computed, ensuring that we never use an "unlucky" polynomial more than once.

Keep in mind that Algorithm 5 only returns *one* factor, and that factor might not be irreducible! This is not a problem, since

(a) we can repeat the algorithm on f/g to extract another factor of f;
(b) if $\deg q = d$, then q is irreducible; otherwise;
(c) $d < \deg q < n$, so we can repeat the algorithm in q to extract a smaller factor.

Since the degree of f or q decreases each time we feed it as input to the algorithm, the well-ordering of $\mathbb{N}$ implies that we will eventually conclude with an irreducible factor.

Example 9.42: Recall from Example 9.40 that $f = x(x+3)\left(x^3+4\right) \in \mathbb{Z}_5[x]$ gave us the distinct degree factorization $f = \left(x^3+2x^2+2x\right)\left(x^2+x+1\right)$. The second polynomial is in fact the one irreducible quadratic factor of f; the first polynomial, $p_1 = x^3+2x^2+2x$, is the product of the irreducible linear factors of f. We use Algorithm 5 to factor the linear factors.

- We have to pick $h \in \mathbb{Z}_5[x]$ with $\deg h < \deg p_1 = 3$. Let $h = x^2+3$.
  - Using the Euclidean algorithm, we find that $\gcd(h, f) = 1$. (Since $r_1 = f - (x+2)h = 4x+4$ and $r_2 = h - (4x+1)r_1 = 4$.)
  - The remainder of division of $h^{\frac{5^1-1}{2}}$ by f is $3x^2+4x+4$.
  - Now $q = \gcd\left(\left(3x^2+4x+4\right)-1, p_1\right) = x+4$.
  - Return $x+4$ as a factor of p_1.

We did not know this factor from the outset! In fact, $f = x(x+3)(x+4)\left(x^2+x+1\right)$. ◿

As with Algorithm 4, we need efficient algorithms to compute gcd's and exponents in order to perform Algorithm 5. Doing these as efficiently as possible is beyond the scope of these notes, but we do in fact have relatively efficient algortihms to do both: the Euclidean algorithm (Algorithm 1 on page 130) and fast exponentiation (Section 6.4).

Squarefree factorization

We can take two approaches to squarefree factorization. The first, which works fine for any polynomial $f \in \mathbb{C}[x]$, is to compute its derivative f', then to compute $g = \gcd(f, f')$, and finally to factor $\frac{f}{g}$, which (as you will show in the exercises) is squarefree.

Another approach is to combine the previous two algorithms in such a way as to guarantee that, once we identify an irreducible factor, we remove all powers of that factor from f before proceeding to the next factor. See Algorithm 6.

Algorithm 6. Squarefree factorization in $\mathbb{Z}_p[x]$

inputs
  $f \in \mathbb{Z}_p[x]$
outputs
  An irreducible factorization $b \in \mathbb{Z}_p, p_1, \ldots, p_m \in \mathbb{Z}_p[x], \alpha_1, \ldots, \alpha_m \in \mathbb{N}^+$ such that the p_i are irreducible and $f = b\, p_1^{\alpha_1} \cdots p_m^{\alpha_m}$
do
  Let $b = \operatorname{lc}(f)$
  Let $h_0 = x$
  Let $f_0 = b^{-1} \cdot f$ — After this step, f is monic
  Let $i = 0$
  Let $j = 0$
  repeat while $f_i \neq 1$
    — Perform only one step of the distinct degree factorization
    Increment i
    Let h_i be the remainder of division of h_{i-1}^p by f
    Let $q_i = \gcd(h_i - x, f_{i-1})$
    Let $f_i = \frac{f_{i-1}}{q_i}$
    — Find the equal degree factors of q_i
    repeat while $q_i \neq 1$
      Increment j
      Find a degree-i factor p_j of q_i using Algorithm 5
      Let $q_i = \frac{q_i}{p_j}$
      — Divide out all copies of p_j from f_i
      Let $\alpha_j = 1$
      repeat while p_j divides f_i
        Increment α_j
        Let $f_i = \frac{f_i}{p_j}$
  Let $m = j$
  return $b, p_1, \ldots, p_m, \alpha_1, \ldots, \alpha_m$

Example 9.43: In Exercise 9.47 you will try (and fail) to perform a distinct degree factorization on $f = x^5 + x^3$ using only Algorithm 4. Suppose that we use Algorithm 6 to factor f instead.

- Since f is monic, $b = 1$.
- With $i = 1$, distinct-degree factorization gives us $h_1 = 4x^3$, $q_1 = x^3 + x$, $f_1 = x^2$.
    - Suppose that the first factor that Algorithm 5 gives us is x. We can then divide f_1 twice by x, so $\alpha_j = 3$ and we conclude the innermost loop with $f_1 = 1$.
    - Algorithm 5 subsequently gives us the remaining factors $x+2$ and $x+3$, none of which divides f_1 more than once..

The algorithm thus terminates with $b = 1$, $p_1 = x$, $p_2 = x+2$, $p_3 = x_3$, $\alpha_1 = 3$, and $\alpha_2 = \alpha_3 = 1$. ◿

Exercises.

Exercise 9.44: Show that $\frac{f}{g}$ is squarefree if $f \in \mathbb{C}[x]$, f' is the usual derivative from Calculus, and $g = \gcd(f, f')$.

Exercise 9.45: Use the distinct degree factorization of Example 9.40 and the fact that $f = x(x+3)(x^3+4)$ to find a complete factorization of f, using only the fact that you now know three irreducible factors f (two linear, one quadratic).

Exercise 9.46: Compute the distinct degree factorization of $f = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1$ in $\mathbb{Z}_5[x]$. Explain why you know this factorization is into irreducible elements.

Exercise 9.47: Explain why you might think that Algorithm 4 might not work for $f = x^5 + x^3$. Then try using the algorithm to factor f in $\mathbb{Z}_5[x]$, and explain why the result is incorrect.

Exercise 9.48: Suppose that we don't want the factors of f, but only its roots. Explain how we can use $\gcd(x^p - x, f)$ to give us the maximum number of roots of f in $\mathbb{Z}_p$. Use the polynomial from example 9.46 to illustrate your argument.

9.5: Factoring integer polynomials

We conclude, at the end of this chapter, to factorization in $\mathbb{Z}[x]$. In the previous section, we showed how one could factor a polynomial in an arbitrary finite field whose characteristic is an odd irreducible integer. We can use this technique to factor a polynomial $f \in \mathbb{Z}[x]$. As in the previous section, this method is not necessarily the most efficient, but it does illustrate techniques that are used in practice.

We show this using the example

$$f = x^4 + 8x^3 - 33x^2 + 120x - 720.$$

Suppose f factors as

$$f = p_1^{\alpha_1} \cdots p_m^{\alpha_m}.$$

Now let $p \in \mathbb{N}^+$ be odd and irreducible, and consider $\widehat{f} \in \mathbb{Z}_p[x]$ such that the coefficients of $\widehat{f}$ are the coefficients of f mapped to their cosets in $\mathbb{Z}_p$. That is,

$$\widehat{f} = [1]_p x^4 + [8]_p x^3 + [-33]_p x^2 + [120]_p x + [-720]_p .$$

By the properties of arithmetic in $\mathbb{Z}_p$, we know that $\widehat{f}$ will factor as

$$\widehat{f} = \widehat{p}_1^{\alpha_1} \cdots \widehat{p}_m^{\alpha_m},$$

where the coefficients of each $\widehat{p}_i$ are the coefficeints of p_i mapped to their cosets in $\mathbb{Z}_p$. As we will see, these $\widehat{p}_i$ might not be irreducible for each choice of p; we might have instead

$$\widehat{f} = \widehat{q}_1^{\beta_1} \cdots \widehat{q}_n^{\beta_n}$$

where each $\widehat{q}_i$ divides some $\widehat{p}_j$. Nevertheless, we will be able to recover the irreducible factors of f even from these factors; it will simply be more complicated.

We will approach factorization by two different routes: using one big irreducible p, or several small irreducibles along with the Chinese Remainder Theorem.

One big irreducible.

One approach is to choose an odd, irreducible $p \in \mathbb{N}^+$ sufficiently large that, once we factor $\widehat{f}$, the coefficient a_i of any p_i is either the corresponding coefficient in $\widehat{p}_i$ or (on account of the modulus) the largest negative integer corresponding to it. Sophisticated methods to obtain p exist, but for our purposes it will suffice to choose p that is approximately twice the size of the maximum coefficient of $\widehat{f}$.

Example 9.49: The maximum coefficient in the example f given above is 720. There are several irreducible integers larger than 1440 and "close" to it. We'll try the closest one, 1447. Using the techniques of the previous section, we obtain the factorization in $\mathbb{Z}_{1447}[x]$

$$\widehat{f} = (x+12)(x+1443)\left(x^2+15\right) \in \mathbb{Z}_{1447}[x] .$$

It is "obvious" that this cannot be the correct factorization in $\mathbb{Z}[x]$, because 1443 is too large. On the other hand, properties of modular arithmetic tell us that

$$\widehat{f} = (x+12)(x-4)\left(x^2+15\right) \in \mathbb{Z}_{1447}[x] .$$

In fact,

$$f = (x+12)(x-4)\left(x^2+15\right) \in \mathbb{Z}[x] .$$

This is why we chose an irreducible number that is approximately twice the largest coefficient of f: it will recover negative factors as integers that are "too large". ◿

We mentioned above that we can get "false positives" in the finite field.

Example 9.50: Let $f = x^2 + 1$. In $\mathbb{Z}_5[x]$, this factors as $x^2 + [1]_5 = \left(x + [2]_5\right)\left(x + [3]_5\right)$, but certainly $f \neq (x+2)(x+3)$ in $\mathbb{Z}[x]$. ◿

Avoiding this problem requires techniques that are beyond the scope of these notes. However, it is certain easy enough to verify whether a potential factor of p_i is a factor of f using division; once we find all the factors $\widehat{q}_j$ of $\widehat{f}$ that do not give us factors p_i of f, we can try combinations of them until they give us the correct factor. Unfortunately, this can be very time-consuming, which is why in general one would want to avoid this problem entirely.

Several small primes.

For various reasons, we may not want to try factorization modulo one large prime; in this case, it would be possible to factor using several small primes, then recover f using the Chinese Remainder Theorem. Recall that the Chinese Remainder Theorem tells us that if $\gcd\left(m_i, m_j\right) = 1$ for each $1 \leq i < j \leq n$, then we can find x satisfying

$$\begin{cases} [x] &= [\alpha_1] \text{ in } \mathbb{Z}_{m_1}; \\ [x] &= [\alpha_2] \text{ in } \mathbb{Z}_{m_2}; \\ &\vdots \\ [x] &= [\alpha_n] \text{ in } \mathbb{Z}_{m_n}; \end{cases}$$

and $[x]$ is unique in $\mathbb{Z}_N$ where $N = m_1 \cdots m_n$. If we choose $m_1, \ldots, m_n$ to be all irreducible, they will certainly satisfy $\gcd\left(m_i, m_j\right) = 1$; if we factor f in each $\mathbb{Z}_{m_i}$, we can use the Chinese Remainder Theorem to recover the coefficients of each p_i from the corresponding $\widehat{q}_j$.

Example 9.51: Returning to the polynomial given previously; we would like a unique solution in $\mathbb{Z}_{720}$ (or so). Unfortunately, the factorization $720 = 2^4 \cdot 3^2 \cdot 5$ is not very convenient for factorization. We can, however, use $3 \cdot 5 \cdot 7 \cdot 11 = 1155$:

- in $\mathbb{Z}_3[x]$, $\widehat{f} = x^3(x+2)$;
- in $\mathbb{Z}_5[x]$, $\widehat{f} = (x+1)(x+2)x^2$;
- in $\mathbb{Z}_7[x]$, $\widehat{f} = (x+3)(x+5)\left(x^2+1\right)$; and
- in $\mathbb{Z}_{11}[x]$, $\widehat{f} = (x+1)(x+7)\left(x^2+4\right)$.

If we examine all these factorizations, we can see that there appears to be a "false positive" in $\mathbb{Z}_3[x]$; we should have

$$f = (x+a)(x+b)\left(x^2+c\right).$$

The easiest of the coefficients to recover will be c, since it is unambiguous that

$$\begin{cases} c = [0]_3 \\ c = [0]_5 \\ c = [1]_7 \\ c = [4]_{11} \end{cases}$$

In fact, the Chinese Remainder Theorem tells us that $c = [15] \in \mathbb{Z}_{1155}$.

The problem with recovering a and b is that we have to guess "correctly" which arrangement of the coefficients in the finite fields give us the arrangement corresponding to $\mathbb{Z}$. For example, the system

$$\begin{cases} b = [0]_3 \\ b = [1]_5 \\ b = [3]_7 \\ b = [1]_{11} \end{cases}$$

gives us $b = [276]_{1155}$, which will turn out to be wrong, but the system

$$\begin{cases} b = [0]_3 \\ b = [2]_5 \\ b = [5]_7 \\ b = [1]_{11} \end{cases}$$

gives us $b = [12]_{1155}$, the correct coefficient in $\mathbb{Z}$.

The drawback to this approach is that, in the worst case, we would try $2^4 = 16$ combinations before we can know whether we have found the correct one. ◿

Exercises.

Exercise 9.52: Factor $x^7 + 8x^6 + 5x^5 + 53x^4 - 26x^3 + 93x^2 - 96x + 18$ using each of the two approaches described here.

Chapter 10:
Gröbner bases

A chemist named A— once emailed me about a problem he was studying that involved microarrays. Microarrays measure gene expression, and A— was using some data to build a system of equations of this form:

$$\begin{aligned} axy - b_1 x - cy + d_1 &= 0 \\ axy - b_2 x - cy + d_2 &= 0 \\ axy - b_2 x - b_1 y + d_3 &= 0 \end{aligned} \tag{25}$$

where $a, b_1, b_2, c, d_1, d_2, d_3 \in \mathbb{N}$ are known constants and $x, y \in \mathbb{R}$ were unknown. A— wanted to find values for x and y that made all the equations true.

This already is an interesting problem, and it is well-studied. In fact, A— had a fancy software program that sometimes solved the system. However, it didn't *always* solve the system, and he didn't understand whether it was because there was something wrong with his numbers, or with the system itself. All he knew is that for some values of the coefficients, the system gave him a solution, but for other values the system turned red, which meant that it found no solution.

The software that A— was using relied on well-know*numerical techniques* to look for a solution. There are many reasons that numerical techniques can fail; most importantly, they can fail *even when a solution exists.*

Analyzing these systems with an *algebraic* technique, I was able to give A— some glum news: the reason the software failed to find a solution is that, in fact, no solution existed in $\mathbb{R}$. Sometimes, solutions existed in $\mathbb{C}$, and sometimes no solution existed at all! So the problem wasn't with the software's numerical techniques.

This chapter develops and describes the algebraic techniques that allowed me to reach this conclusion. Most of the material in these notes are relatively "old": at least a century old. Gröbner bases, however, are relatively new: they were first described in 1965 [Buc65]. We will develop Gröbner bases, and finally explain how they answer the following important questions for any system of polynomial equations

$$f_1(x_1, x_2, \ldots, x_n) = 0, \quad f_2(x_1, x_2, \ldots, x_n) = 0 \quad \cdots \quad f_m(x_1, x_2, \ldots, x_n) = 0$$

whose coefficients are in $\mathbb{R}$:

1. Does the system have any solutions in $\mathbb{C}$?
2. If so,
   (a) Are there infinitely many, or finitely many?
      i. If finitely many, exactly how many are there?
      ii. If infinitely many, what is the "dimension" of the solution set?
   (b) Are any of the solutions in $\mathbb{R}$?

We will refer to these five question as ***five natural questions about the roots of a polynomial system***.

Remark 10.1: From here on, all rings are polynomial rings over a field $\mathbb{F}$, *unless we say otherwise.*

10.1: Gaussian elimination

Let's look again at the system (25) described in the introduction:

$$\begin{aligned} axy - b_1x - cy + d_1 &= 0 \\ axy - b_2x - cy + d_2 &= 0 \\ axy - b_2x - b_1y + d_3 &= 0. \end{aligned}$$

It is *almost* a linear system, and you've studied linear systems in the past. In fact, you've even studied how to answer the five natural questions about the roots of a linear polynomial system. Let's review how we accomplish this in the linear case.

A generic system of m linear equations in n variables looks like

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \vdots \qquad\qquad & \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

where the a_{ij} and b_i are elements of a field $\mathbb{F}$. Linear algebra can be done over *any* field $\mathbb{F}$, although it is typically taught with $\mathbb{F} = \mathbb{Q}$; in computational mathematics it is frequent to have $\mathbb{F} = \mathbb{R}$. Since these are notes in *algebra*, let's use a field constructed from cosets!

Example 10.2: A linear system with $m = 3$ and $n = 5$ and coefficients in $\mathbb{Z}_{13}$ is

$$\begin{aligned} 5x_1 + x_2 + 7x_5 &= 7 \\ x_3 + 11x_4 + 2x_5 &= 1 \\ 3x_1 + 7x_2 + 8x_3 &= 2. \end{aligned}$$

An equivalent system, with the same solutions, is

$$\begin{aligned} 5x_1 + x_2 + 7x_5 + 8 &= 0 \\ x_3 + 11x_4 + 2x_5 + 12 &= 0 \\ 3x_1 + 7x_2 + 8x_3 + 11 &= 0. \end{aligned}$$

In these notes, we favor the latter form. ◿

To answer the five natural questions about the linear system, we use a technique called *Gaussian elimination* to obtain a "triangular system" that is equivalent to the original system. By "equivalent", we mean that $(a_1, \ldots, a_n) \in \mathbb{F}^n$ is a solution to the triangular system if and only if it is a solution to the original system as well. What is meant by triangular form?

Definition 10.3: Let $G = (g_1, g_2, \ldots, g_m)$ be a list of linear polynomials in n variables. For each $i = 1, 2, \ldots, m$ designate the **leading variable of** g_i, as the variable with smallest index whose coefficient is non-zero. Write $\mathrm{lv}(g_i)$ for this variable, and order the variables as $x_1 > x_2 > \ldots > x_n$.
The leading variable of the zero polynomial is undefined.

Example 10.4: Using the example from 10.2,

$$\mathrm{lv}(5x_1 + x_2 + 7x_5 + 8) = x_1 \quad \text{and} \quad \mathrm{lv}(x_3 + 11x_4 + 2x_5 + 12) = x_3. \triangle$$

Remark 10.5: There are other ways to decide on a leading term, and some are smarter than others. However, we will settle on this rather straightforward method, and refer to it as the **lexicographic term ordering**.

Definition 10.6: A list of linear polynomials F is in **triangular form** if for each $i < j$,

- $f_j = 0$, or
- $f_i \neq 0$, $f_j \neq 0$, and $\mathrm{lv}(f_i) > \mathrm{lv}\left(f_j\right)$.

Example 10.7: Using the example from 10.2,the list

$$F = (5x_1 + x_2 + 7x_5 + 8, x_3 + 11x_4 + 2x_5 + 12, 3x_1 + 7x_2 + 8x_3 + 11)$$

is not in triangular form, since $\mathrm{lv}(f_2) = x_3$ and $\mathrm{lv}(f_3) = x_1$, so $\mathrm{lv}(f_2) < \mathrm{lv}(f_3)$, whereas we want $\mathrm{lv}(f_2) > \mathrm{lv}(f_3)$.

On the other hand, the list

$$G = (x_1 + 6, x_2 + 3x_4, 0)$$

is in triangular form, because $\mathrm{lv}(g_1) > \mathrm{lv}(g_2)$ and g_3 is zero. However, if we permute G using the permutation $\pi = \begin{pmatrix} 2 & 3 \end{pmatrix}$, then

$$H = \pi(G) = (x_1 + 6, 0, x_2 + 3x_4)$$

is not in triangular form, because $h_3 \neq 0$ but $h_2 = 0$. $\triangle$

Algorithm 7 describes one way to apply the method.

Theorem 10.8: *Algorithm (7) terminates correctly.*

PROOF: All the loops of the algorithm are explicitly finite, so the algorithm terminates. To show that it terminates correctly, we must show both that G is triangular and that its roots are the roots of F.

Algorithm 7. Gaussian elimination

inputs
  $F = (f_1, f_2, \ldots, f_m)$, a list of linear polynomials in n variables, whose coefficients are from a field $\mathbb{F}$.
outputs
  $G = (g_1, g_2, \ldots, g_m)$, a list of linear polynomials in n variables, in triangular form, whose roots are precisely the roots of F (if F has any roots).
do
  Let $G := F$
  for $i = 1, 2, \ldots, m-1$
    Use permutations to rearrange $g_i, g_{i+1}, \ldots, g_m$ so that for each $k < \ell$, $g_\ell = 0$, or $\mathrm{lv}(g_k) \geq \mathrm{lv}(g_\ell)$
    if $g_i \neq 0$
      Denote the coefficient of $\mathrm{lv}(g_i)$ by a
      for $j = i+1, i+2, \ldots m$
        if $\mathrm{lv}\left(g_j\right) = \mathrm{lv}(g_i)$
          Denote the coefficient of $\mathrm{lv}\left(g_j\right)$ by b
          Replace g_j with $a\,g_j - b\,g_i$
  return G

That G is triangular: We claim that each iteration of the outer loop terminates with G in *i-subtriangular form*; by this we mean that

- the list $(g_1, \ldots, g_i)$ is in triangular form; *and*
- for each $j = 1, \ldots, i$ if $g_j \neq 0$ then the coefficient of $\mathrm{lv}\left(g_j\right)$ in $g_{i+1}, \ldots, g_m$ is 0.

Note that G is in triangular form if and only if G is in i-subtriangular form for all $i = 1, 2, \ldots, m$.

We proceed by induction on i.

Inductive base: Consider $i = 1$. If $g_1 = 0$, then the form required by line (8) ensures that $g_2 = \ldots = g_m = 0$, in which case G is in triangular form, which implies that G is in 1-subtriangular form. Otherwise, $g_1 \neq 0$, so let $x = \mathrm{lv}(g_1)$. Line (14) implies that the coefficient of x in g_j will be zero for $j = 2, \ldots, m$. Thus (g_1) is in triangular form, and the coefficient of $\mathrm{lv}(g_1)$ in $g_2, \ldots, g_m$ is 0. In either case, G is in 1-subtriangular form.

Inductive step: Let $i > 1$. Use the inductive hypothesis to show that $\left(g_1, g_2, \ldots, g_{i-1}\right)$ is in triangular form *and* for each $j = 1, \ldots, i-1$ if $\mathrm{lv}\left(g_j\right)$ is defined then its coefficient in $g_i, \ldots, g_m$ is 0. If $g_i = 0$ then the form required by line (8) ensures that $g_{i+1} = \ldots = g_m = 0$, in which case G is in triangular form. This implies that G is in i-subtriangular form. Otherwise, $g_i \neq 0$, so let $x = \mathrm{lv}(g_i)$. Line (14) implies that the coefficient of x in g_j will be zero for $j = i+1, \ldots, m$. In addition, the form required by line (8) ensures that $x < \mathrm{lv}\left(g_j\right)$ for $j = 1, \ldots, i-1$. Thus $(g_1, \ldots, g_i)$ is in triangular form, and the coefficient of $\mathrm{lv}(g_i)$ in $g_2, \ldots, g_m$ is 0. In either case, G is in i-subtriangular form.

By induction, each outer loop terminates with G in i-subtriangular form. When the mth

loop terminates, G is in m-subtriangular form, which is precisely triangular form.

That G is equivalent to F: The combinations of F that produce G are all linear; that is, for each $j = 1, \ldots, m$ there exist $c_{i,j} \in \mathbb{F}$ such that

$$g_j = c_{1,j} f_1 + c_{2,j} f_2 + \cdots + a_{m,j} f_m.$$

Hence if $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n$ is a common root of F, it is also a common root of G. For the converse, observe from the algorithm that there exists some i such that $f_i = g_1$; then there exists some $j \in \{1, \ldots, m\} \setminus \{i\}$ and some $a, b \in \mathbb{F}$ such that $f_j = a\, g_1 - b\, g_2$; and so forth. Hence the elements of F are also a linear combination of the elements of G, and a similar argument shows that the common roots of G are common roots of F. □

Remark 10.9: There are other ways to define both triangular form and Gaussian elimination. Our method is perhaps stricter than necessary, but we have chosen this definition first to keep matters relatively simple, and second to assist us in the development of Gröbner bases.

Example 10.10: We use Algorithm 7 to illustrate Gaussian elimination for the system of equations described in Example 10.2.

- We start with the input,

$$F = (5x_1 + x_2 + 7x_5 + 8, x_3 + 11x_4 + 2x_5 + 12, 3x_1 + 7x_2 + 8x_3 + 11).$$

- Line 6 tells us to set $G = F$, so now

$$G = (5x_1 + x_2 + 7x_5 + 8, x_3 + 11x_4 + 2x_5 + 12, 3x_1 + 7x_2 + 8x_3 + 11).$$

- We now enter an *outer* loop:
  - In the first iteration, $i = 1$.
  - We rearrange G, obtaining

$$G = (5x_1 + x_2 + 7x_5 + 8, 3x_1 + 7x_2 + 8x_3 + 11, x_3 + 11x_4 + 2x_5 + 12).$$

  - Since $g_i \neq 0$, we proceed: Line 10 now tell us to denote a as the coefficient of $\mathrm{lv}(g_i)$; since $\mathrm{lv}(g_i) = x_1$, $a = 5$.
  - We now enter an *inner* loop:
    - ⋆ In the first iteration, $j = 2$.
    - ⋆ Since $\mathrm{lv}\left(g_j\right) = \mathrm{lv}(g_i)$, we proceed: denote b as the coefficient of $\mathrm{lv}\left(g_j\right)$; since $\mathrm{lv}\left(g_j\right) = x_1$, $b = 3$.
    - ⋆ Replace g_j with

$$\begin{aligned} a\, g_j - b\, g_i &= 5\,(3x_1 + 7x_2 + 8x_3 + 11) - 3\,(5x_1 + x_2 + 7x_5 + 8) \\ &= 32x_2 + 40x_3 - 21x_5 + 31. \end{aligned}$$

Recall that the field is $\mathbb{Z}_{13}$, so we can rewrite this as

$$6x_2 + x_3 + 5x_5 + 5.$$

We now have

$$G = (5x_1 + x_2 + 7x_5 + 8, 6x_2 + x_3 + 5x_5 + 5, x_3 + 11x_4 + 2x_5 + 12).$$

- We continue with the inner loop:
  - In the second iteration, $j = 3$.
  - Since $\mathrm{lv}(g_j) \neq \mathrm{lv}(g_i)$, we do not proceed with this iteration.
- Now $j = 3 = m$, and the inner loop is finished.

- We continue with the outer loop:
  - In the second iteration, $i = 2$.
  - We do not rearrange G, as it is already in the form indicated. (In fact, it is in triangular form already, but the algorithm does not "know" this yet.)
  - Since $g_i \neq 0$, we proceed: Line 10 now tell us to denote a as the coefficient of $\mathrm{lv}(g_i)$; since $\mathrm{lv}(g_i) = x_2$, $a = 6$.
  - We now enter an *inner* loop:
    - In the first iteration, $j = 2$.
    - Since $\mathrm{lv}(g_j) \neq \mathrm{lv}(g_i)$, we do not proceed with this iteration.
  - Now $j = 3 = m$, and the inner loop is finished.
- Now $i = 2 = m - 1$, and the outer loop is finished.
- We return G, which is in triangular form! ◿

Once we have found the triangular form of a linear system, it is easy to answer the five natural questions.

Theorem 10.11: *Let $G = (g_1, g_2, \ldots, g_m)$ is a list of nonzero linear polynomials in n variables over a field $\mathbb{F}$. Denote by S the system of linear equations $\{g_i = 0\}_{i=1}^m$. If G is in triangular form, then each of the following holds.*

(A) *S has a solution if and only if none of the g_i is a constant.*

(B) *S has finitely many solutions if and only if S has a solution and $m = n$. In this case, there is exactly one solution.*

(C) *S has solutions of dimension d if and only if S has a solution and $d = n - m$.*

A proof of Theorem 10.11 can be found in any textbook on linear algebra, although probably not in one place.

Example 10.12: Continuing with the system that we have used in this section, we found that a triangular form of

$$F = (5x_1 + x_2 + 7x_5 + 8, x_3 + 11x_4 + 2x_5 + 12, 3x_1 + 7x_2 + 8x_3 + 11)$$

is

$$G = (5x_1 + x_2 + 7x_5 + 8, 6x_2 + x_3 + 5x_5 + 5, x_3 + 11x_4 + 2x_5 + 12).$$

Let $S = \{g_1 = 0, g_2 = 0, g_3 = 0\}$. Theorem 10.11 implies that

(A) S has a solution, because none of the g_i is a constant.

(B) S has infinitely many solutions, because the number of polynomials ($m = 3$) is *not* the same as the number of variables ($n = 5$).

(C) S has solutions of dimension $d = n - m = 2$.

In fact, from linear algebra we can parametrize the solution set. Let $s, t \in \mathbb{Z}_{13}$ be arbitrary values, and let $x_4 = s$ and $x_5 = t$. Back-substituting in S, we have:

- From $g_3 = 0$, $x_3 = 2s + 11t + 1$.
- From $g_2 = 0$,

$$6x_2 = 12x_3 + 8t + 8. \tag{26}$$

  The Euclidean algorithm helps us derive the multiplicative inverse of 6 in $\mathbb{Z}_2$; we get 11. Multiplying both sides of (26) by 11, we have

$$x_2 = 2x_3 + 10t + 10.$$

  Recall that we found $x_3 = 2s + 11t + 1$, so

$$x_2 = 2(2s + 11t + 1) + 10t + 10 = 4s + 6t + 12.$$

- From $g_1 = 0$,

$$5x_1 = 12x_2 + 6x_5 + 5.$$

  Repeating the process that we carried out in the previous step, we find that

$$x_1 = 7s + 9.$$

We can verify this solution by substituting it into the original system:

$$\begin{aligned}
f_1 &:= 5(7s + 9) + (4s + 6t + 12) + 7t + 8 \\
&= (9s + 6) + 4s + 20 \\
&= 0 \\
f_2 &:= (2s + 11t + 1) + 11s + 2t + 12 \\
&= 0 \\
f_3 &:3(7s + 9) + 7(4s + 6t + 12) + 8(2s + 11t + 1) + 11 \\
&= (8s + 1) + (2s + 3t + 6) + (3s + 10t + 8) + 11 \\
&= 0.\triangle
\end{aligned}$$

Before proceeding to the next section, study the proof of Theorem (10.8) carefully. Think about how we might relate these ideas to non-linear polynomials.

Exercises.

Exercise 10.13: A *homogeneous linear system* is one where none of the polynomials has a constant term: that is, every term of every polynomial contains a variable. Explain why homogeneous systems always have at least one solution.

Exercise 10.14: Find the triangular form of the following linear systems, and use it to find the common solutions of the corresponding system of equations (if any).

(a) $f_1 = 3x + 2y - z - 1$, $f_2 = 8x + 3y - 2z$, and $f_3 = 2x + z - 3$; over the field $\mathbb{Z}_7$.

(b) $f_1 = 5a + b - c + 1$, $f_2 = 3a + 2b - 1$, $f_3 = 2a - b - c + 1$; over the same field.

(c) The same system as (a), over the field $\mathbb{Q}$.

Exercise 10.15: In linear algebra you also used matrices to solve linear systems, by rewriting them in echelon (or triangular) form. Do the same with system (a) of the previous exercise.

Exercise 10.16: Does Algorithm 7 also terminate correctly if the coefficients of F are not from a field, but from an integral domain? If so, and if $m = n$, can we then solve the resulting triangular system G for the roots of F as easily as if the coefficients were from a field? Why or why not?

10.2: Monomial orderings

As with linear polynomials, we need some way to identify the "most important" monomial in a polynomial. With linear polynomials, this was relatively easy; we picked the variable with the smallest index. With non-linear polynomials, the situation is (again) more complicated. In the polynomial on the right hand side of equation (27), which monomial should be the *leading* monomial? Should it be x, y^3, or y? It seems clear enough that y should not be the leading term, since it divides y^3, and therefore seems not to "lead". With x and y^3, however, things are not so obvious. We need to settle on a method.

Recall from Section 7.3 the definition of $\mathbb{M}$, the set of monomials over $x_1, x_2, \ldots, x_n$.

Definition 10.17: Let $t, u \in \mathbb{M}$. The **lexicographic ordering** orders $t > u$ if

- $\deg_{x_1} t > \deg_{x_1} u$, or
- $\deg_{x_1} t = \deg_{x_1} u$ and $\deg_{x_2} t > \deg_{x_2} u$, or
- $\ldots$
- $\deg_{x_i} t = \deg_{x_i} u$ for $i = 1, 2, \ldots, n-1$ and $\deg_{x_n} t > \deg_{x_n} u$.

Another way of saying this is that $t > u$ iff there exists i such that

- $\deg_{x_j} t = \deg_{x_j} u$ for all $j = 1, 2, \ldots, i-1$, and
- $\deg_{x_i} t > \deg_{x_i} u$.

The **leading monomial** of a non-zero polynomial p is any monomial t such that $t > u$ for all other terms u of p. *The leading monomial of 0 is left undefined.*

Notation 10.18: We denote the leading monomial of a polynomial p as $\mathrm{lm}(p)$.

Example 10.19: Using the lexicographic ordering over x, y,

$$\begin{aligned}\mathrm{lm}\left(x^2+y^2-4\right) &= x^2\\ \mathrm{lm}\left(xy-1\right) &= xy\\ \mathrm{lm}\left(x+y^3-4y\right) &= x.\end{aligned}$$

Before proceeding, we should prove a few simple, but important, properties of the lexicographic ordering.

Proposition 10.20: *The lexicographic ordering on* $\mathbb{M}$
(A) *is a linear ordering;*
(B) *is a* ***subordering of divisibility****: for any* $t, u \in \mathbb{M}$*, if* $t \mid u$*, then* $t \leq u$*;*
(C) *is* ***preserved by multiplication****: for any* $t, u, v \in \mathbb{M}$*, if* $t < u$*, then for any monomial* v *over* $\mathbf{x}$*,* $tv < uv$*;*
(D) *orders* $1 \leq t$ *for any* $t \in \mathbb{M}$*; and*
(E) *is a well ordering.*

(Recall that we defined a monoid way back in Section 1.2, and used $\mathbb{M}$ as an example.)

PROOF: For (A), suppose that $t \neq u$. Then there exists i such that $\deg_{x_i} t \neq \deg_{x_i} u$. Pick the smallest i for which this is true; then $\deg_{x_j} t = \deg_{x_j} u$ for $j = 1, 2, \ldots, i-1$. If $\deg_{x_i} t < \deg_{x_i} u$, then $t < u$; otherwise, $\deg_{x_i} t > \deg_{x_i} u$, so $t > u$.

For (B), we know that $t \mid u$ iff $\deg_{x_i} t \leq \deg_{x_i} u$ for all $i = 1, 2, \ldots, m$. Hence $t \leq u$.

For (C), assume that $t < u$. Let i be such that $\deg_{x_j} t = \deg_{x_j} u$ for all $j = 1, 2, \ldots, i-1$ and $\deg_{x_i} t < \deg_{x_i} u$. Then

$$\deg_{x_j}(tv) = \deg_{x_j} t + \deg_{x_j} v = \deg_{x_j} u + \deg_{x_j} v = \deg_{x_j} uv \quad \forall j = 1, 2, \ldots, i-1$$

and

$$\deg_{x_i}(tv) = \deg_{x_i} t + \deg_{x_i} v < \deg_{x_i} u + \deg_{x_i} v = \deg_{x_i} uv.$$

Hence $tv < uv$.

(D) is a special case of (B).

For (E), let $M \subset \mathbb{M}$. We proceed by induction on the number of variables n. *For the inductive base,* if $n = 1$ then the monomials are ordered according to the exponent on x_1, which is a natural number. Let E be the set of all exponents of the monomials in M; then $E \subset \mathbb{N}$. Recall that $\mathbb{N}$ is well-ordered. Hence E has a least element; call it e. By definition of E, e is the exponent of some monomial m of M. Since $e \leq \alpha$ for any other exponent $x^\alpha \in M$, m is a least element of M. *For the inductive hypothesis,* assume that for all $i < n$, the set of monomials in i variables is well-ordered. *For the inductive step,* let N be the set of all monomials in $n-1$

variables such that for each $t \in N$, there exists $m \in M$ such that $m = t \cdot x_n^e$ for some $e \in \mathbb{N}$. By the inductive hypothesis, N has a least element; call it t. Let

$$P = \left\{ t \cdot x_n^e : \ t \cdot x_n^e \in M \ \exists e \in \mathbb{N} \right\}.$$

All the elements of P are equal in the first $n-1$ variables: their exponents are the exponents of t. Let E be the set of all exponents of x_n for any monomial $u \in P$. As before, $E \subset \mathbb{N}$. Hence E has a least element; call it e. By definition of E, there exists $u \in P$ such that $u = t \cdot x_n^e$; since $e \leq \alpha$ for all $\alpha \in E$, u is a least element of P.

Finally, let $v \in M$. Since t is minimal in N, either there exists i such that

$$\deg_{x_j} u = \deg_{x_j} t = \deg_{x_j} v \quad \forall j = 1, 2, \ldots, i-1 \qquad \text{and} \qquad \deg_{x_i} u = \deg_{x_i} t < \deg_{x_i} v$$

or

$$\deg_{x_j} u = \deg_{x_j} t = \deg_{x_j} v \quad \forall j = 1, 2, \ldots, n-1$$

In the first case, $u < v$ by definition. Otherwise, since e is minimal in E,

$$\deg_{x_n} u = e \leq \deg_{x_n} v,$$

in which case $u \leq v$. Hence u is a least element of M.

Since M is arbitrary in $\mathbb{M}$, every subset of $\mathbb{M}$ has a least element. Hence $\mathbb{M}$ is well-ordered. □

Before we start looking for a triangular form of non-linear systems, let's observe one more thing.

Proposition 10.21: *Let p be a polynomial in the variables $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. If $\operatorname{lm}(p) = x_i^\alpha$, then every other monomial u of p has the form*

$$u = \prod_{j=i}^{n} x_j^{\beta_j}$$

for some $\beta_j \in \mathbb{N}$. In addition, $\beta_i < \alpha$.

PROOF: Assume that $\operatorname{lm}(p) = x_i^\alpha$. Let u be any monomial of p. Write

$$u = \prod_{j=1}^{n} x_j^{\beta_j}$$

for appropriate $\beta_j \in \mathbb{N}$. Since $u < \operatorname{lm}(p)$, the definition of the lexicographic ordering implies that

$$\deg_{x_j} u = \deg_{x_j} \operatorname{lm}(p) = \deg_{x_j} x_i^\alpha \quad \forall j = 1, 2, \ldots, i-1 \qquad \text{and} \qquad \deg_{x_i} u < \deg_{x_i} t.$$

Hence u has the form claimed. □

We now identify and generalize the properties of Proposition 10.20 to a generic ordering on monomials.

Definition 10.22: An **admissible ordering** $<$ on $\mathbb{M}$ is a relation that
(O1) is a linear ordering;
(O2) is a subordering of divisibility; and
(O3) is preserved by multiplication.

(The terms, "subordering with divisibility" and "preserved by multiplication" are identical to their description in Proposition 10.20.)

By definition, properties (B)–(D) of Proposition 10.20 hold for an admissible ordering. What of the others?

Proposition 10.23: *The following properties of an admissible ordering all hold.*
(A) $1 \leq t$ *for all* $t \in \mathbb{M}$.
(B) *The set* $\mathbb{M}$ *of all monomials over* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ *is well-ordered by any admissible ordering. That is, every subset* M *of* $\mathbb{M}$ *has a least element.*

PROOF: For (A), you do it! See Exercise 10.33. For (B), the argument is identical to Proposition 10.20—after all, we now have (O1)–(O3) and (A), which were used in Proposition 10.20. □

We can now introduce an ordering that you haven't seen before.

Definition 10.24: For a monomial t, the **total degree** of t is the sum of the exponents, denoted $\operatorname{tdeg}(t)$. For two monomials t, u, a **total-degree ordering** orders $t < u$ whenever $\operatorname{tdeg}(t) < \operatorname{tdeg}(u)$.

Example 10.25: The total degree of x^3y^2 is 5, and $x^3y^2 < xy^5$. ◿

However, a total degree ordering is not admissible, because not it does not satisfy (O1) for all pairs of monomials.

Example 10.26: We cannot order x^3y^2 and x^2y^3 by total degree alone, because $\operatorname{tdeg}(x^3y^2) = \operatorname{tdeg}(x^2y^3)$ but $x^3y^2 \neq x^2y^3$. ◿

When there is a tie in the total degree, we need to fall back on another method. An interesting way of doing this is the following.

Definition 10.27: For two monomials t, u the **graded reverse lexicographic ordering**, or **grevlex**, orders $t < u$ whenever
- $\operatorname{tdeg}(t) < \operatorname{tdeg}(u)$, or
- $\operatorname{tdeg}(t) = \operatorname{tdeg}(u)$ *and* there exists $i \in \{1, \ldots, n\}$ such that for all $j = i+1, \ldots, n$
  - $\deg_{x_j} t = \deg_{x_j} u$, and
  - $\deg_{x_i} t > \deg_{x_i} u$.

Notice that to break a total-degree tie, grevlex reverses the lexicographic ordering in a double way: it searches *backwards* for the *smallest* degree, and designates the winner as the larger monomial.

Example 10.28: Under grevlex, $x^3y^2 > x^2y^3$ because the total degrees are the same and $y^2 < y^3$. ◿

Theorem 10.29: *The graded reverse lexicographic ordering is an admissible ordering.*

PROOF: We have to show properties (O1)–(O3). Let $t, u \in \mathbb{M}$.

(O1) Assume $t \neq u$; by definition, there exists $i \in \mathbb{N}^+$ such that $\deg_{x_i} t \neq \deg_{x_i} u$. Choose the largest such i, so that $\deg_{x_j} t = \deg_{x_j} u$ for all $j = i+1, \ldots, n$. Then $t < u$ if $\deg_{x_i} t < \deg_{x_i} u$; otherwise $u < t$.

(O2) Assume $t \mid u$. By definition, $\deg_{x_i} t \leq \deg_{x_i} u$ for all $i = 1, \ldots, n$. If $t = u$, then we're done. Otherwise, $t \neq u$. If $\operatorname{tdeg}(t) > \operatorname{tdeg}(u)$, then the fact that the degrees are all natural numbers implies (see Exercise) that for some $i = 1, \ldots, n$ we have $\deg_{x_i} t > \deg_{x_i} u$, contradicting the hypothesis that $t \mid u$! Hence $\operatorname{tdeg}(t) = \operatorname{tdeg}(u)$. Since $t \neq u$, there exists $i \in \{1, \ldots, n\}$ such that $\deg_{x_i} t \neq \deg_{x_i} u$. Choose the largest such i, so that $\deg_{x_j} t = \deg_{x_j} u$ for $j = i+1, \ldots, n$. Since $t \mid u$, $\deg_{x_i} t < \deg_{x_i} u$, and $\deg_{x_j} t \leq \deg_{x_j} u$. Hence

$$\begin{aligned}
\operatorname{tdeg}(t) &= \sum_{j=1}^{i-1} \deg_{x_j} t + \deg_{x_i} t + \sum_{j=i+1}^{n} \deg_{x_j} t \\
&= \sum_{j=1}^{i-1} \deg_{x_j} t + \deg_{x_i} t + \sum_{j=i+1}^{n} \deg_{x_j} u \\
&\leq \sum_{j=1}^{i-1} \deg_{x_j} u + \deg_{x_i} t + \sum_{j=i+1}^{n} \deg_{x_j} u \\
&< \sum_{j=1}^{i-1} \deg_{x_j} u + \deg_{x_i} u + \sum_{j=i+1}^{n} \deg_{x_j} u \\
&= \operatorname{tdeg}(u).
\end{aligned}$$

Hence $t < u$.

(O3) Assume $t < u$, and let $v \in \mathbb{M}$. By definition, $\operatorname{tdeg}(t) < \operatorname{tdeg}(u)$ or there exists $i \in \{1, 2, \ldots, n\}$ such that $\deg_{x_i} t > \deg_{x_i} u$ and $\deg_{x_j} t = \deg_{x_j} u$ for all $j = i+1, \ldots, n$. In the first case, you will show in the exercises that

$$\operatorname{tdeg}(tv) = \operatorname{tdeg}(t) + \operatorname{tdeg}(v) < \operatorname{tdeg}(u) + \operatorname{tdeg}(v) = \operatorname{tdeg}(uv).$$

In the second,

$$\deg_{x_i} tv = \deg_{x_i} t + \deg_{x_i} v > \deg_{x_i} u + \deg_{x_i} v = \deg_{x_i} uv$$

while

$$\deg_{x_j} tv = \deg_{x_j} t + \deg_{x_j} v = \deg_{x_j} u + \deg_{x_j} v = \deg_{x_j} uv.$$

In either case, $tv < uv$ as needed. □

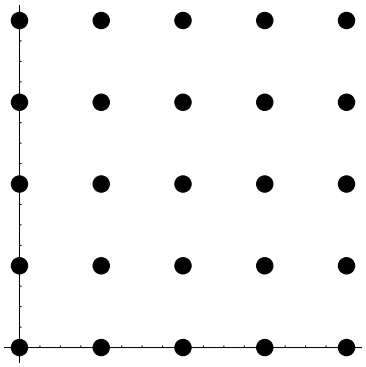
A useful tool when dealing with monomial orderings is a **monomial diagram**. These are most useful for monomials in a bivariate polynomial ring $\mathbb{F}[x,y]$, but we can often imagine important aspects of these diagrams in multivariate rings, as well. We discuss the bivariate case here.

Definition 10.30: Let $t \in \mathbb{M}$. Define the **exponent vector** $(\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$ where $\alpha_i = \deg_{x_i} t$.

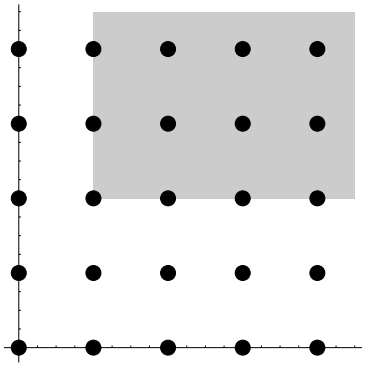
Let $t \in \mathbb{F}[x,y]$ be a monomial, and (α,β) its exponent vector. That is,

$$t = x^\alpha y^\beta.$$

We can consider (α,β) as a point in the x-y plane. If we do this with all the monomials of $\mathbb{M} \subset \mathbb{F}[x,y]$, and we obtain the following diagram:



This diagram is not especially useful, aside from pointing out that the monomial x^2 is the third point on the left in the bottom row, and the monomial 1 is the point in the lower left corner. What does make diagrams like this useful is the fact that if $t \mid u$, then the point corresponding to u lies above and/or to the right of the point corresponding to t, but *never* below or to the left of it. We often shade the points corresponding monomials divisible by a given monomial; for example, the points corresponding to monomials divisible by xy^2 lie within the shaded region of the following diagram:

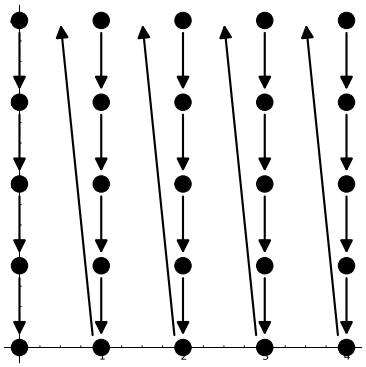


As we will see later, diagrams such as the one above can come in handy when visualizing certain features of an ideal.

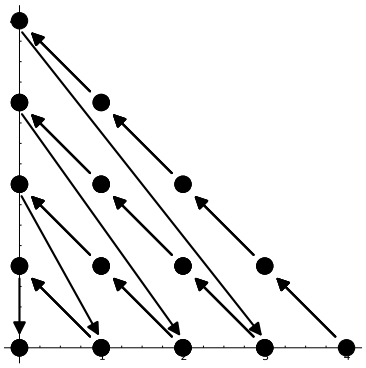
What interests us most for now is that we can sketch vectors on a monomial diagram that show the ordering of the monomials.

Example 10.31: We sketch monomial diagrams that show how lex and grevlex order $\mathbb{M}$. We already know that the smallest monomial is 1. The next smallest will always be y.

For the *lex* order, $y^a < x$ for *every* choice of $a \in \mathbb{N}$, no matter how large. Hence the next largest monomial is y^2, followed by y^3, etc. Once we have marked every power of y, the next largest monomial is x, followed by xy, by xy^2, etc., for $xy^a < x^2$ for all $a \in \mathbb{N}$. Continuing in this fashion, we have the following diagram:



With the *grevlex* order, by contrast, the next largest monomial after y is x, since $\text{tdeg}(x) < \text{tdeg}(y^2)$. After x come y^2, xy, and x^2, in that order, followed by the degree-three monomials y^2, xy^2, x^2y, and x^3, again in that order. This leads to the following monomial diagram:



These diagrams illustrate an important and useful fact.

Theorem 10.32: *Let $t \in \mathbb{M}$.*

(A) In the lexicographic order, there are infinitely many monomials smaller than t if and only if t is not a power of x_n alone.

(B) In the grevlex order, there are finitely many monomials smaller than t.

PROOF: You do it! See Exercise . □

Exercises.

Exercise 10.33: Show that for any admissible ordering and any $t \in \mathbb{M}$, $1 \leq t$.

Exercise 10.34: The **graded lexicographic order**, which we will denote by **gralex**, orders $t < u$ if

- $\text{tdeg}(t) < \text{tdeg}(u)$, or
- $\text{tdeg}(t) = \text{tdeg}(u)$ and the lexicographic ordering would place $t < u$.

(a) Order x^2y, xy^2, and z^5 by gralex.
(b) Show that gralex is an admissible order.
(d) Sketch a monomial diagram that shows how gralex orders $\mathbb{M}$.

Exercise 10.35: Prove Theorem 10.32.

10.3: Matrix representations of monomial orderings

Aside from lexicographic and graded reverse lexicographic orderings, there are limitless ways to design an admissible ordering.

Definition 10.36: Let $M \in \mathbb{R}^{n \times n}$. We define the **weighted vector** $w(t) = M\mathbf{t}$.

Example 10.37: Consider the matrix

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ & & & & -1 \\ & & & -1 & \\ & & \cdots & & \\ & -1 & & & \end{pmatrix}$$

where the empty entries are zeroes. We claim that M represents the grevlex ordering, and weighted vectors computed with M can be read from top to bottom, where the first entry that does not tie determines the larger monomial.

Why? The top row of M adds all the elements of the exponent vector, so the top entry of the weighted vector is the total degree of the monomial. Hence if the two monomials have different total degrees, the top entry of the weighted vector determines the larger monomial. In case they have the same total degree, the second entry of $M\mathbf{t}$ contains $-\deg_{x_n} t$, so if they have different degree in the smallest variable, the second entry determines the larger variables. And so forth.

The monomials $t = x^3y^2$, $u = x^2y^3$, and $v = xy^5$ have exponent vectors $\mathbf{t} = (3,2)$, $\mathbf{u} = (2,3)$, and $\mathbf{v} = (1,5)$, respectively. We have

$$M\mathbf{t} = \begin{pmatrix} 5 \\ -2 \end{pmatrix}, \qquad M\mathbf{u} = \begin{pmatrix} 5 \\ -3 \end{pmatrix}, \qquad M\mathbf{v} = \begin{pmatrix} 6 \\ -5 \end{pmatrix},$$

from which we conclude that $v > t > u$. ◿

Not all matrices can represent admissible orderings. It would be useful to know in advance which ones do.

Theorem 10.38: *Let $M \in \mathbb{R}^{m\times m}$. The following are equivalent.*
(A) M represents a admissible ordering.
(B) Each of the following holds:
(MO1) Its rows are linearly independent over $\mathbb{Z}$.
(MO2) The topmost nonzero entry in each column is positive.

To prove the theorem, we need the following lemma.

Lemma 10.39: *If a matrix M satisfies (B) of Theorem 10.38, then there exists a matrix N that satisfies (B), whose entries are all nonnegative, and for all $\mathbf{t} \in \mathbb{Z}^n$ comparison from top to bottom implies that $N\mathbf{t} > N\mathbf{u}$ if and only if $M\mathbf{t} > M\mathbf{u}$.*

Example 10.40: In Example 10.37, we saw that grevlex could be represented by

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ & & & & -1 \\ & & & -1 & \\ & & \cdots & & \\ & -1 & & & \end{pmatrix}.$$

However, it can also be represented by

$$N = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 & \\ & \cdots & & & \\ 1 & 1 & & & \\ 1 & & & & \end{pmatrix}$$

where the empty entries are, again, zeroes. Notice that the first row operates exactly the same, while the second row adds all the entries *except the last*. If $t_n < y_n$ then from $t_1 + \cdots + t_n = u_1 + \cdots + u_n$ we infer that $t_1 + \cdots + t_{n-1} > u_1 + \cdots + u_{n-1}$, so the second row of $N\mathbf{t}$ and $N\mathbf{u}$ would break the tie in exactly the same way as the second row of $M\mathbf{t}$ and $M\mathbf{u}$. And so forth.

In addition, notice that we can obtain N by adding row 1 of M to row 2 of M, then adding the modified row 2 of M to the modified row 3, and so forth. ◿

PROOF: Let $M \in \mathbb{R}^{n\times n}$ satisfy (B) of Theorem 10.38. Construct N in the following way by building matrices $M_0, M_1, \ldots$ in the following way. Let $M_1 = M$. Suppose that $M_1, M_2, \ldots, M_{i-1}$ all have nonnegative entries in rows 1, 2, etc. but M has a negative entry α in row i, column j. The topmost nonzero entry β of column j in M_{i-1} is positive; say it is in row k. Use the Archimedean property of $\mathbb{R}$ to find $K \in \mathbb{N}^+$ such that $K\beta \geq |\alpha|$, and add K times row k of M_{i-1}

to row j. The entry in row i and column j of M_i is now nonnegative, and if there were other negative values in row i of M_i, the fact that row k of M_{i-1} contained nonnegative entries implies that the absolute values of these negative entries are no larger than before, so we can repeat this on each entry. Since there is a finite number of entries in each row, and a finite number of rows in M, this process does not continue indefinitely, and terminates with a matrix N whose entries are all nonnegative.

In addition, we can write the ith row $N_{(i)}$ of N as

$$N_{(i)} = K_1 M_{(1)} + K_2 M_{(2)} + \cdots + K_i M_{(i)}$$

where $M_{(k)}$ indicates the kth row of M. For any $\mathbf{t} \in \mathbb{M}$, the ith entry of $N\mathbf{t}$ is therefore

$$N_{(i)}\mathbf{t} = \left(K_1 M_{(1)} + K_2 M_{(2)} + \cdots + K_i M_{(i)}\right)\mathbf{t} = K_1\left(M_{(1)}\mathbf{t}\right) + K_2\left(M_{(2)}\mathbf{t}\right) + \cdots + K_i\left(M_{(i)}\mathbf{t}\right).$$

We see that if $M_{(1)}\mathbf{t} = \cdots = M_{(i-1)}\mathbf{t} = 0$ and $M_{(i)}\mathbf{t} = \alpha \neq 0$, then $N_{(1)}\mathbf{t} = \cdots = N_{(i-1)}\mathbf{t} = 0$ and $N_{(i)}\mathbf{t} = K_i\alpha \neq 0$. Hence $N\mathbf{t} > N\mathbf{u}$ if and only if $M\mathbf{t} > M\mathbf{u}$. □

Now we can prove Theorem 10.38.

PROOF OF THEOREM 10.38: *That (A) implies (B):* Assume that M represents an admissible ordering. For (MO2), observe that the monomial 1 has the exponent vector $\mathbf{t} = (0,\ldots,0)$ and the monomial x_i has the exponent vector $\mathbf{u}$ with zeroes everywhere except in the ith position. The product $M\mathbf{t} > M\mathbf{u}$ if the ith element of the top row of M is negative, but this contradicts Proposition 10.23(A). For (MO1), observe that property (O1) of Definition 10.22 implies that no pair of distinct monomials can produce the same weighted vector. Hence the rows of M are linearly independent over $\mathbb{Z}$.

That (B) implies (A): Assume that M satisfies (B); thus it satisfies (MO1) and (MO2). We need to show that properties (O1)–(O3) of Definition 10.22 are satisfied.

(O1): Since the rows of M are linearly independent over $\mathbb{Z}$, every pair of monomials t and u produces a pair of distinct weighted vectors $M\mathbf{t}$ and $M\mathbf{u}$ if and only if $t \neq u$. Reading these vectors from top to bottom allows us to decide whether $t > u$, $t < u$, or $t = u$.

(O2): This follows from linear algebra. Let $t, u \in \mathbb{M}$, and assume that $t \mid u$. Then $\deg_{x_i} t \leq \deg_{x_i} u$ for all $i = 1, 2, \ldots, n$. In the exponent vectors $\mathbf{t}$ and $\mathbf{u}$, $t_i \leq u_i$ for each i. Let $\mathbf{v} \in \mathbb{N}^n$ such that $\mathbf{u} = \mathbf{t} + \mathbf{v}$; then

$$M\mathbf{u} = M(\mathbf{t} + \mathbf{v}) = M\mathbf{t} + M\mathbf{v}.$$

From Lemma 10.39 we can assume that the entries of M are all nonnegative. Thus the entries of $M\mathbf{u}$, $M\mathbf{t}$, and $M\mathbf{v}$ are also nonnegative. Thus the topmost nonzero entry of $M\mathbf{v}$ is positive, and $M\mathbf{u} > M\mathbf{t}$.

(O3): This is similar to (O2), so we omit it. □

In the Exercises you will find other matrices that represent term orderings, some of them somewhat exotic.

Exercises

Exercise 10.41: Find a matrix that represents (a) the lexicographic term ordering, and (b) the gralex ordering.

Exercise 10.42: Explain why the matrix

$$M = \begin{pmatrix} 1 & 1 & & & & & & \\ 1 & 1 & 1 & & & & & \\ 1 & 1 & 1 & 1 & & & & \\ -1 & & & & & & & \\ & & & & 1 & 1 & 1 & 1 \\ & & & & & 1 & 1 & 1 \\ & & & & & & 1 & 1 \\ & & & & & & & -1 \end{pmatrix}$$

represents an admissible ordering. Use M to order the monomials

$$x_1x_3^2x_4x_6, \quad x_1x_4^8x_7, \quad x_2x_3^2x_4x_6, \quad x_8, \quad ,x_8^2, \quad x_7x_8.$$

Exercise 10.43: Suppose you know nothing about an admissible order $<$ on $\mathbb{F}[x,y]$ except that $x > y$ and $x^2 < y^3$. Find a matrix that represents this order.

10.4: The structure of a Gröbner basis

When we consider the non-linear case, things become a little more complicated. Consider the following system of equations:

$$\begin{aligned} x^2 + y^2 &= 4 \\ xy &= 1. \end{aligned}$$

We can visualize the real solutions to this system; see Figure 10.1 on the next page. The common solutions occur wherever the circle and the hyperbola intersect. We see four intersections in the real plane; one of them is hilighted with a dot.

However, we don't know if complex solutions exist. In addition, plotting equations involving more than two variables is difficult, and more than three is effectively impossible. Finally, while it's relatively easy to solve the system given above, it isn't a "triangular" system in the sense that the last equation is only in one variable. So we can't solve for one variable immediately and then go backwards. We can solve for y in terms of x, but not for an exact value of y.

It gets worse! Although the system is triangular in a "linear" sense, it is not triangular in a non-linear sense: we can multiply the two polynomials above by monomials and obtain a new

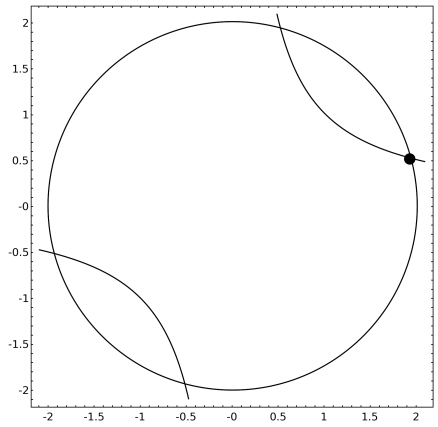


Figure 10.1. Plots of $x^2 + y^2 = 4$ and $xy = 1$

polynomial that isn't obviously spanned by either of these two:

$$y\left(x^2 + y^2 - 4\right) - x\left(xy - 1\right) = x + y^3 - 4y. \tag{27}$$

None of the terms of this new polynomial appears in either of the original polynomials. This sort of thing does *not* happen in the linear case, largely because

- cancellation of *variables* can be resolved using *scalar multiplication*, hence in a vector space; but
- cancellation of *terms* cannot be resolved without *monomial multiplication*, hence it requires an ideal.

So we need to find a "triangular form" for non-linear systems.

Let's rephrase this problem in the language of rings and ideals. The primary issue we would like to resolve is the one that we remarked immediately after computing the subtraction polynomial of equation (27): we built a polynomial p whose leading term x was not divisible by the leading term of either the hyperbola (xy) or the circle (x^2). When we built p, we used operations of the polynomial ring that allowed us to remain within the ideal generated by the hyperbola and the circle. That is,

$$p = x + y^3 - 4y = y\left(x^2 + y^2 - 4\right) - x\left(xy - 1\right);$$

by Theorem 8.10 ideals absorb multiplication and are closed under subtraction, so

$$p \in \left\langle x^2 + y^2 - 4, xy - 1 \right\rangle.$$

So one problem appears to be that p is in the ideal, but its leading monomial is not divisible by the leading monomials of the ideal's basis. Let's define a special kind of idael basis that will not give us this problem.

Definition 10.44: Let $\{g_1, g_2, \ldots, g_m\}$ be a basis of an ideal I; that is, $I = \langle g_1, g_2, \ldots, g_m \rangle$. We say that $G = (g_1, g_2, \ldots, g_m)$ is a **Gröbner basis of** I if for every $p \in I$, $\operatorname{lm}(g_k) \mid \operatorname{lm}(p)$ for some $k \in \{1, 2, \ldots, m\}$.

It isn't obvious at the moment how we can decide that any given basis forms a Gröbner basis, because there are infinitely many polynomials that we'd have to check. However, we can certainly determine that the list

$$\left(x^2 + y^2 - 4, xy - 1\right)$$

is *not* a Gröbner basis, because we found a polynomial in its ideal that violated the definition of a Gröbner basis: $x + y^3 - 4y$.

How did we find that polynomial? We built a *subtraction polynomial* that was calculated in such a way as to "raise" the polynomials to the lowest level where their leading monomials would cancel! Let t, u be monomials in the variables $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Write $t = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ and $u = x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$. Any common multiple of t and u must have the form

$$v = x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_n^{\gamma_n}$$

where $\gamma_i \geq \alpha_i$ and $\gamma_i \geq \beta_i$ for each $i = 1, 2, \ldots, n$. We can thus identify a **least common multiple** $\operatorname{lcm}(t, u) = x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_n^{\gamma_n}$ where $\gamma_i = \max(\alpha_i, \beta_i)$ for each $i = 1, 2, \ldots, n$. It really is the *least* because no common multiple can have a smaller degree in any of the variables, and so it is smallest by the definition of the lexicographic ordering.

Lemma 10.45: *For any two polynomials $p, q \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, with $\operatorname{lm}(p) = t$ and $\operatorname{lm}(q) = u$, we can build a polynomial in the ideal of p and q that would raise the leading terms to the smallest level where they would cancel by computing*

$$S = \operatorname{lc}(q) \cdot \frac{\operatorname{lcm}(t, u)}{t} \cdot p - \operatorname{lc}(p) \cdot \frac{\operatorname{lcm}(t, u)}{u} \cdot q.$$

Moreover, for all other monomials τ, μ and $a, b \in \mathbb{F}$, if $a\tau p - b\mu q$ cancels the leading terms of τp and μq, then it is a multiple of S.

PROOF: First we show that the leading monomials of the two polynomials in the subtraction cancel. By Proposition 10.20,

$$\operatorname{lm}\left(\frac{\operatorname{lcm}(t, u)}{t} \cdot p\right) = \frac{\operatorname{lcm}(t, u)}{t} \cdot \operatorname{lm}(p) = \frac{\operatorname{lcm}(t, u)}{t} \cdot t = \operatorname{lcm}(t, u);$$

likewise

$$\operatorname{lm}\left(\frac{\operatorname{lcm}(t, u)}{u} \cdot q\right) = \frac{\operatorname{lcm}(t, u)}{u} \cdot \operatorname{lm}(q) = \frac{\operatorname{lcm}(t, u)}{u} \cdot u = \operatorname{lcm}(t, u).$$

Thus

$$\operatorname{lc}\left(\operatorname{lc}(q)\cdot\frac{\operatorname{lcm}(t,u)}{t}\cdot p\right)=\operatorname{lc}(q)\cdot\operatorname{lc}(p)$$

and

$$\operatorname{lc}\left(\operatorname{lc}(p)\cdot\frac{\operatorname{lcm}(t,u)}{t}\cdot q\right)=\operatorname{lc}(p)\cdot\operatorname{lc}(q).$$

Hence the leading monomials of the two polynomials in S cancel.

Let τ,μ be monomials over $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ and $a,b\in\mathbb{F}$ such that the leading monomials of the two polynomials in $a\tau p-b\mu q$ cancel. Let $\tau=x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ and $\mu=x_1^{\beta_1}\cdots x_n^{\beta_n}$ for appropriate α_i and β_i in $\mathbb{N}$. Write $\operatorname{lm}(p)=x_1^{\zeta_1}\cdots x_n^{\zeta_n}$ and $\operatorname{lm}(q)=x_1^{\omega_1}\cdots x_n^{\omega_n}$ for appropriate ζ_i and ω_i in $\mathbb{N}$. The leading monomials of $a\tau p-b\mu q$ cancel, so for each $i=1,2,\ldots,n$

$$\alpha_i+\zeta_i=\beta_i+\omega_i.$$

We have

$$\alpha_i=\beta_i+(\omega_i-\zeta_i).$$

Thus

$$\begin{aligned}\alpha_i-(\max(\zeta_i,\omega_i)-\zeta_i)&=[(\beta_i+(\omega_i-\zeta_i))-(\max(\zeta_i,\omega_i)-\zeta_i)]\\&=\beta_i-(\max(\zeta_i,\omega_i)-\omega_i).\end{aligned}$$

Let $\eta_i=\alpha_i-(\max(\zeta_i,\omega_i)-\zeta_i)$ and let

$$v=\prod_{i=1}^{n}x_i^{\eta_i}.$$

Then

$$a\tau p-b\mu q=v\left(a\cdot\frac{\operatorname{lcm}(t,u)}{t}\cdot p-b\cdot\frac{\operatorname{lcm}(t,u)}{u}\cdot q\right),$$

as claimed. □

The subtraction polynomial of Lemma 10.45 is important enough that we give it a special name.

Definition 10.46: Let $p,q\in\mathbb{F}[x_1,x_2,\ldots,x_n]$. We define the **$S$-polynomial of p and q with respect to the lexicographic ordering** to be

$$\operatorname{Spol}(p,q)=\operatorname{lc}(q)\cdot\frac{\operatorname{lcm}(\operatorname{lm}(p),\operatorname{lm}(q))}{\operatorname{lm}(p)}\cdot p-\operatorname{lc}(p)\cdot\frac{\operatorname{lcm}(\operatorname{lm}(p),\operatorname{lm}(q))}{\operatorname{lm}(q)}\cdot q.$$

It should be clear from the discussion above the definition that S-poly-nomials capture the cancellation of leading monomials. In fact, they are a natural generalization of the cancellation used

in Algorithm 7, Gaussian elimination, to obtain the triangular form of a linear system. In the same way, we need to generalize the notion that cancellation does not introduce any new leading variables. In our case, we have to make sure that cancellation does not introduce any new leading terms. We introduce the notion of top-reduction for this.

Definition 10.47: Let $p, q \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. If $\operatorname{lm}(p)$ divides $\operatorname{lm}(q)$, then we say that p **top-reduces** q.
If p top-reduces q, let $t = \operatorname{lm}(q)/\operatorname{lm}(p)$ and $c = \operatorname{lc}(q)/\operatorname{lc}(p)$. Let $r = q - ct \cdot p$; we say that p **top-reduces** q **to** r.
Finally, let $F = (f_1, f_2, \ldots, f_m)$ be a list of polynomials in $\mathbb{F}[x_1, x_2, \ldots, x_n]$, and $r_1, r_2, \ldots, r_k \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that

- some polynomial of F top-reduces p to r_1,
- some polynomial of F top-reduces r_1 to r_2,
- $\ldots$
- some polynomial of F top-reduces r_{k-1} to r_k.

In this case, we say that p **top-reduces to** r_k **with respect to** F.

Example 10.48: Let $p = x + 1$ and $q = x^2 + 1$. We have $\operatorname{lm}(p) = x$ and $\operatorname{lm}(q) = x^2$. Since $\operatorname{lm}(p)$ divides $\operatorname{lm}(q)$, p top-reduces q. Let $t = \frac{x^2}{x} = x$ and $c = \frac{1}{1} = 1$; we see that p top-reduces q to $r = q - 1 \cdot x \cdot p = -x + 1$. ◿

Remark 10.49: Observe that top-reduction is a kind of S-polynomial computation. To see this, write $\operatorname{lm}(p) = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $\operatorname{lm}(q) = x_1^{\beta_1} \cdots x_n^{\beta_n}$. Since $\operatorname{lm}(p)$ divides $\operatorname{lm}(q)$, $\alpha_i \leq \beta_i$ for each i. Thus $\operatorname{lcm}(\operatorname{lm}(q), \operatorname{lm}(p)) = \operatorname{lm}(p)$. Let $t = \frac{\operatorname{lm}(q)}{\operatorname{lm}(p)}$ and $c = \frac{\operatorname{lc}(q)}{\operatorname{lc}(p)}$; substitution gives us

$$\begin{aligned}
\operatorname{Spol}(q, p) &= \operatorname{lc}(p) \cdot \frac{\operatorname{lm}(q)}{\operatorname{lm}(q)} \cdot q - \operatorname{lc}(q) \cdot \frac{\operatorname{lm}(q)}{\operatorname{lm}(p)} \cdot p \\
&= \operatorname{lc}(p) \cdot q - \frac{\operatorname{lc}(p)}{\operatorname{lc}(p)} \cdot \operatorname{lc}(q) \cdot t \cdot p \\
&= \operatorname{lc}(p) \cdot (q - ct \cdot p)
\end{aligned}$$

where $q - ct \cdot p$ is the ordinary top-reduction of q by p. Thus top-reduction is a scalar multiple of an S-polynomial.

We will need the following properties of polynomial operations.

Proposition 10.50: *Let $p, q, r \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Each of the following holds:*

(A) $\operatorname{lm}(pq) = \operatorname{lm}(p) \cdot \operatorname{lm}(q)$
(B) $\operatorname{lm}(p \pm q) \leq \max(\operatorname{lm}(p), \operatorname{lm}(q))$
(C) $\operatorname{lm}(\operatorname{Spol}(p, q)) < \operatorname{lcm}(\operatorname{lm}(p), \operatorname{lm}(q))$
(D) *If p top-reduces q to r, then* $\operatorname{lm}(r) < \operatorname{lm}(q)$.

PROOF: For convenience, write $t = \operatorname{lm}(p)$ and $u = \operatorname{lm}(q)$.

(A) Any monomial of pq can be written as the product of two monomials vw, where v is a monomial of p and w is a monomial of q. If $v \neq \operatorname{lm}(p)$, then the definition of a leading monomial implies that $v < t$. Proposition 10.20 implies that

$$vw \leq tw,$$

with equality only if $v = t$. The same reasoning implies that

$$vw \leq tw \leq tu,$$

with equality only if $w = u$. Hence $\operatorname{lm}(pq) = tu = \operatorname{lm}(p)\operatorname{lm}(q)$.

(B) Any monomial of $p \pm q$ is also a monomial of p or a product of q. Hence $\operatorname{lm}(p \pm q)$ is a monomial of p or of q. The maximum of these is $\max(\operatorname{lm}(p), \operatorname{lm}(q))$. Hence $\operatorname{lm}(p \pm q) \leq \max(\operatorname{lm}(p), \operatorname{lm}(q))$.

(C) Definition 10.46 and (B) imply that $\operatorname{lm}(\operatorname{Spol}(p,q)) < \operatorname{lcm}(\operatorname{lm}(p), \operatorname{lm}(q))$.

(D) Assume that p top-reduces q to r. Top-reduction is a special case of of an S-polynomial; that is, $r = \operatorname{Spol}(p,q)$. Here $\operatorname{lcm}(\operatorname{lm}(p), \operatorname{lm}(q)) = \operatorname{lm}(q)$, and (C) implies that $\operatorname{lm}(r) < \operatorname{lm}(q)$. □

In a triangular linear system, we achieve a triangular form by rewriting all polynomials that share a leading variable. In the *linear* case we can accomplish this using *scalar multiplication*, requiring nothing else. In the non-linear case, we need to check for divisibility of monomials. The following result should, therefore, not surprise you very much.

Theorem 10.51 (Buchberger's characterization): *Let $g_1, g_2, \ldots, g_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. The following are equivalent.*

(A) *$G = (g_1, g_2, \ldots, g_m)$ is a Gröbner basis of the ideal $I = \langle g_1, g_2, \ldots, g_m \rangle$.*

(B) *For any pair i, j with $1 \leq i < j \leq m$, $\operatorname{Spol}\left(g_i, g_j\right)$ top-reduces to zero with respect to G.*

Example 10.52: Recall two systems considered at the beginning of this chapter,

$$F = \left(x^2 + y^2 - 4, xy - 1\right)$$

and

$$G = \left(x^2 + y^2 - 4, xy - 1, x + y^3 - 4y, -y^4 + 4y^2 - 1\right).$$

Is either of these a Gröbner basis?

- Certainly F is not; we already showed that the one S-polynomial is

$$S = \operatorname{Spol}(f_1, f_2) = y\left(x^2 + y^2 - 4\right) - x(xy - 1) = x + y^3 - 4y;$$

this does not top-reduce to zero because $\operatorname{lm}(S) = x$, and neither leading term of F divides this.

- On the other hand, G is a Gröbner basis. We will not show all six S-polynomials (you will verify this in Exercise 10.55), but

$$\operatorname{Spol}(g_1, g_2) - g_3 = 0,$$

so the problem with F does not reappear. It is also worth noting that when G top-reduces $\operatorname{Spol}(g_1, g_4)$, we derive the following equation:

$$\operatorname{Spol}(g_1, g_4) - \left(4y^2 - 1\right) g_1 + \left(y^2 - 4\right) g_4 = 0.$$

If we rewrite $\operatorname{Spol}(g_1, g_4) = y^4 g_1 + x^2 g_4$ and substitute it into the above equation, something very interesting turns up:

$$\begin{aligned} \left(y^4 g_1 + x^2 g_4\right) - \left(4y^2 - 1\right) g_1 + \left(y^2 - 4\right) g_4 &= 0 \\ -\left(-y^4 + 4y^2 - 1\right) g_1 + \left(x^2 + y^2 - 4\right) g_4 &= 0 \\ -g_4 g_1 + g_1 g_4 &= 0. \end{aligned}$$

◿

Remark 10.53: Example 10.52 suggests a method to compute a Gröbner basis of an ideal: given a basis, use S-polynomials to find elements of the ideal that do not satisfy Definition 10.44; then keep adding these to the basis until all of them reduce to zero. Eventually, this is exactly what we will do, but until then there are two problems with acknowledging it:

- We don't know that a Gröbner basis exists for every ideal. For all we know, there may be ideals for which no Gröbner basis exists.
- We don't know that the proposed method will even terminate! It could be that we can go on forever, adding new polynomials to the ideal without ever stopping.

We resolve these questions in the following section.

It remains to prove Theorem 10.51, but before we can do that we will need the following useful lemma. While small, it has important repercussions later.

Lemma 10.54: *Let $p, f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Let $F = (f_1, f_2, \ldots, f_m)$. Then (A) implies (B) where*

(A) *p top-reduces to zero with respect to F.*

(B) *There exist $q_1, q_2, \ldots, q_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that each of the following holds:*

(B1) *$p = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$; and*

(B2) *For each $k = 1, 2, \ldots, m$, $q_k = 0$ or $\operatorname{lm}(q_k)\operatorname{lm}(g_k) \leq \operatorname{lm}(p)$.*

PROOF: You do it! See Exercise 10.61. □

You will see in the following that Lemma 10.54allows us to replace polynomials that are "too large" with smaller polynomials. This allows us to obtain the desired form.

PROOF OF THEOREM 10.51: *That (A) ⇒ (B):* Assume that G is a Gröbner basis, and let i, j be such that $1 \leq i < j \leq m$. Then

$$\operatorname{Spol}\left(g_i, g_j\right) \in \left\langle g_i, g_j \right\rangle \subset \langle g_1, g_2, \ldots, g_m \rangle,$$

and the definition of a Gröbner basis implies that there exists $k_1 \in \{1, 2, \ldots, m\}$ such that g_{k_1} top-reduces $\operatorname{Spol}\left(g_i, g_j\right)$ to a new polynomial, say r_1. The definition further implies that if r_1 is not zero, then there exists $k_2 \in \{1, 2, \ldots, m\}$ such that g_{k_2} top-reduces r_1 to a new polynomial, say r_2. Repeating this iteratively, we obtain a chain of polynomials $r_1, r_2, \ldots$ such that r_ℓ top-reduces to $r_{\ell+1}$ for each $\ell \in \mathbb{N}$. From Proposition 10.50, we see that

$$\operatorname{lm}(r_1) > \operatorname{lm}(r_2) > \cdots.$$

Recall that the set of all monomials over $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is well-ordered, so any set of monomials over $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ has a least element. This includes the set $R = \{\operatorname{lm}(r_1), \operatorname{lm}(r_2), \ldots\}$! Thus the chain of top-reductions cannot continue indefinitely. It cannot conclude with a non-zero polynomial r_{last}, since: □

- top-reduction keeps each r_ℓ in the ideal:
  - subtraction by the subring property, and
    - multiplication by the absorption property; hence
  - by the definition of a Gröbner basis, a non-zero r_{last} would be top-reducible by some element of G.

PROOF: The chain of top-reductions must conclude with zero, so $\operatorname{Spol}\left(g_i, g_j\right)$ top-reduces to zero.

That (A) ⇐ (B): Assume (B). We want to show (A); that is, any element of I is top-reducible by an element of G. So let $p \in I$; by definition, there exist polynomials $h_1, \ldots, h_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that

$$p = h_1 g_1 + \cdots + h_m g_m.$$

For each i, write $t_i = \operatorname{lm}(g_i)$ and $u_i = \operatorname{lm}(h_i)$. Let $T = \max_{i=1,2,\ldots,m}(u_i t_i)$. We call T the **maximal term of the representation** $h_1, h_2, \ldots, h_m$. If $\operatorname{lm}(p) = T$, then we are done, since

$$\operatorname{lm}(p) = T = u_k t_k = \operatorname{lm}(h_k)\operatorname{lm}(g_k) \quad \exists k \in \{1, 2, \ldots, m\}.$$

Otherwise, there must be some cancellation among the leading monomials of each polynomial in the sum on the right hand side. That is,

$$T = \operatorname{lm}\left(h_{\ell_1} g_{\ell_1}\right) = \operatorname{lm}\left(h_{\ell_2} g_{\ell_2}\right) = \cdots = \operatorname{lm}\left(h_{\ell_s} g_{\ell_s}\right)$$

for some $\ell_1, \ell_2, \ldots, \ell_s \in \{1, 2, \ldots, m\}$. From Lemma 10.45, we know that we can write the sum

of these leading terms as a sum of multiples of a S-polynomials of G. That is,

$$\operatorname{lc}\left(h_{\ell_1}\right)\operatorname{lm}\left(h_{\ell_1}\right)g_{\ell_1}+\cdots+\operatorname{lc}\left(h_{\ell_s}\right)\operatorname{lm}\left(h_{\ell_s}\right)g_{\ell_s}=\sum_{1\leq a<b\leq s}c_{a,b}u_{a,b}\operatorname{Spol}\left(g_{\ell_a},g_{\ell_b}\right)$$

where for each a,b we have $c_{a,b}\in\mathbb{F}$ and $u_{a,b}\in\mathbb{M}$. Let

$$S=\sum_{1\leq a<b\leq s}c_{a,b}u_{a,b}\operatorname{Spol}\left(g_{\ell_a},g_{\ell_b}\right).$$

Observe that

$$\left[\operatorname{lm}\left(h_{\ell_1}\right)g_{\ell_1}+\operatorname{lm}\left(h_{\ell_2}\right)g_{\ell_2}+\cdots+\operatorname{lm}\left(h_{\ell_s}\right)g_{\ell_s}\right]-S=0. \tag{28}$$

By (B), we know that each S-polynomial of S top-reduces to zero. This fact, Lemma 10.54 and Proposition 10.50, implies that for each a,b we can find $q_\lambda^{(a,b)}\in\mathbb{F}[x_1,x_2,\ldots,x_n]$ such that

$$\operatorname{Spol}\left(g_{\ell_a},g_{\ell_b}\right)=q_1^{(a,b)}g_1+\cdots+g_m^{(a,b)}g_m$$

and for each $\lambda=1,2,\ldots,m$ we have $q_\lambda^{(a,b)}=0$ or

$$\operatorname{lm}\left(q_\lambda^{(a,b)}\right)\operatorname{lm}\left(g_\lambda\right)\leq\operatorname{lm}\left(\operatorname{Spol}\left(g_{\ell_a},g_{\ell_b}\right)\right)<\operatorname{lcm}\left(\operatorname{lm}\left(g_{\ell_a}\right),\operatorname{lm}\left(g_{\ell_b}\right)\right). \tag{29}$$

Let $Q_1,Q_2,\ldots,Q_m\in\mathbb{F}[x_1,x_2,\ldots,x_n]$ such that

$$Q_k=\begin{cases}\sum_{1\leq a<b\leq s}c_{a,b}u_{a,b}q_k^{(a,b)}, & k\in\{\ell_1,\ldots,\ell_s\};\\ 0, & \text{otherwise.}\end{cases}$$

Then

$$S=Q_1g_1+Q_2g_2+\cdots+Q_mg_m.$$

In other words,

$$S-(Q_1g_1+Q_2g_2+\cdots+Q_mg_m)=0.$$

By equation (29) and Proposition 10.50, for each $k=1,2,\ldots,m$ we have $Q_k=0$ or

$$\begin{aligned}\operatorname{lm}\left(Q_k\right)\operatorname{lm}\left(g_k\right)&\leq\max_{1\leq a<b\leq s}\left\{\left[u_{a,b}\operatorname{lm}\left(q_k^{(a,b)}\right)\right]\operatorname{lm}\left(g_k\right)\right\}\\&=\max_{1\leq a<b\leq s}\left\{u_{a,b}\left[\operatorname{lm}\left(q_k^{(a,b)}\right)\operatorname{lm}\left(g_k\right)\right]\right\}\\&\leq\max_{1\leq a<b\leq s}\left\{u_{a,b}\operatorname{lm}\left(\operatorname{Spol}\left(g_{\ell_a},g_{\ell_b}\right)\right)\right\}\\&<u_{a,b}\operatorname{lcm}\left(\operatorname{lm}\left(g_{\ell_a}\right),\operatorname{lm}\left(g_{\ell_b}\right)\right)\\&=T.\end{aligned} \tag{30}$$

By substitution,

$$\begin{aligned} p &= (h_1 g_1 + h_2 g_2 + \cdots + h_m g_m) - \left(S - \sum_{k \in \{\ell_1, \ldots, \ell_s\}} Q_k g_k \right) \\ &= \left[\sum_{k \notin \{\ell_1, \ldots, \ell_s\}} h_k g_k + \sum_{k \in \{\ell_1, \ldots, \ell_s\}} (h_k - \operatorname{lc}(h_k) \operatorname{lm}(h_k)) g_k \right] \\ &\quad + \left[\sum_{k \in \{\ell_1, \ldots, \ell_s\}} \operatorname{lc}(h_k) \operatorname{lm}(h_k) g_k - S \right] \\ &\quad + \sum_{k \in \{\ell_1, \ldots, \ell_s\}} Q_k g_k. \end{aligned}$$

Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that

$$\mathcal{Q}_k(x) = \begin{cases} h_k, & k \notin \{\ell_1, \ldots, \ell_s\}; \\ h_k - \operatorname{lc}(h_k) \operatorname{lm}(h_k) + Q_k, & \text{otherwise.} \end{cases}$$

By susbtitution,

$$p = \mathcal{Q}_1 g_1 + \cdots + \mathcal{Q}_m g_m.$$

If $k \notin \{\ell_1, \ldots, \ell_s\}$, then the choice of T as the maximal term of the representation implies that

$$\operatorname{lm}(\mathcal{Q}_k) \operatorname{lm}(g_k) = \operatorname{lm}(h_k) \operatorname{lm}(g_k) < T.$$

Otherwise, Proposition 10.50 and equation (30) imply that

$$\operatorname{lm}(\mathcal{Q}_k) \operatorname{lm}(g_k) \leq \max((\operatorname{lm}(h_k - \operatorname{lc}(h_k) \operatorname{lm}(h_k)), \operatorname{lm}(Q_k)) \operatorname{lm}(g_k)) < \operatorname{lm}(h_k) \operatorname{lm}(g_k) = T.$$

What have we done? We have rewritten the original representation of p over the ideal, which had maximal term T, with another representation, which has maximal term smaller than T. This was possible because all the S-polynomials reduced to zero; S-polynomials appeared because $T > \operatorname{lm}(p)$, implying cancellation in the representation of p over the ideal. We can repeat this as long as $T > \operatorname{lm}(p)$, generating a list of monomials

$$T_1 > T_2 > \cdots.$$

The well-ordering of $\mathbb{M}$ implies that this cannot continue indefinitely! Hence there must be a representation

$$p = H_1 g_1 + \cdots + H_m g_m$$

such that for each $k = 1, 2, \ldots, m$ $H_k = 0$ or $\operatorname{lm}(H_k) \operatorname{lm}(g_k) \leq \operatorname{lm}(p)$. Both sides of the equa-

tion must simplify to the same polynomial, with the same leading variable, so at least one k has $\mathrm{lm}(H_k)\,\mathrm{lm}(g_k) = \mathrm{lm}(p)$; that is, $\mathrm{lm}(g_k) \mid \mathrm{lm}(p)$. Since p was arbitrary, G satisfies the definition of a Gröbner basis. □

Exercises.

Exercise 10.55: Show that $G = \left(x^2+y^2-4, xy-1, x+y^3-4y, -y^4+4y^2-1\right)$ is a Gröbner basis with respect to the lexicographic ordering.

Exercise 10.56: Show that G of Exercise 10.55 is *not* a Gröbner basis with respect to the grevlex ordering. As a consequence, the Gröbner basis property depends on the choice of term ordering!

Exercise 10.57: Show that any Gröbner basis G of an ideal I is a basis of the ideal; that is, any $p \in I$ can be written as $p = \sum_{i=1}^{m} h_i g_i$ for appropriate $h_i \in \mathbb{F}[x_1, \ldots, x_n]$.

Exercise 10.58: Show that for any non-constant polynomial f, $F = (f, f+1)$ is not a Gröbner basis.

Exercise 10.59: Show that every list of monomials is a Gröbner basis.

Exercise 10.60: We call a basis G of an ideal a **minimal basis** if no monomial of any $g_1 \in G$ is divisible by the leading monomial of any $g_2 \in G$.

(a) Suppose that a Gröbner basis G is not minimal. Show that we obtain a minimal basis by repeatedly replacing each $g \in G$ by $g - t\,g'$ where $t\,\mathrm{lm}(g')$ is a monomial of g.

(b) Explain why the minimal basis obtained in part (a) is also a Gröbner basis of the same ideal.

Exercise 10.61: Let

$$p = 4x^4 - 3x^3 - 3x^2y^4 + 4x^2y^2 - 16x^2 + 3xy^3 - 3xy^2 + 12x$$

and $F = \left(x^2+y^2-4, xy-1\right)$.

(a) Show that p reduces to zero with respect to F.

(b) Show that there exist $q_1, q_2 \in \mathbb{F}[x,y]$ such that $p = q_1 f_1 + q_2 f_2$.

(c) Generalize the argument of (b) to prove Lemma 10.54.

Exercise 10.62: For G to be a Gröbner basis, Definition 10.44 requires that every polynomial in the ideal generated by G be top-reducible by some element of G. If polynomials in the basis are top-reducible by other polynomials in the basis, we call them **redundant elements of the basis**.

(a) The Gröbner basis of Exercise 10.55 has redundant elements. Find a subset $G_{\min}$ of G that contains no redundant elements, but is still a Gröbner basis.

(b) Describe the method you used to find $G_{\min}$.

(c) Explain why redundant polynomials are not required to satisfy Definition 10.44. That is, if we know that G is a Gröbner basis, then we could remove redundant elements to obtain a smaller list, G_{min}, which is also a Gröbner basis *of the same ideal*.

10.5: Buchberger's algorithm

Algorithm 7 on page 240 shows how to triangularize a linear system. If you study it, you will see that essentially it looks for parts of the system that are not triangular (equations with the same leading variable) then adds a new polynomial to account for the triangular form. The new polynomial replaces one of the older polynomials in the pair.

For non-linear systems, we will try an approach that is similar, not but identical. We *will* look for polynomials in the ideal that do not satisfy the Gröbner basis property, we *will* add a new polynomial to repair this defect. We will not, however, replace the older polynomials, because in a non-linear system this might cause us either to lose the Gröbner basis property or even to change the ideal.

Example 10.63: Let $F = \left(xy + xz + z^2, yz + z^2\right)$, and use grevlex with $x > y > z$. The S-polynomial of f_1 and f_2 is

$$S = z\left(xy + xz + z^2\right) - x\left(yz + z^2\right) = z^3.$$

Let $G = \left(xy + xz + z^2, z^3\right)$; that is, G is F with f_2 replaced by S. It turns out that $yz + z^2 \notin \langle G \rangle$. If it were, then

$$yz + z^2 = h_1\left(xy + xz + z^2\right) + h_2 \cdot z^3.$$

Every term of the right hand side will be divisible either by x or by z^2, but yz is divisible by neither. Hence $yz + z^2 \in \langle G \rangle$. ◿

Thus we will adapt Algorithm 7 without replacing or discarding any polynomials. How will we look for polynomials in the ideal that do not satisfy the Gröbner basis property? For Guassian elimination with linear polynomials, this was "obvious": look for polynomials whose leading variables are the same. With non-linear polynomials, Buchberger's characterization (Theorem 10.51) suggests that we compute the S-polynomials, and top-reduce them. If they all top-reduce to zero, then Buchberger's characterization implies that we have a Gröbner basis already, so there is nothing to do. Otherwise, at least one S-polynomial does *not* top-reduce to zero, so we add its reduced form to the basis and test the new S-polynomials as well. This suggests Algorithm 8.

Theorem 10.64: *For any list of polynomials F over a field, Buchberger's algorithm terminates with a Gröbner basis of $\langle F \rangle$.*

Correctness isn't hard *if* Buchberger's algorithm terminates, because it discards nothing, adds only polynomials that are already in $\langle F \rangle$, and terminates only if all the S-polynomials of G top-reduce to zero. The problem is termination, which relies on the Ascending Chain Condition.

Algorithm 8. Buchberger's algorithm to compute a Gröbner basis

```
1:  inputs
2:    F = (f_1, f_2, ..., f_m), where each f_i ∈ 𝔽[x_1, ..., x_n].
3:    <, an admissible ordering.
4:  outputs
5:    G, a Gröbner basis of ⟨F⟩ with respect to <.
6:  do
7:    Let G := F
8:    Let P = {(f, g) : ∀ f, g ∈ G such that f ≠ g}
9:    repeat while P ≠ ∅
10:     Choose (f, g) ∈ P
11:     Remove (f, g) from P
12:     Let S be the S-polynomial of f, g
13:     Let r be the top-reduction of S with respect to G
14:     if r ≠ 0
15:       Replace P by P ∪ {(h, r) : h ∈ G}
16:       Append r to G
17:   return G
```

PROOF: For *termination,* let $\mathbb{F}$ be a field, and F a list of polynomials over $\mathbb{F}$. Designate

$$\begin{aligned}
I_0 &= \langle \operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_m) \rangle \\
I_1 &= \langle \operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_m), \operatorname{lm}(g_{m+1}) \rangle \\
I_2 &= \langle \operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_m), \operatorname{lm}(g_{m+1}), \operatorname{lm}(g_{m+2}) \rangle \\
&\vdots \\
I_i &= \langle \operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_m), \operatorname{lm}(g_{m+1}), \operatorname{lm}(g_{m+2}), \ldots, \operatorname{lm}(g_{m+i}) \rangle
\end{aligned}$$

where g_{m+i} is the ith polynomial added to G by line 16 of Algorithm 8.

We claim that $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ is a strictly ascending chain of ideals. After all, a polynomial r is added to the basis only when it is non-zero (line 14); since it has not top-reduced to zero, $\operatorname{lm}(r)$ is not top-reducible by

$$G_{i-1} = (g_1, g_2, \ldots, g_{m+i-1}).$$

Thus for any $p \in G_{i-1}$, $\operatorname{lm}(p)$ does not divide $\operatorname{lm}(r)$. We further claim that this implies that $\operatorname{lm}(p) \notin I_{i-1}$. By way of contradiction, suppose that it is. By Exercise 10.59 on page 264, any list of monomials is a Gröbner basis; hence

$$T = (\operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_{m+i-1}))$$

is a Gröbner basis, and by Definition 10.44 every polynomial in I_{i-1} is top-reducible by T. Since

p is not top-reducible by T, $\operatorname{lm}(p) \notin I_{i-1}$.

Thus $I_{i-1} \subsetneq I_i$, and $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ is a strictly ascending chain of ideals in $\mathbb{F}[x_1 x_2, \ldots, x_n]$. By Proposition 8.34 and Definition 8.32, there exists $M \in \mathbb{N}$ such that $I_M = I_{M+1} = \cdots$. This implies that the algorithm can add at most $M - m$ polynomials to G; after having done so, any remaining elements of P generate S-polynomials that top-reduce to zero! Line 11 removes each pair (i, j) from P, so P decreases after we have added these $M - m$ polynomials. Eventually P decreases to $\emptyset$, and the algorithm terminates.

For *correctness,* we have to show two things: first, that G is a basis of the same ideal as F, and second, that G satisfies the Gröbner basis property. For the first, observe that every polynomial added to G is by construction an element of $\langle G \rangle$, so the ideal does not change. For the second, let $p \in \langle G \rangle$; there exist $h_1, \ldots, h_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that

$$p = h_1 g_1 + \cdots + h_m g_m. \tag{31}$$

We consider three cases. □

Case 1. There exists i such that $\operatorname{lm}(h_i) \operatorname{lm}(g_i) = \operatorname{lm}(p)$.
In this case $\operatorname{lm}(g_i)$ divides $\operatorname{lm}(p)$, and we are done.
Case 1. For all $i = 1, 2, \ldots, m$, $\operatorname{lm}(h_i) \operatorname{lm}(g_i) = \operatorname{lm}(p)$.
This and Proposition 10.23 contradict equation (31), so this case cannot occur.
Case 1. There exists i such that $\operatorname{lm}(h_i) \operatorname{lm}(g_i) > \operatorname{lm}(p)$.
Choose i such that $\operatorname{lm}(h_i) \operatorname{lm}(g_i)$ is maximal among the monomials *and* i is maximal among the indices. Write $t = \operatorname{lm}(h_i) \operatorname{lm}(g_i)$. To satisfy equation (31), t must cancel with another term on the right hand side. Thus, there exists $j \neq i$ such that $t = \operatorname{lm}\left(h_j\right) \operatorname{lm}\left(g_j\right)$; choose such a j. We now show how to use the S-polynomial of g_i and g_j to rewrite equation (31) with a "smaller" representation.

Let $a \in \mathbb{F}$ such that

$$a \cdot \operatorname{lc}\left(h_j\right) \operatorname{lc}\left(g_j\right) = -\operatorname{lc}(h_i) \operatorname{lc}(g_i).$$

Thus

$$\begin{aligned} &\operatorname{lc}(h_i) \operatorname{lm}(h_i) \operatorname{lc}(g_i) \operatorname{lm}(g_i) \\ &\quad + a \cdot \operatorname{lc}\left(h_j\right) \operatorname{lm}\left(h_j\right) \operatorname{lc}\left(g_j\right) \operatorname{lm}\left(g_j\right) = \left[\operatorname{lc}(h_i) \operatorname{lc}(g_i) + a \cdot \operatorname{lc}\left(h_j\right) \operatorname{lc}\left(g_j\right)\right] \cdot t \\ &\qquad = 0. \end{aligned}$$

By Lemma 10.45, $\operatorname{lc}(h_i) \operatorname{lm}(h_i)\, g_i + a \cdot \operatorname{lc}\left(h_j\right) \operatorname{lm}\left(h_j\right) g_j$ is a multiple of $\operatorname{Spol}\left(g_i, g_j\right)$; choose a constant $b \in \mathbb{F}$ and a monomial $t \in \mathbb{M}$ such that

$$\operatorname{lc}(h_i) \operatorname{lm}(h_i)\, g_i + a \cdot \operatorname{lc}\left(h_j\right) \operatorname{lm}\left(h_j g_j\right) = b\, t \cdot \operatorname{Spol}\left(g_i, g_j\right).$$

The algorithm has terminated, so it considered this S-polynomial and top-reduced it to zero with

respect to G. By Lemma 10.54 there exist $q_1,\dots,q_m \in \mathbb{F}[x_1,\dots,x_n]$ such that

$$\operatorname{Spol}\left(g_i,g_j\right) = q_1 g_1 + \cdots + q_m g_m$$

and $\operatorname{lm}(q_k)\operatorname{lm}(g_k) \le \operatorname{lm}\left(\operatorname{Spol}\left(g_i,g_j\right)\right) < \operatorname{lcm}\left(\operatorname{lm}(g_i),\operatorname{lm}\left(g_j\right)\right)$ for each $k = 1,2,\dots,m$. Rewrite equation (31) in the following way:

$$\begin{aligned}
p &= h_1 g_1 + \cdots + h_m g_m \\
&= (h_1 g_1 + \cdots + h_m g_m) - bt \cdot \operatorname{Spol}\left(g_i,g_j\right) + bt \cdot (q_1 g_1 + \cdots + q_m g_m) \\
&= (h_1 g_1 + \cdots + h_m g_m) \\
&\quad - bt \cdot \left[\operatorname{lc}\left(g_j\right) \frac{\operatorname{lcm}\left(\operatorname{lm}(g_i),\operatorname{lm}\left(g_j\right)\right)}{\operatorname{lm}(g_i)} \cdot g_i - \operatorname{lc}(g_i) \frac{\operatorname{lcm}\left(\operatorname{lm}(g_i),\operatorname{lm}\left(g_j\right)\right)}{\operatorname{lm}\left(g_j\right)} \cdot g_j \right] \\
&\quad + bt \cdot (q_1 g_1 + \cdots + q_m g_m).
\end{aligned}$$

Let

$$H_k = \begin{cases} h_k + bt \cdot q_k, & k \neq i,j \\ h_i - bt \cdot \operatorname{lc}\left(g_j\right) \cdot \frac{\operatorname{lcm}\left(\operatorname{lm}(g_i),\operatorname{lm}\left(g_j\right)\right)}{\operatorname{lm}(g_i)} + bt \cdot q_i, & k = i \\ h_j - bt \cdot \operatorname{lc}(g_i) \cdot \frac{\operatorname{lcm}\left(\operatorname{lm}(g_i),\operatorname{lm}\left(g_j\right)\right)}{\operatorname{lm}\left(g_j\right)} + bt \cdot q_j, & k = j. \end{cases}$$

Now $\operatorname{lm}(H_i)\operatorname{lm}(g_i) < \operatorname{lm}(h_i)\operatorname{lm}(g_i)$ because of cancellation in H_i. In a similar way, we can show that $\operatorname{lm}\left(H_j\right)\operatorname{lm}\left(g_j\right) < \operatorname{lm}\left(h_j\right)\operatorname{lm}\left(g_j\right)$. By substitution,

$$p = H_1 g_1 + \cdots + H_m g_m.$$

There are only finitely many elements in G, so there were finitely many candidates

PROOF: We have now rewritten the representation of p so that $\operatorname{lm}(H_i) < \operatorname{lm}(h_i)$, so $\operatorname{lm}(H_i)\operatorname{lm}(g_i) < t$. We had chosen i maximal among the indices satisfying $\operatorname{lm}(h_i)\operatorname{lm}(g_i) = t$, so if there exists k such that the new representation has $\operatorname{lm}(h_k)\operatorname{lm}(g_k) = t$, then $k < i$. Thanks to the Gröbner basis property, we can continue to do this as long as any $\operatorname{lm}(h_i)\operatorname{lm}(g_i) = t$, so after finitely many steps we rewrite equation (31) so that $\operatorname{lm}(h_k)\operatorname{lm}(g_k) < t$ for all $k = 1,2,\dots,m$.

If we can still find i such that $\operatorname{lm}(h_i)\operatorname{lm}(g_i) > \operatorname{lm}(p)$, then we repeat the process again. This gives us a descending chain of monomials $t = u_1 > u_2 > \cdots$; Proposition 10.23(B) on page 247, the well-ordering of the monomials under $<$, implies that eventually each chain must stop. It stops only when $\operatorname{lm}(h_i)\operatorname{lm}(g_i) \le \operatorname{lm}(p)$ for each i. As in the case above, we cannot have all of them smaller, so there must be at least one i such that $\operatorname{lm}(h_i)\operatorname{lm}(g_i) = \operatorname{lm}(p)$. This implies that $\operatorname{lm}(g_i)$ divides $\operatorname{lm}(p)$ for at least one $g_i \in G$. □

Exercises

Exercise 10.65: Using G of Exercise 10.55, compute a Gröbner basis with respect to the grevlex ordering.

Exercise 10.66: Following up on Exercises 10.56 and 10.65, a simple diagram will help show that it is "easier" to compute a Gröbner basis in any total degree ordering than it is in the lexicographic ordering. We can diagram the monomials in x and y on the x-y plane by plotting $x^\alpha y^\beta$ at the point (α, β).

(a) Shade the region of monomials that are smaller than x^2y^3 with respect to the lexicographic ordering.

(b) Shade the region of monomials that are smaller than x^2y^3 with respect to the graded reverse lexicographic ordering.

(c) Explain why the diagram implies that top-reduction of a polynomial with leading monomial x^2y^3 will *probably* take less effort in grevlex than in the lexicographic ordering.

Exercise 10.67: Let $g_1, g_2, \ldots, g_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. We say that a non-linear polynomial is *homogeneous* if every term is of the same total degree. For example, $xy - 1$ is not homogeneous, but $xy - h^2$ is. As you may have guessed, we can homogenize any polynomial by multiplying every term by an appropriate power of a *homogenizing variable* h. When $h = 1$, we have the original polynomial.

(a) Homogenize the following polynomials.
   (i) $x^2 + y^2 - 4$
   (ii) $x^3 - y^5 + 1$
   (iii) $xz + z^3 - 4x^5y - xyz^2 + 3x$

(b) Explain the relationship between solutions to a system of nonlinear polynomials G and solutions to the system of homogenized polynomials H.

(c) With homogenized polynomials, we usually use a variant of the lexicographic ordering. Although h comes *first* in the dictionary, we pretend that it comes last. So $x > yh^2$ and $y > h^{10}$. Use this modified lexicographic ordering to determine the leading monomials of your solutions for part (a).

(d) Does homogenization preserve leading monomials?

Exercise 10.68: Assume that the $g_1, g_2, \ldots, g_m$ are homogeneous; in this case, we can build the *ordered Macaulay matrix of G of degree D* in the following way.

- Each row of the matrix represents a monomial multiple of some g_i. If g_i is of degree $d \leq D$, then we compute all the monomial multiples of g_i that have degree D. There are of these.
- Each column represents a monomial of degree d. Column 1 corresponds to the largest monomial with respect to the lexicographic ordering; column 2 corresponds to the next-largest polynomial; etc.
- Each entry of the matrix is the coefficient of a monomial for a unique monomial multiple of some g_i.

(a) The homogenization of the circle and the hyperbola gives us the system

$$F = \left(x^2 + y^2 - 4h^2, xy - h^2\right).$$

Verify that its ordered Macaulay matrix of degree 3 is

$$\begin{pmatrix}
x^3 & x^2y & xy^2 & y^3 & x^2h & xyh & y^2h & xh^2 & yh^2 & h^3 & \\
1 & & 1 & & & & & -4 & & & xf_1 \\
& 1 & & 1 & & & & & -4 & & yf_1 \\
& & & & 1 & & 1 & & & -4 & hf_1 \\
& 1 & & & & & & -1 & & & xf_2 \\
& & 1 & & & & & & -1 & & yf_2 \\
& & & & & 1 & & & & -1 & hf_2
\end{pmatrix}.$$

Show that if you triangularize this matrix *without swapping columns*, the row corresponding to xf_2 now contains coefficients that correspond to the homogenization of $x + y^3 - 4y$.

(b) Compute the ordered Macaulay matrix of F of degree 4, then triangularize it. Be sure *not to swap columns*, nor to destroy rows that provide new information. Show that

- the entries of at least one row correspond to the coefficients of a multiple of the homogenization of $x + y^3 - 4y$, and
- the entries of at least one other row correspond to the coefficients of the homogenization of $\pm\left(y^4 - 4y^2 + 1\right)$.

(c) Explain the relationship between triangularizing the ordered Macaulay matrix and Buchberger's algorithm.

Sage programs

The following programs can be used in Sage to help make the amount of computation involved in the exercises less burdensome. Use

- `M, mons = sylvester_matrix(F,d)` to make an ordered Macaulay matrix of degree d for the list of polynomials F,
- `N = triangularize_matrix(M)` to triangularize M in a way that respects the monomial order, and
- `extract_polys(N,mons)` to obtain the polynomials of N.

```
def make_monomials(xvars,d,p=0,order="lex"):
  result = set([1])
  for each in range(d):
    new_result = set()
    for each in result:
      for x in xvars:
        new_result.add(each*x)
    result = new_result
  result = list(result)
  result.sort(lambda t,u:  monomial_cmp(t,u))
  n = sage.rings.integer.Integer(len(xvars))
  return result

def monomial_cmp(t,u):
  xvars = t.parent().gens()
  for x in xvars:
    if t.degree(x) != u.degree(x):
      return u.degree(x) - t.degree(x)
  return 0

def homogenize_all(polys):
  for i in range(len(polys)):
    if not polys[i].is_homogeneous():
      polys[i] = polys[i].homogenize()

def sylvester_matrix(polys,D,order="lex"):
  L = [ ]
  homogenize_all(polys)
  xvars = polys[0].parent().gens()
  for p in polys:
    d = D - p.degree()
    R = polys[0].parent()
    mons = make_monomials(R.gens(),d,order=order)
```

```
    for t in mons:
      L.append(t*p)
  mons = make_monomials(R.gens(),D,order=order)
  mons_dict = {}
  for each in range(len(mons)):
    mons_dict.update({mons[each]:each})
  M = matrix(len(L),len(mons))
  for i in range(len(L)):
    p = L[i]
    pmons = p.monomials()
    pcoeffs = p.coefficients()
    for j in range(len(pmons)):
      M[i,mons_dict[pmons[j]]] = pcoeffs[j]
  return M, mons

def triangularize_matrix(M):
  N = M.copy()
  m = N.nrows()
  n = N.ncols()
  for i in range(m):
    pivot = 0
    while pivot < n and N[i,pivot] == 0:
      pivot = pivot + 1
    if pivot < n:
      a = N[i,pivot]
      for j in range(i+1,m):
        if N[j,pivot] != 0:
          b = N[j,pivot]
          for k in range(pivot,n):
            N[j,k] = a * N[j,k] - b * N [i,k]
  return N

def extract_polys(M, mons):
  L = [ ]
  for i in range(M.nrows()):
    p = 0 for j in range(M.ncols()):
    if M[i,j] != 0:
      p = p + M[i,j]*mons[j]
    L.append(p)
  return L
```

10.6: Elementary applications

We now turn our attention to posing, and answering, questions that make Gröbner bases interesting. Recall from Section

- $\mathbb{F}$ is an *algebraically closed* field—that is, all polynomials over $\mathbb{F}$ have their roots in $\mathbb{F}$;
- $\mathcal{R} = \mathbb{F}[x_1, x_2, \ldots, x_n]$ is a polynomial ring;
- $F \subset \mathcal{R}$;
- $V_F \subset \mathbb{F}^n$ is the set of common roots of elements of F;
- $I = \langle F \rangle$; and
- $G = (g_1, g_2, \ldots, g_m)$ is a Gröbner basis of I with respect to an admissible ordering.

Note that $\mathbb{C}$ is algebraically closed, but $\mathbb{R}$ is not, since the roots of $x^2 + 1 \in \mathbb{R}[x]$ are not in $\mathbb{R}$.

Our first question regards membership in an ideal.

Theorem 10.69 (The Ideal Membership Problem): *Let $p \in \mathcal{R}$. The following are equivalent.*
(A) $p \in I$.
(B) p *top-reduces to zero with respect to* G.

PROOF: That (A) $\Longrightarrow$ (B): Assume that $p \in I$. If $p = 0$, then we are done. Otherwise, the definition of a Gröbner basis implies that $\operatorname{lm}(p)$ is top-reducible by some element of G. Let $g \in G$ such that $\operatorname{lm}(g) \mid \operatorname{lm}(p)$, and choose $c \in \mathbb{F}$ and $u \in \mathbb{M}$ such that $\operatorname{lc}(p)\operatorname{lm}(p) = cu \cdot \operatorname{lc}(g)\operatorname{lm}(g)$. Let r_1 be the result of the top-reduction; that is,

$$r_1 = p - cu \cdot g.$$

Then $\operatorname{lm}(r_1) < \operatorname{lm}(p)$ and by the definition of an ideal, $r_1 \in I$. If $r_1 = 0$, then we are done; otherwise the definition of a Gröbner basis implies that $\operatorname{lm}(p)$ is top-reducible by some element of G. Continuing as above, we generate a list of polynomials $p, r_1, r_2, \ldots$ such that

$$\operatorname{lm}(p) > \operatorname{lm}(r_1) > \operatorname{lm}(r_2) > \cdots.$$

By the well-ordering of $\mathbb{M}$, this list cannot continue indefinitely, so eventually top-reduction must be impossible. Choose i such that r_i does not top-reduce with respect to G. Inductively, $r_i \in I$, and G is a Gröbner basis of I, so it must be that $r_i = 0$.

That (B) $\Longrightarrow$ (A): Assume that p top-reduces to zero with respect to G. Lemma 10.54 implies that $p \in I$. □

Now that we have ideal membership, let us return to a topic we considered briefly in Chapter 7. In Exercise 8.25 on page 189 you showed that

> …the common roots of $f_1, f_2, \ldots, f_m$ are common roots of all polynomials in the ideal I.

Since $I = \langle G \rangle$, the common roots of $g_1, g_2, \ldots, g_m$ are common roots of all polynomials in I. Thus if we start with a system F, and we want to analyze its polynomials, we can do so by

analyzing the roots of any Gröbner basis G of $\langle F\rangle$. This might seem unremarkable, except that like triangular linear systems, *it is easy to analyze the roots of Gröbner bases!* Our next result gives an easy test for the existence of common roots.

Theorem 10.70: *The following both hold.*
(A) $V_F = V_G$; that is, common roots of F are common roots of G, and vice versa.
(B) F has no common roots if and only if G contains a nonzero constant polynomials.

PROOF: (A) Let $\alpha \in V_F$. By definition, $f_i(\alpha_1,\ldots,\alpha_n) = 0$ for each $i = 1,\ldots,m$. By construction, $G \subseteq \langle F\rangle$, so $g \in G$ implies that $g = h_1 f_1 + \cdots + h_m f_m$ for certain $h_1,\ldots,h_m \in \mathcal{R}$. By substitution,

$$\begin{aligned} g(\alpha_1,\ldots,\alpha_n) &= \sum_{i=1}^{m} h_i(\alpha_1,\ldots,\alpha_n) f_i(\alpha_1,\ldots,\alpha_n) \\ &= \sum_{i=1}^{m} h_i(\alpha_1,\ldots,\alpha_n)\cdot 0 \\ &= 0. \end{aligned}$$

That is, α is also a common root of G. In other words, $V_F \subseteq V_G$.

On the other hand, $F \subseteq \langle F\rangle = \langle G\rangle$ by Exercise 10.57, so a similar argument shows that $V_F \supseteq V_G$. We conclude that $V_F = V_G$.

(B) Let g be a nonzero constant polynomial, and observe that $g(\alpha_1,\ldots,\alpha_n) \neq 0$ for any $\alpha \in \mathbb{F}^n$. Thus, if $g \in G$, then $V_G = \emptyset$. By (A), $V_F = V_G = \emptyset$, so F has no common roots if G contains a nonzero constant polynomial.

For the converse, we need the Weak Nullstellensatz, Theorem 8.95 on page 213. If F has no common roots, then $V_F = \emptyset$, and by the Weak Nullstellensatz, $I = \mathcal{R}$. In this case, $1_{\mathcal{R}} \in I$. By definition of a Gröbner basis, there is some $g \in G$ such that $\operatorname{lm}(g) \mid \operatorname{lm}(1_{\mathcal{R}})$. This requires g to be a constant. □

Once we know common solutions exist, we want to know how many there are.

Theorem 10.71: *There are finitely many complex solutions if and only if for each $i = 1,2,\ldots,n$ we can find $g \in G$ and $a \in \mathbb{N}$ such that $\operatorname{lm}(g) = x_i^a$.*

Theorem 10.71 is related to a famous result called Hilbert's Nullstellensatz.

PROOF OF THEOREM 10.71: Observe that we can find $g \in G$ and $\alpha \in \mathbb{N}$ such that $\operatorname{lm}(g) = x_i^a$ for each $i = 1,2,\ldots,n$ if and only if $\mathcal{R}/I$ is finite; see Figure . However, $\mathcal{R}/I$ is independent of any monomial ordering. Thus, we can assume, without loss of generality, that the ordering is lexicographic.

Assume first that for each $i = 1,\ldots,n$ we can find $g \in G$ and $a \in \mathbb{N}$ such that $\operatorname{lm}(g) = x_i^a$. Since x_n is the smallest variable, even $x_{n-1} > x_n$, so g must be a polynomial in x_n *alone;*

any other variable in a non-leading monomial would contradict the assumption that $\operatorname{lm}(g) = x_n^a$. The Fundamental Theorem of Algebra implies that g has a complex solutions. We can back-substitute these solutions into the remaining polynomials, using similar logic. Each back-substitution yields only finitely many solutions. There are finitely many polynomials, so G has finitely many complex solutions.

Conversely, assume G has finitely many solutions; call them $\alpha^{(1)}, \ldots, \alpha^{(\ell)} \in \mathbb{F}^n$. Let

$$J = \left\langle x_1 - \alpha_1^{(1)}, \ldots, x_n - \alpha_n^{(1)} \right\rangle \bigcap \cdots \bigcap \left\langle x_1 - \alpha_1^{(\ell)}, \ldots, x_n - \alpha_n^{(\ell)} \right\rangle.$$

Recall that J is an ideal. You will show in the exercises that I and J have the same common solutions; that is, $V_I = V_J$.

For any $f \in \sqrt{I}$, the fact that $\mathcal{R}$ is an integral domain implies that

$$f(\alpha) = 0 \qquad \Longleftrightarrow \qquad f^a(\alpha) = 0 \; \exists a \in \mathbb{N}^+,$$

so $V_I = V_{\sqrt{I}}$. Let K be the ideal of polynomials that vanish on V_I. Notice that $I \subseteq \sqrt{I} \subseteq K$ by definition. We claim that $\sqrt{I} \supseteq K$ as well. Why? Let $p \in K$ be nonzero. Consider the polynomial ring $\mathbb{F}[x_1, \ldots, x_n, y]$ where y is a new variable. Let $A = \langle f_1, \ldots, f_m, 1 - yp \rangle$. Notice that $V_A = \emptyset$, since $f_i = 0$ for each i implies that $p = 0$, but then $1 - yp \neq 0$. By Theorem 10.70, any Gröbner basis of A has a nonconstant polynomial, call it c. By definition of A, there exist $H_1, \ldots, H_{m+1} \in \mathbb{F}[x_1, \ldots, x_n, y]$ such that

$$c = H_1 f_1 + \cdots + H_m f_m + H_{m+1}(1 - yp).$$

Let $h_i = c^{-1} H_i$ and

$$1 = h_1 f_1 + \cdots + h_m f_m + h_{m+1}(1 - yp).$$

Put $y = \frac{1}{p}$ and we have

$$1 = h_1 f_1 + \cdots + h_m f_m + h_{m+1} \cdot 0$$

where each h_i is now in terms of x_1, …, x_n and $1/p$. Clear the denominators by multiplying both sides by a suitable power a of p, and we have

$$p^a = h_1' f_1 + \cdots + h_m' f_m$$

where each $h_i' \in \mathcal{R}$. Since $I = \langle f_1, \ldots, f_m \rangle$, we see that $p^a \in I$. Thus $p \in \sqrt{I}$. Since p was abitrary in K, we have $\sqrt{I} \supseteq K$, as claimed.

We have shown that $K = \sqrt{I}$. Since K is the ideal of polynomials that vanish on V_I, and by construction, $V_{\sqrt{I}} = V_I = V_J$, You will show in the exercises that $J = \sqrt{J}$, so $V_{\sqrt{I}} = V_{\sqrt{J}}$.

Hence $\sqrt{I} = \sqrt{J}$. By definition of J,

$$q_j = \prod_{i=1}^{\ell} \left(x_j - a_j^{(i)} \right) \in J$$

for each $j = 1, \ldots, n$. Since $\sqrt{I} = J$, suitable choices of $a_1, \ldots, a_n \in \mathbb{N}^+$ give us

$$q_1 = \prod_{i=1}^{\ell} \left(x_1 - \alpha_1^{(i)} \right)^{a_1}, \ldots, q_n = \prod_{i=1}^{\ell} \left(x_n - \alpha_n^{(i)} \right)^{a_n} \in I.$$

Notice that $\operatorname{lm}(q_i) = x_i^{a_i}$ for each i. Since G is a Gröbner basis of I, the definition of a Gröbner basis implies that for each i there exists $g \in G$ such that $\operatorname{lm}(g) \mid \operatorname{lm}(q_i)$. In other words, for each i there exists $g \in G$ and $a \in \mathbb{N}$ such that $\operatorname{lm}(g) = x_i^a$. □

Example 10.72: Recall the system from Example 10.52,

$$F = \left(x^2 + y^2 - 4, xy - 1 \right).$$

In Exercise 10.55 you computed a Gröbner basis in the lexicographic ordering. You probably obtained this a superset of

$$G = \left(x + y^3 - 4y, y^4 - 4y^2 + 1 \right).$$

G is also a Gröbner basis of $\langle F \rangle$. Since G contains no constants, we know that F has common roots. Since $x = \operatorname{lm}(g_1)$ and $y^4 = \operatorname{lm}(g_2)$, we know that there are finitely many common roots. ◿

We conclude by pointing in the direction of how to find the common roots of a system.

Theorem 10.73 (The Elimination Theorem): *Suppose the ordering is lexicographic with $x_1 > x_2 > \cdots > x_n$. For all $i = 1, 2, \ldots, n$, each of the following holds.*

(A) $\widehat{I} = I \cap \mathbb{F}\left[x_i, x_{i+1}, \ldots, x_n\right]$ *is an ideal of* $\mathbb{F}\left[x_i, x_{i+1}, \ldots, x_n\right]$. *(If $i = n$, then $\widehat{I} = I \cap \mathbb{F}$.)*

(B) $\widehat{G} = G \cap \mathbb{F}\left[x_i, x_{i+1}, \ldots, x_n\right]$ *is a Gröbner basis of the ideal $\widehat{I}$.*

PROOF: For (A), let $f, g \in \widehat{I}$ and $h \in \mathbb{F}\left[x_i, x_{i+1}, \ldots, x_n\right]$. Now $f, g \in I$ as well, we know that $f - g \in I$, and subtraction does not add any terms with factors from $x_1, \ldots, x_{i-1}$, so $f - g \in \mathbb{F}\left[x_i, x_{i+1}, \ldots, x_n\right]$ as well. By definition of $\widehat{I}$, $f - g \in \widehat{I}$. Similarly, $h \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ as well, so $fh \in I$, and multiplication does not add any terms with factors from $x_1, \ldots, x_{i-1}$, so $fh \in \mathbb{F}\left[x_i, x_{i+1}, \ldots, x_n\right]$ as well. By definition of $\widehat{I}$, $fh \in \widehat{I}$.

For (B), let $p \in \widehat{I}$. Again, $p \in I$, so there exists $g \in G$ such that $\operatorname{lm}(g)$ divides $\operatorname{lm}(p)$. The ordering is lexicographic, so g cannot have *any* terms with factors from $x_1, \ldots, x_{i-1}$. Thus

$g \in \mathbb{F}\left[x_i, x_{i+1}, \ldots, x_n\right]$. By definition of $\widehat{G}$, $g \in \widehat{G}$. Thus $\widehat{G}$ satisfies the definition of a Gröbner basis of $\widehat{I}$. □

The ideal $\widehat{I}$ is important enough to merit its own terminology.

Definition 10.74: For $i = 1, 2, \ldots, n$ the ideal $\widehat{I} = I \cap \mathbb{F}\left[x_i, x_{i+1}, \ldots, x_n\right]$ is called the i**th elimination ideal of** I.

Theorem 10.73 suggests that to find the common roots of F, we use a lexicographic ordering, then:

- find common roots of $G \cap \mathbb{F}[x_n]$;
- back-substitute to find common roots of $G \cap \mathbb{F}\left[x_{n-1}, x_n\right]$;
- ...
- back-substitute to find common roots of $G \cap \mathbb{F}[x_1, x_2, \ldots, x_n]$.

Example 10.75: We can find the common solutions of the circle and the hyperbola in Figure 10.1 on page 255 using the Gröbner basis computed in Example 276 on page 10.72. Since

$$G = \left(x + y^3 - 4y, y^4 - 4y^2 + 1\right),$$

we have

$$\widehat{G} = G \cap \mathbb{C}[y] = \left\{y^4 - 4y^2 + 1\right\}.$$

It isn't hard to find the roots of this polynomial. Let $u = y^2$; the resulting substitution gives us the quadratic equation $u^2 - 4u + 1$ whose roots are

$$u = \frac{4 \pm \sqrt{(-4)^2 - 4 \cdot 1 \cdot 1}}{2} = 2 \pm \sqrt{3}.$$

Back-substituting u into $\widehat{G}$,

$$y = \pm\sqrt{u} = \pm\sqrt{2 \pm \sqrt{3}}.$$

We can now back-substitute y into G to find that

$$\begin{aligned} x &= -y^3 + 4y \\ &= \mp\left(\sqrt{2 \pm \sqrt{3}}\right)^3 \pm 4\sqrt{2 \pm \sqrt{3}}. \end{aligned}$$

Thus there are four common roots, all of them real, illustrated by the four intersections of the circle and the hyperbola. ◿

Exercises.

Exercise 10.76: Determine whether $x^6 + x^4 + 5y - 2x + 3xy^2 + xy + 1$ is an element of the ideal $\left\langle x^2 + 1, xy + 1\right\rangle$.

Exercise 10.77: Determine the common roots of x^2+1 and $xy+1$ in $\mathbb{C}$.

Exercise 10.78: Repeat the problem in $\mathbb{Z}_2$.

Exercise 10.79: Suppose A, B are ideals of $\mathcal{R}$.
(a) Show that $V_{A\cap B} = V(A) \cup V(B)$.
(b) Explain why this shows that for the ideals I and J defined in the proof of Theorem 10.71, $V_I = V_J$.

Chapter 11:
Advanced methods of computing Gröbner bases

11.1: The Gebauer-Möller algorithm

Buchberger's algorithm (Algorithm 8 on page 266) allows us to compute Gröbner bases, but it turns out that, without any optimizations, the algorithm is quite inefficient. To explain why this is the case, we make the following observations:

1. The goal of the algorithm is to add polynomials until we have a Gröbner basis. That is, the algorithm is looking for new information.
2. We obtain this new information whenever an S-polynomial does *not* reduce to zero.
3. When an S-polynomial does reduce to zero, we do not add anything. In other words, we have no new information.
4. Thus, reducing an S-polynomial to zero is a wasted computation.

With these observations, we begin to see why the basic Buchberger algorithm is inefficient: it computes every S-polynomial, including those that reduce to zero. Once we have added the last polynomial necessary to satisfy the Gröbner basis property, there is no need to continue. However, at the very least, line 15 of the algorithm generates a larger number of new pairs for P that will create S-polynomials that will reduce to zero. It is also possible that a large number of other pairs will not yet have been considered, and so will also need to be reduced to zero! This prompts us to look for criteria that detect useless computations, and to apply these criteria in such a way as to maximize their usage. Buchberger discovered two additional criteria that do this; this section explores these criteria, then presents a revised Buchberger algorithm that attempts to maximize their effect.

The first criterion arises from an observation that you might have noticed already.

Example 11.1: Let $p = x^2 + 2xy + 3x$ and $q = y^2 + 2x + 1$. Consider any ordering such that $\mathrm{lm}(p) = x^2$ and $\mathrm{lm}(q) = y^2$. Notice that the leading monomials of p and q are *relatively prime*; that is, they have no variables in common.

Now consider the S-polynomial of p and q (we highlight in each step the leading monomial under the grevlex ordering):

$$\begin{aligned} S &= y^2 p - x^2 q \\ &= \mathbf{2xy^3} - 2x^3 + 3xy^2 - x^2. \end{aligned}$$

This S-polynomial top-reduces to zero:

$$\begin{aligned} S - 2xyq &= \left(3xy^2 - 2x^3 - x^2\right) - \left(4x^2y + 2xy\right) \\ &= -\mathbf{2x^3} - 4x^2y + 3xy^2 - x^2 - 2xy; \end{aligned}$$

then

$$\begin{aligned}(S-2xyq)+2xp &= \left(-4x^2y+3xy^2-x^2-2xy\right)+\left(4x^2y+6x^2\right)\\ &= 3\mathbf{xy^2}+5x^2-2xy;\end{aligned}$$

then

$$\begin{aligned}(S-2xyq+2xp)-3xq &= \left(5x^2-2xy\right)-\left(6x^2+3x\right)\\ &= -\mathbf{x^2}-2xy-3x;\end{aligned}$$

finally

$$\begin{aligned}(S-2xyq+2xp-3xq)+p &= (-2xy-3x)+(2xy+3x)\\ &= 0.\end{aligned}$$

To generalize this beyond the example, observe that we have shown that

$$S+(2x+1)\,p-(2xy+3x)\,q=0$$

or

$$S=-(2x+1)\,p+(2xy+3x)\,q.$$

If you study p, q, and the polynomials in that last equation, you might notice that the quotients from top-reduction allow us to write:

$$S=-(q-\mathrm{lc}(q)\,\mathrm{lm}(q))\cdot p+(p-\mathrm{lc}(p)\,\mathrm{lm}(p))\cdot q.$$

This is rather difficult to look at, so we will adopt the notation for the trailing terms of p—that is, all the terms of p except the term containing the leading monomial. Rewriting the above equation, we have

$$S=-\mathrm{tts}(q)\cdot p+\mathrm{tts}(q)\cdot p.$$

If this were true in general, it might—*might*—be helpful.

Lemma 11.2 (Buchberger's gcd criterion): *Let p and q be two polynomials whose leading monomials are u and v, respectively. If u and v have no common variables, then the S-polynomial of p and q has the form*

$$S=-\mathrm{tts}(q)\cdot p+\mathrm{tts}(p)\cdot q.$$

PROOF: Since u and v have no common variables, $\mathrm{lcm}(u,v)=uv$. Thus the S-polynomial of

p and q is

$$\begin{aligned}
S &= \mathrm{lc}(q)\cdot\frac{uv}{u}\cdot(\mathrm{lc}(p)\cdot u+\mathrm{tts}(p))-\mathrm{lc}(p)\cdot\frac{uv}{v}\cdot(\mathrm{lc}(q)\cdot v+\mathrm{tts}(q))\\
&= \mathrm{lc}(q)\cdot v\cdot\mathrm{tts}(p)-\mathrm{lc}(p)\cdot u\cdot\mathrm{tts}(q)\\
&= \mathrm{lc}(q)\cdot v\cdot\mathrm{tts}(p)-\mathrm{lc}(p)\cdot u\cdot\mathrm{tts}(q)+[\mathrm{tts}(p)\cdot\mathrm{tts}(q)-\mathrm{tts}(p)\cdot\mathrm{tts}(q)]\\
&= \mathrm{tts}(p)\cdot[\mathrm{lc}(q)\cdot v+\mathrm{tts}(q)]-\mathrm{tts}(q)\cdot[\mathrm{lc}(p)\cdot u+\mathrm{tts}(p)]\\
&= \mathrm{tts}(p)\cdot q-\mathrm{tts}(q)\cdot p.
\end{aligned}$$

□

Lemma 11.2 is not quite enough. Recall Theorem 10.51 on page 259, the characterization theorem of a Gröbner basis:

Theorem 11.3 (Buchberger's characterization): *Let* $g_1, g_2, \ldots, g_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. *The following are equivalent.*

(A) $G = (g_1, g_2, \ldots, g_m)$ *is a Gröbner basis of the ideal* $I = \langle g_1, g_2, \ldots, g_m\rangle$.

(B) *For any pair* i, j *with* $1 \leq i < j \leq m$, $\mathrm{Spol}\left(g_i, g_j\right)$ top-reduces to zero with respect to G.

To satisfy Theorem 10.51, we have to show that the S-polynomials top-reduce to zero. However, the proof of Theorem 10.51 used Lemma 10.54:

Lemma 11.4: *Let* $p, f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. *Let* $F = (f_1, f_2, \ldots, f_m)$. *Then (A) implies (B) where*

(A) p *top-reduces to zero with respect to* F.

(B) *There exist* $q_1, q_2, \ldots, q_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ *such that each of the following holds:*

  (B1) $p = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$; *and*

  (B2) *For each* $k = 1, 2, \ldots, m, q_k = 0$ *or* $\mathrm{lm}(q_k)\,\mathrm{lm}(g_k) \leq \mathrm{lm}(p)$.

We can describe this in the following way, due to Daniel Lazard:

Theorem 11.5 (Lazard's characterization): *Let* $g_1, g_2, \ldots, g_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. *The following are equivalent.*

(A) $G = (g_1, g_2, \ldots, g_m)$ *is a Gröbner basis of the ideal* $I = \langle g_1, g_2, \ldots, g_m\rangle$.

(B) *For any pair* i, j *with* $1 \leq i < j \leq m$, $\mathrm{Spol}\left(g_i, g_j\right)$ top-reduces to zero with respect to G.

(C) *For any pair* i, j *with* $1 \leq i < j \leq m$, $\mathrm{Spol}\left(g_i, g_j\right)$ *has the form*

$$\mathrm{Spol}\left(g_i, g_j\right) = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m$$

and for each $k = 1, 2, \ldots, m$, $q_k = 0$ *or* $\mathrm{lm}(q_k)\,\mathrm{lm}(g_k) < \mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(q))$.

PROOF: That (A) is equivalent to (B) was the substance of Buchberger's characterization. That (B) implies (C) is a consequence of Lemma 10.54. That (C) implies (A) is implicit in the proof of Buchberger's characterization: you will extract it in Exercise 11.13. □

The form of an S-polynomial described in (C) of Theorem 11.5 is important enough to identify with a special term.

Definition 11.6: Let $G = (g_1, g_2, \ldots, g_m)$. We say that the S-polynomial of g_i and g_j has an **S-representation $(q_1, \ldots, q_m)$ with respect to G** if $q_1, q_2, \ldots, q_m \in \mathbb{F}[x_1, \ldots, x_n]$ and (C) of Theorem 11.5 is satisfied.

Lazard's characterization allows us to show that Buchberger's gcd criterion allows us to avoid top-reducing the S-polynomial of any pair whose leading monomials are relatively prime.

Corollary 11.7: *Let $g_1, g_2, \ldots, g_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. The following are equivalent.*

(A) $G = (g_1, g_2, \ldots, g_m)$ *is a Gröbner basis of the ideal* $I = \langle g_1, g_2, \ldots, g_m \rangle$.

(B) *For any pair (i, j) with $1 \leq i < j \leq m$, one of the following holds:*

(B1) The leading monomials of g_i and g_j have no common variables.

(B2) $\operatorname{Spol}\left(g_i, g_j\right)$ top-reduces to zero with respect to G.

PROOF: Since (A) implies (B2), (A) also implies (B). For the converse, assume (B). Let $\widehat{P}$ be the set of all pairs of P that have an S-representation with respect to G. If (i, j) satisfies (B1), then Buchberger's gcd criterion (Lemma 11.2) implies that

$$\operatorname{Spol}\left(g_i, g_j\right) = q_1 g_1 + \cdots + q_m g_m \tag{32}$$

where $q_i = -\operatorname{tts}\left(g_j\right)$, $q_j = \operatorname{tts}(g_i)$, and $q_k = 0$ for $k \neq i, j$. Notice that

$$\operatorname{lm}(q_i)\operatorname{lm}(g_i) = \operatorname{lm}\left(\operatorname{tts}\left(g_j\right)\right) \cdot \operatorname{lm}(g_i) < \operatorname{lm}\left(g_j\right)\operatorname{lm}(g_i) = \operatorname{lcm}\left(\operatorname{lm}(g_i), \operatorname{lm}\left(g_j\right)\right).$$

Thus 32 is an S-representation of $\operatorname{Spol}\left(g_i, g_j\right)$, so $(i, j) \in \widehat{P}$. If (i, j) satisfes (B2), then by Lemma 10.54, $(i, j) \in \widehat{P}$ also. Hence every pair (i, j) is in $\widehat{P}$. Lazard's characterization now implies that G is a Gröbner basis of $\langle G \rangle$; that is, (A). □

Although the gcd criterion is clearly useful, it is rare to encounter in practice a pair of polynomials whose leading monomials have no common variables. That said, you have seen such pairs once already, in Exercises 10.55 and 10.65.

We need, therefore, a stronger criterion. The next one is a little harder to discover, so we present it directly.

Lemma 11.8 (Buchberger's lcm criterion): *Let p and q be two polynomials whose leading monomials are u and v, respectively. Let f be a polynomial whose leading monomial is t. If t divides* $\operatorname{lcm}(u,v)$*, then the S-polynomial of p and q has the form*

$$S = \frac{\operatorname{lc}(q)\cdot\operatorname{lcm}(u,v)}{\operatorname{lc}(f)\cdot\operatorname{lcm}(t,u)}\cdot\operatorname{Spol}(p,f) + \frac{\operatorname{lc}(p)\cdot\operatorname{lcm}(u,v)}{\operatorname{lc}(f)\cdot\operatorname{lcm}(t,v)}\cdot\operatorname{Spol}(f,q). \tag{33}$$

PROOF: First we show that the fractions in equation (33) reduce to monomials. Let x be any variable. Since t divides $\operatorname{lcm}(u,v)$, we know that

$$\deg_x t \le \deg_x \operatorname{lcm}(u,v) = \max\left(\deg_x u, \deg_x v\right).$$

(See Exercise 11.12.) Thus

$$\deg_x \operatorname{lcm}(t,u) = \max\left(\deg_x t, \deg_x u\right) \le \max\left(\deg_x u, \deg_x v\right) = \deg_x \operatorname{lcm}(u,v).$$

A similar argument shows that

$$\deg_x \operatorname{lcm}(t,v) \le \deg_x \operatorname{lcm}(u,v).$$

Thus the fractions in (33) reduce to monomials.

It remains to show that (33) is, in fact, consistent. This is routine; working from the right, and writing $S_{a,b}$ for the S-polynomial of a and b and $L_{a,b}$ for $\operatorname{lcm}(a,b)$, we have

$$\begin{aligned}
\frac{\operatorname{lc}(q)\cdot L_{u,v}}{\operatorname{lc}(f)\cdot L_{t,u}}\cdot S_{p,f} + \frac{\operatorname{lc}(p)\cdot L_{u,v}}{\operatorname{lc}(f)\cdot L_{t,v}}\cdot S_{f,q} &= \operatorname{lc}(q)\cdot\frac{L_{u,v}}{u}\cdot p \\
&\quad - \cancel{\frac{\operatorname{lc}(p)\cdot\operatorname{lc}(q)}{\operatorname{lc}(f)}\cdot\frac{L_{u,v}}{t}\cdot f} \\
&\quad + \cancel{\frac{\operatorname{lc}(p)\cdot\operatorname{lc}(q)}{\operatorname{lc}(f)}\cdot\frac{L_{u,v}}{t}\cdot f} \\
&\quad - \operatorname{lc}(p)\cdot\frac{L_{u,v}}{v}\cdot q \\
&= S_{p,q}.
\end{aligned}$$

□

How does this help us?

Corollary 11.9: *Let* $g_1, g_2, \ldots, g_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. *The following are equivalent.*

(A) $G = (g_1, g_2, \ldots, g_m)$ *is a Gröbner basis of the ideal* $I = \langle g_1, g_2, \ldots, g_m \rangle$.

(B) *For any pair* i, j *with* $1 \leq i < j \leq m$, *one of the following holds:*

(B1) The leading monomials of g_i and g_j have no common variables.

(B2) *There exists* k *such that*

- $\mathrm{lm}(g_k)$ *divides* $\mathrm{lcm}\left(\mathrm{lm}(g_i), \mathrm{lm}\left(g_j\right)\right)$;
- $\mathrm{Spol}(g_i, g_k)$ *has an S-representation with respect to* G; *and*
- $\mathrm{Spol}\left(g_k, g_j\right)$ *has an S-representation with respect to* G.

(B3) $\mathrm{Spol}\left(g_i, g_j\right)$ top-reduces to zero with respect to G.

PROOF: We need merely show that (B2) implies the existence of an S-representation of $\mathrm{Spol}\left(g_i, g_j\right)$ with respect to G; Lazard's characterization and the proof of Corollary 11.7 supply the rest. So assume (B2). Choose $h_1, h_2, \ldots, h_m$ such that

$$\mathrm{Spol}(g_i, g_k) = h_1 g_1 + \cdots + h_m g_m$$

and for each $\ell = 1, 2, \ldots, m$ we have $h_\ell = 0$ or

$$\mathrm{lm}(h_\ell)\,\mathrm{lm}(g_\ell) < \mathrm{lcm}(\mathrm{lm}(g_i), \mathrm{lm}(g_k)).$$

Also choose $q_1, q_2, \ldots, q_m$ such that

$$\mathrm{Spol}\left(g_k, g_j\right) = q_1 g_1 + \cdots + q_m g_m$$

and for each $\ell = 1, 2, \ldots, m$ we have $q_\ell = 0$ or

$$\mathrm{lm}(q_\ell)\,\mathrm{lm}(g_\ell) < \mathrm{lcm}\left(\mathrm{lm}(g_k), \mathrm{lm}\left(g_j\right)\right).$$

Write $L_{a,b} = \mathrm{lcm}(\mathrm{lm}(g_a), \mathrm{lm}(g_b))$. Buchberger's lcm criterion tells us that

$$\mathrm{Spol}\left(g_i, g_j\right) = \frac{\mathrm{lc}\left(g_j\right) \cdot L_{i,j}}{\mathrm{lc}(g_k) \cdot L_{i,k}} \cdot \mathrm{Spol}(g_i, g_k) + \frac{\mathrm{lc}(g_i) \cdot L_{i,j}}{\mathrm{lc}(g_k) \cdot L_{j,k}} \cdot \mathrm{Spol}\left(g_k, g_j\right).$$

For $i = 1, 2, \ldots, m$ let

$$H_i = \frac{\mathrm{lc}\left(g_j\right) \cdot L_{i,j}}{\mathrm{lc}(g_k) \cdot L_{i,k}} \cdot h_i + \frac{\mathrm{lc}(g_i) \cdot L_{i,j}}{\mathrm{lc}(g_k) \cdot L_{j,k}} \cdot q_i.$$

Substitution implies that

$$\operatorname{Spol}\left(g_i, g_j\right) = H_1 g_1 + \cdots + H_m g_m. \tag{34}$$

In addition, for each $i = 1, 2, \ldots, m$ we have $H_i = 0$ or

$$\begin{aligned}
\operatorname{lm}(H_i)\operatorname{lm}(g_i) &\leq \max\left(\frac{L_{i,j}}{L_{i,k}} \cdot \operatorname{lm}(h_i), \frac{L_{i,j}}{L_{j,k}} \cdot \operatorname{lm}(q_i)\right) \cdot \operatorname{lm}(g_i) \\
&= \max\left(\frac{L_{i,j}}{L_{i,k}} \cdot \operatorname{lm}(h_i)\operatorname{lm}(g_i), \frac{L_{i,j}}{L_{j,k}} \cdot \operatorname{lm}(q_i)\operatorname{lm}(g_i)\right) \\
&< \max\left(\frac{L_{i,j}}{\cancel{L_{i,k}}} \cdot \cancel{L_{i,k}}, \frac{L_{i,j}}{\cancel{L_{j,k}}} \cdot \cancel{L_{j,k}}\right) \\
&= L_{i,j} \\
&= \operatorname{lcm}\left(\operatorname{lm}(g_i), \operatorname{lm}\left(g_j\right)\right).
\end{aligned}$$

Thus equation (34) is an S-representation of $\operatorname{Spol}\left(g_i, g_j\right)$.

The remainder of the corollary follows as described. □

It is not hard to exploit Corollary 11.9 and modify Buchberger's algorithm in such a way as to take advantage of these criteria. The result is Algorithm 9. The only changes to Buchberger's algorithm are the addition of lines 8, 19, 12, and 13; they ensure that an S-polynomial is computed only if the corresponding pair does not satisfy one of the gcd or lcm criteria.

It is possible to exploit Buchberger's criteria more efficiently, using the Gebauer-Möller algorithm (Algorithms 10 and 11). This implementation attempts to apply Buchberger's criteria as quickly as possible. Thus the first `while` loop of Algorithm 11 eliminates new pairs that satisfy Buchberger's lcm criterion; the second `while` loop eliminates new pairs that satisfy Buchberger's gcd criterion; the third `while` loop eliminates *some* old pairs that satisfy Buchberger's lcm criterion; and the fourth `while` loop removes redundant elements of the basis in a safe way (see Exercise 10.62).

We will not give here a detailed proof that the Gebauer-Möller algorithm terminates correctly. That said, you should be able to see intuitively that it does so, and to fill in the details as well. Think carefully about why it is true. Notice that unlike Buchberger's algorithm, the pseudocode here builds critical pairs using elements (f, g) of G, rather than indices (i, j) of G.

For some time, the Gebauer-Möller algorithm was considered the benchmark by which other algorithms were measured. Many optimizations of the algorithm to compute a Gröbner basis can be applied to the Gebauer-Möller algorithm without lessening the effectiveness of Buchberger's criteria. Nevertheless, the Gebauer-Möller algorithm continues to reduce a large number of S-polynomials to zero.

Exercises.

Algorithm 9. Buchberger's algorithm with Buchberger's criteria

inputs
  $F = (f_1, f_2, \ldots, f_m)$, a list of polynomials in n variables, whose coefficients are from a field $\mathbb{F}$.
outputs
  $G = (g_1, g_2, \ldots, g_M)$, a Gröbner basis of $\langle F \rangle$. Notice $\#G = M$ which might be different from m.
do
  Let $G := F$
  Let $P = \{(f, g) : \forall f, g \in G \text{ such that } f \neq g\}$
  Let $Done = \{\}$
  repeat while $P \neq \emptyset$
    Choose $(f, g) \in P$
    Remove (f, g) from P
    if $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$ share at least one variable — check gcd criterion
      if not $(\exists p \neq f, g$ such that $\mathrm{lm}(p)$ divides $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ **and** $(p, f), (p, g) \in Done)$ — check lcm criterion
        Let S be the S-polynomial of f, g
        Let r be the top-reduction of S with respect to G
        if $r \neq 0$
          Replace P by $P \cup \{(h, r) : \forall h \in G\}$
          Append r to G
    Add (f, g) to $Done$
  return G

Algorithm 10. Gebauer-Möller algorithm

inputs
  $F = (f_1, f_2, \ldots, f_m)$, a list of polynomials in n variables, whose coefficients are from a field $\mathbb{F}$.
outputs
  $G = (g_1, g_2, \ldots, g_M)$, a Gröbner basis of $\langle F \rangle$. Notice $\#G = M$ which might be different from m.
do
  Let $G := \{\}$
  Let $P := \{\}$
  repeat while $F \neq \emptyset$
    Let $f \in F$
    Remove f from F
    — See Algorithm 11 for a description of Update
    $G, P :=$ Update (G, P, f)
  repeat while $P \neq \emptyset$
    Pick any $(f, g) \in P$, and remove it
    Let h be the top-reduction of Spol (f, g) with respect to G
    if $h \neq 0$
      $G, P :=$ Update (G, P, h)
  return G

Algorithm 11. Update the Gebauer-Möller pairs

inputs
  G_{old}, a list of polynomials in n variables, whose coefficients are from a field $\mathbb{F}$.
  P_{old}, a set of critical pairs of elements of G_{old}
  a non-zero polynomial p in $\langle G_{\text{old}} \rangle$
outputs
  G_{new}, a (possibly different) basis of $\langle G_{\text{old}} \rangle$.
  P_{old}, a set of critical pairs of G_{new}
do
  Let $C := \{(p,g) : g \in G_{\text{old}}\}$
  — C is the set of all pairs of the new polynomial p with an older element of the basis
  Let $D := \{\}$
  — D is formed by pruning pairs of C using Buchberger's lcm criterion
  — We do not yet check Buchberger's gcd criterion because with the original input there may be some cases of the lcm criterion that are eliminated by the gcd criterion
  repeat while $C \neq \emptyset$
    Pick any $(p,g) \in C$, and remove it
    if $\operatorname{lm}(p)$ and $\operatorname{lm}(g)$ share no variables **or** no $(p,h) \in C \cup D$ satisfies $\operatorname{lcm}(\operatorname{lm}(p),\operatorname{lm}(h)) \mid \operatorname{lcm}(\operatorname{lm}(p),\operatorname{lm}(g))$
      Add (p,g) to D
  Let $E := \emptyset$
  — E is the result of pruning pairs of D using Buchberger's gcd criterion
  repeat while $D \neq \emptyset$
    Pick any $(p,g) \in D$, and remove it
    if $\operatorname{lm}(p)$ and $\operatorname{lm}(g)$ share at least one variable
      $E := E \cup (p,g)$
  — P_{int} is the result of pruning pairs of P_{old} using Buchberger's lcm criterion
  Let $P_{\text{int}} := \{\}$
  repeat while $P_{\text{old}} \neq \emptyset$
    Pick $(f,g) \in P_{\text{old}}$, and remove it
    if $\operatorname{lm}(p)$ does not divide $\operatorname{lcm}(\operatorname{lm}(f),\operatorname{lm}(g))$ **or** $\operatorname{lcm}(\operatorname{lm}(p),\operatorname{lm}(h)) = \operatorname{lcm}(\operatorname{lm}(f),\operatorname{lm}(g))$ for $h \in \{f,g\}$
      Add (f,g) to P_{int}
  — Add new pairs to surviving pre-existing pairs
  $P_{\text{new}} := P_{\text{int}} \cup E$
  — Prune redundant elements of the basis, but not their critical pairs
  Let $G_{\text{new}} := \{\}$
  repeat while $G_{\text{old}} \neq \emptyset$
    Pick any $g \in G_{\text{old}}$, and remove it
    if $\operatorname{lm}(p)$ does not divide $\operatorname{lm}(g)$
      Add g to G_{new}
  Add p to G_{new}
  return $G_{\text{new}}, P_{\text{new}}$

Exercise 11.10: In Exercise 10.55 on page 264 you computed the Gröbner basis for the system

$$F = \left(x^2 + y^2 - 4, xy - 1\right)$$

in the lexicographic ordering using Algorithm 8 on page 266. Review your work on that problem, and identify which pairs (i, j) would not generate an S-polynomial if you had used Algorithm 9 on page 286 instead.

Exercise 11.11: Use the Gebauer-Möller algorithm to compute the Gröbner basis for the system

$$F = \left(x^2 + y^2 - 4, xy - 1\right).$$

Indicate clearly the values of the sets C, D, E, G_{new}, and P_{new} after each `while` loop in Algorithm 11 on the preceding page.

Exercise 11.12: Let t, u be two monomials, and x any variable. Show that

$$\deg_x \operatorname{lcm}(t, u) = \max\left(\deg_x t, \deg_x u\right).$$

Exercise 11.13: Study the proof of Buchberger's characterization, and extract from it a proof that (C) implies (A) in Theorem 11.5.

11.2: The F4 algorithm

An interesting development of the last ten years in the computation of Gröbner bases has revolved around changing the point of view to that of linear algebra. Recall from Exercise 10.68 that for any polynomial system we can construct a matrix whose triangularization simulates the computation of S-polynomials and top-reduction involved in the computation of a Gröbner basis. However, a naïve implementation of this approach is worse than Buchberger's method:

- every possible multiple of each polynomial appears as a row of a matrix;
- many rows do not correspond to S-polynomials, and so are useless for triangularization;
- as with Buchberger's algorithm, where most of the S-polynomials are not necessary to compute the basis, most of the rows that are not useless for triangularization are useless for computing the Gröbner basis!

Jean-Charles Faugère devised two algorithms that use the ordered Macaulay matrix to compute a Gröbner basis: F4 and F5. We focus on F4, as F5 requires more discussion than, quite frankly, I'm willing to put into these notes at this time.

Remark 11.14: F4 does not strictly require homogeneous polynomials, but for the sake of simplicity we stick with homogeneous polynomials, so as to introduce d-Gröbner bases.

Rather than build the entire ordered Macaulay matrix for any particular degree, Faugère first applied the principle of building only those rows that correspond to S-polynomials. Thus, given the homogeneous input

$$F = \left(x^2 + y^2 - 4h^2, xy - h^2\right),$$

the usual degree-3 ordered Macaulay matrix would be

$$\begin{pmatrix} x^3 & x^2y & xy^2 & y^3 & x^2h & xyh & y^2h & xh^2 & yh^2 & h^3 & \\ 1 & & 1 & & & & & -4 & & & xf_1 \\ & 1 & & 1 & & & & & -4 & & yf_1 \\ & & & & 1 & & 1 & & & -4 & hf_1 \\ & 1 & & & & & & -1 & & & xf_2 \\ & & 1 & & & & & & -1 & & yf_2 \\ & & & & & 1 & & & & -1 & hf_2 \end{pmatrix}.$$

However, only two rows of the matrix correspond to an S-polynomial: yf_1 and xf_2. For top-reduction we might need other rows: non-zero entries of rows yf_1 and xf_2 involve the monomials

$$y^3, xh^2, \text{ and } yh^2;$$

but no other row might reduce those monomials: that is, there is no top-reduction possible. We could, therefore, triangularize just as easily if we built the matrix

$$\begin{pmatrix} x^3 & x^2y & xy^2 & y^3 & x^2h & xyh & y^2h & xh^2 & yh^2 & h^3 & \\ & 1 & & 1 & & & & & -4 & & yf_1 \\ & 1 & & & & & & -1 & & & xf_2 \end{pmatrix}.$$

Triangularizing it results in

$$\begin{pmatrix} x^3 & x^2y & xy^2 & y^3 & x^2h & xyh & y^2h & xh^2 & yh^2 & h^3 & \\ & 1 & & 1 & & & & & -4 & & yf_1 \\ & & & 1 & & & & 1 & 4 & & yf_1 - xf_2 \end{pmatrix},$$

whose corresponds to the S-polynomial $yf_1 - xf_2$. We have thus generated a new polynomial,

$$f_3 = y^3 + xh^2 + 4yh^2.$$

Proceeding to degree four, there are two possible S-polynomials: for (f_1, f_3) and for (f_2, f_3). We can discard (f_1, f_3) thanks to Buchberger's gcd criterion, but not (f_2, f_3). Building the S-polynomial for (f_2, f_3) would require us to subtract the polynomials y^2f_2 and xf_3. The non-leading monomial of y^2f_2 is y^2h^2, and no leading monomial divides that, but the non-leading monomials of xf_3 are x^2h^2 and xyh^2, both of which are divisible by h^2f_1 and h^2f_2. The non-leading monomials of h^2f_1 are y^2h^2, for which we have already introduced a row, and h^4, which no leading monomial divides; likewise, the non-leading monomial of h^2f_2 is h^4.

We have now identified all the polynomials that *might* be necessary in the top-reduction of the S-polynomial for (f_2, f_3):

$$y^2f_2, xf_3, h^2f_1, \text{ and } h^2f_2.$$

We build the matrix using rows that correspond to these polynomials, resulting in

$$\begin{pmatrix} xy^3 & x^2h^2 & xyh^2 & y^2h^2 & h^2 & \\ 1 & & & -1 & & y^2f_2 \\ 1 & 1 & 4 & & & xf_3 \\ & 1 & & 1 & -4 & h^2f_1 \\ & & 1 & & -1 & h^2f_2 \end{pmatrix}.$$

Triangularizing this matrix results in (step-by-step)

$$\begin{pmatrix} xy^3 & x^2h^2 & xyh^2 & y^2h^2 & h^2 & \\ 1 & & & -1 & & y^2f_2 \\ & -1 & -4 & -1 & & y^2f_2 - xf_3 \\ & 1 & & 1 & -4 & h^2f_1 \\ & & 1 & & -1 & h^2f_2 \end{pmatrix};$$

$$\begin{pmatrix} xy^3 & x^2h^2 & xyh^2 & y^2h^2 & h^2 & \\ 1 & & & -1 & & y^2f_2 \\ & & -4 & 0 & -4 & y^2f_2 - xf_3 + h^2f_1 \\ & 1 & & 1 & -4 & h^2f_1 \\ & & 1 & & -1 & h^2f_2 \end{pmatrix};$$

and finally

$$\begin{pmatrix} xy^3 & x^2h^2 & xyh^2 & y^2h^2 & h^2 & \\ 1 & & & -1 & & y^2f_2 \\ & & & & 0 & y^2f_2 - xf_3 + h^2f_1 + 4h^2f_2 \\ & 1 & & 1 & -4 & h^2f_1 \\ & & 1 & & -1 & h^2f_2 \end{pmatrix}.$$

This corresponds to the fact that the S-polynomial of f_2 and f_3 reduces to zero: and we can now stop, as there are no more critical pairs to consider.

Aside from building a matrix, the F4 algorithm thus modifies Buchberger's algorithm (with the additional criteria, Algorithm 9 in the two following ways:

- rather than choose *a* critical pair in line 10, one chooses *all* critical pairs of minimal degree; and
- all the S-polynomials of this minimal degree are computed simultaneously, allowing us to reduce them "all at once".

In addition, the move to a matrix means that linear algebra techniques for triangularizing a matrix can be applied, although the need to preserve the monomial ordering implies that column swaps are forbidden. Algorithm 12 describes a simplified F4 algorithm. The approach outlined has an important advantage that we have not yet explained.

Algorithm 12. A simplified F4 that implements Buchberger's algorithm with Buchberger's criteria

inputs
  $F = (f_1, f_2, \ldots, f_m)$, a list of homogeneous polynomials in n variables, whose coefficients are from a field $\mathbb{F}$.
outputs
  $G = (g_1, g_2, \ldots, g_M)$, a Gröbner basis of $\langle F \rangle$. Notice $\#G = M$ which might be different from m.
do
  Let $G := F$
  Let $P := \{(f, g) : \forall f, g \in G \text{ such that } f \neq g\}$
  Let $Done := \{\}$
  Let $d := 1$
  repeat while $P \neq \emptyset$
    Let P_d be the list of all pairs $(i, j) \in P$ that generate S-polynomials of degree d
    Replace P with $P \backslash P_d$
    Denote $L_{p,q} := \operatorname{lcm}(\operatorname{lm}(p), \operatorname{lm}(q))$
    Let Q be the subset of P_d such that $(f, g) \in Q$ implies that:
    - $\operatorname{lm}(f)$ and $\operatorname{lm}(g)$ share at least one variable; and
    - **not** $(\exists p \in G \backslash \{f, g\}$ such that $\operatorname{lm}(p)$ divides $L_{f,g}$ **and** $(f, p), (g, p) \in Done)$

    Let $R := \left\{ tp, uq : (p, q) \in Q \text{ and } t = L_{p,q} / \operatorname{lm}(p), u = L_{p,q} / \operatorname{lm}(q) \right\}$
    Let S be the set of all tp where t is a monomial, $p \in G$, and $t \cdot \operatorname{lm}(p)$ is a non-leading monomial of some $q \in R \cup S$
    Let M be the submatrix of the ordered Macaulay matrix of F corresponding to the elements of $R \cup S$
    Let N be any triangularization of M that does not swap columns
    Let G_{new} be the set of polynomials that correspond to rows of N that changed from M
    for $p \in G_{\text{new}}$
      Replace P by $P \cup \{(h, p) : \forall h \in G\}$
      Add p to G
    Add (f, g) to $Done$
    Increase d by 1
  return G

Definition 11.15: Let G be a list of homogeneous polynomials, let $d \in \mathbb{N}^+$, and let I be a an ideal of homogeneous polynomials. We say that G is a **d-Gröbner basis of I** if $\langle G \rangle = I$ and for every $a \leq d$, every S-polynomial of degree a top-reduces to zero with respect to G.

Example 11.16: In the example given at the beginning of this section,

$$G = \left(x^2 + y^2 - 4h^2, xy - h^2, y^3 + xh^2 + 4yh^2\right)$$

is a 3-Gröbner basis. ◿

A Gröbner basis G is always a d-Gröbner basis for all $d \in \mathbb{N}$. However, not every d-Gröbner basis is a Gröbner basis.

Example 11.17: Let $G = \left(x^2 + h^2, xy + h^2\right)$. The S-polynomial of g_1 and g_2 is the degree 3 polynomial

$$S_{12} = yh^2 - xh^2,$$

which does not top-reduce. Let

$$G_3 = \left(x^2 + h^2, xy + h^2, xh^2 - yh^2\right);$$

the critical pairs of G_3 are

- (g_1, g_2), whose S-polynomial now reduces to zero;
- (g_1, g_3), which generates an S-polynomial of degree 4 (the lcm of the leading monomials is x^2h^2); and
- (g_2, g_3), which also generates an S-polynomial of degree 4 (the lcm of the leading monomials is xyh^2).

All degree 3 S-polynomials reduce to zero, so G_3 is a 3-Gröbner basis.

However, G_3 is *not* a Gröbner basis, because the pair (g_2, g_3) generates an S-polynomial of degree 4 that does *not* top-reduce to zero:

$$S_{23} = h^4 + y^2h^2.$$

Enlarging the basis to

$$G_4 = \left(x^2 + h^2, xy + h^2, xh^2 - yh^2, y^2h^2 + h^4\right)$$

gives us a 4-Gröbner basis, which is also the Gröbner basis of G. ◿

One useful property of d-Gröbner bases is that we can answer some question that require Gröbner bases by short-circuiting the computation of a Gröbner basis, settling instead for a d-Gröbner basis of sufficiently high degree. For our concluding theorem, we revisit the Ideal Membership Problem, discussed in Theorem 10.69.

Theorem 11.18: *Let $\mathcal{R}$ be a polynomial ring, let $p \in \mathcal{R}$ be a homogeneous polynomial of degree d, and let I be a homogeneous ideal of $\mathcal{R}$. The following are equivalent.*
(A) $p \in I$.
(B) *p top-reduces to zero with respect to a d-Gröbner G_d of I.*

PROOF: That (A) implies (B): If $p = 0$, then we are done; otherwise, let $p_0 = p$ and G_d be a d-Gröbner basis of I. Since $p_0 = p \in I$, there exist $h_1, \ldots, h_m \in \mathcal{R}$ such that

$$p_0 = h_1 g_1 + \cdots + h_m g_m.$$

Moreover, since p is of degree d, we can say that for every i such that the degree of g_i is larger than d, $h_i = 0$.

If there exists $i \in \{1, 2, \ldots, m\}$ such that $\operatorname{lm}(g_i)$ divides $\operatorname{lm}(p_0)$, then we are done. Otherwise, the equality implies that some leading terms on the right hand side cancel; that is, there exists at least one pair (i, j) such that $\operatorname{lm}(h_i)\operatorname{lm}(g_i) = \operatorname{lm}\left(h_j\right)\operatorname{lm}\left(g_j\right) > \operatorname{lm}(p_0)$. This cancellation is a multiple of the S-polynomial of g_i and g_j; by definition of a d-Gröbner basis, this S-polynomial top-reduces to zero, so we can replace

$$\operatorname{lc}(h_i)\operatorname{lm}(h_i)\, g_i + \operatorname{lc}\left(h_j\right)\operatorname{lm}\left(h_j\right) g_j = q_1 g_1 + \cdots + q_m g_m$$

such that each $k = 1, 2, \ldots, m$ satisfies

$$\operatorname{lm}(q_k)\operatorname{lm}(g_k) < \operatorname{lm}(h_i)\operatorname{lm}(g_i).$$

We can repeat this process any time that $\operatorname{lm}(h_i)\operatorname{lm}(g_i) > \operatorname{lm}(p_0)$. The well-ordering of the monomials implies that eventually we must arrive at a representation

$$p_0 = h_1 g_1 + \cdots + h_m g_m$$

where at least one k satisfies $\operatorname{lm}(p_0) = \operatorname{lm}(h_k)\operatorname{lm}(g_k)$. This says that $\operatorname{lm}(g_k)$ divides $\operatorname{lm}(p_0)$, so we can top-reduce p_0 by g_k to a polynomial p_1. Note that $\operatorname{lm}(p_1) < \operatorname{lm}(p_0)$.

By construction, $p_1 \in I$ also, and applying the same argument to p_1 as we did to p_0 implies that it also top-reduces by some element of G_d to an element $p_2 \in I$ where $\operatorname{lm}(p_2) < \operatorname{lm}(p_1)$. Iterating this observation, we have

$$\operatorname{lm}(p_0) > \operatorname{lm}(p_1) > \cdots$$

and the well-ordering of the monomials implies that this chain cannot continue indefinitely. Hence it must stop, but since G_d is a d-Gröbner basis, it does not stop with a non-zero polynomial. That is, p top-reduces to zero with respect to G.

That (B) implies (A): Since p top-reduces to zero with respect to G_d, Lemma 10.54 implies that $p \in I$. □

Exercises.

Exercise 11.19: Use the simplified F4 algorithm given here to compute a d-Gröbner bases for $\langle x^2y - z^2h, xz^2 - y^2h, yz^3 - x^2h^2\rangle$ for $d \leq 6$. Use the grevlex term ordering with $x > y > z > h$.

Exercise 11.20: Given a non-homogeneous polynomial system F, describe how you could use the simplified F4 to compute a non-homogeneous Gröbner basis of $\langle F\rangle$.

11.3: Signature-based algorithms to compute a Gröbner basis

This section is inspired by recent advances in the computation of Gröbner basis, including my own recent work. As with F4, the original algorithm in this area was devised by Faugère, and is named F5 [Fau02]. A few years later, Christian Eder and I published an article that showed how one could improve F5 somewhat [EP10]; the following year, the GGV algorithm was published [GGV10], and Alberto Arri asked me to help him finish an article that sought to generalize some notions of F5 [AP]. Seeing the similarities between Arri's algorithm and GGV, I teamed up with Christian Eder again to author a paper that lies behind this work [EP11]. The algorithm as presented here is intermediate between Arri's algorithm (which is quite general) and the one we present there (which is specialized).

In its full generality, the idea relies on a generalization of vector spaces.

Definition 11.21: Let R be a ring. A **module** M **over** R satisfies the following properties. Let $r, s \in R$ and $x, y, z \in M$. Then

- M is an additive group;
- $rx \in M$;
- $r(x+y) = rx + ry$;
- $(r+s)x = rx + sx$;
- $1_R x = x$.

We will not in fact use modules extensively, but the reader should be aware of the connection. In any case, it is possible to describe it at a level suitable for the intended audience of these notes (namely, me and any of my students whose research might lead in this direction). We adopt the following notation:

- $\mathcal{R} = \mathbb{F}[x_1, \ldots, x_n]$ is a polynomial ring;
- $\mathbb{M}$ the set of monomials of $\mathcal{R}$;
- $\prec$ a monomial ordering;
- $f_1, \ldots, f_m \in \mathcal{R}$;
- $F = (f_1, \ldots, f_m)$;
- $I = \langle F\rangle$.

Definition 11.22: Let $p \in I$ and $h_1, \ldots, h_m \in \mathcal{R}$. We say that $H = (h_1, \ldots, h_m)$ is an F**-representation of** p if

$$p = h_1 f_1 + \cdots + h_m f_m.$$

If, in addition, $p = 0$, then we say that H is a **syzygy** of F.[a]

[a] It can be shown that the set of all syzygies is a module over $\mathcal{R}$, called the **module of syzygies**.

Example 11.23: Suppose $F = \left(x^2 + y^2 - 4, xy - 1\right)$. Recall that $p = x + y^3 - 4y \in \langle F \rangle$, since

$$x + y^3 - 4y = y f_1 - x f_2.$$

In this case, (y, x) is not an S-representation of p, since $y\operatorname{lm}(f_1) = x^2 y = \operatorname{lcm}\left(x^2, xy\right)$. However, it is an F-representation.

On the other hand,

$$0 = f_2 f_1 - f_1 f_2 = (xy - 1) f_1 - \left(x^2 + y^2 - 4\right) f_2,$$

so $(f_2, -f_1)$ is an F-representation of 0; that is, $(f_2, -f_1)$ is a syzygy. ◿

Keep in mind that an F-representation is almost never an S-representation (Definition 11.6). However, an F-representation exists for any element of I, even if F is not a Gröbner basis. An S-representation does *not* exist for at least one S-polynomial when F is not a Gröbner basis.

We now generalize the notion of a leading monomial of a *polynomial* to a leading monomial of an F-representation.

Definition 11.24: Write $\mathbf{F}_i$ for the m-tuple whose entries are all zero *except* for entry i, which is 1.[a] Given an F-representation H of some $p \in I$, whose rightmost nonzero entry occurs in position i, we say that $\operatorname{lm}(h_i)\mathbf{F}_i$ is a **leading monomial of** H, and write $\operatorname{lm}(H) = \operatorname{lm}(h_i)\mathbf{F}_i$. Let

$$\mathbb{S} = \{\operatorname{lm}(H) : h_1 f_1 + \cdots + h_m f_m \in I\};$$

that is, $\mathbb{S}$ is the set of all possible leading monomials of an F-representation.

[a] In the parlance of modules, $\{\mathbf{F}_1, \ldots, \mathbf{F}_m\}$ is the set of **canonical generators** of the free $\mathcal{R}$-module $\mathcal{R}^m$.

Example 11.25: Recall F from Example 11.23. We have $\mathbf{F}_1 = (1, 0)$ and $\mathbf{F}_2 = (0, 1)$. The leading monomial of $(y, 0)$ is $y\mathbf{F}_1$. The leading monomial of (y, x) is $x\mathbf{F}_2 = (0, x)$. The leading monomial of $(f_2, -f_1)$ is $\operatorname{lm}(-f_1)\mathbf{F}_2 = \left(0, x^2\right)$. ◿

Once we have leading monomials of F-representations, it is natural to generalize the ordering of monomials of $\mathbb{M}$ to an ordering of leading monomials.

Definition 11.26: Define a relation $\prec$ on $\mathbb{S}$ as follows: we say that $t\mathbf{F}_i \prec u\mathbf{F}_j$ if
- $i < j$, or
- $i = j$ and $t \lessdot u$.

Lemma 11.27: *$\prec$ is a well-ordering of $\mathbb{S}$.*

PROOF: Let $S \subseteq \mathbb{S}$. Since $<$ is a well-ordering of $\mathbb{N}^+$, there exists a minimal $i \in \mathbb{N}^+$ such that $t\mathbf{F}_i \in S$ for any $t \in \mathbb{M}$. Let $T = \{t : t\mathbf{F}_i \in S\}$; notice that $T \subseteq \mathbb{M}$. Since $\lessdot$ is a well-ordering of $\mathbb{M}$, T has a least element t. By definition, $t\mathbf{F}_i \preceq u\mathbf{F}_j$ for any $u\mathbf{F}_j \in S$.\ □

Corollary 11.28: *Let $p \in I$ and $\mathcal{H}$ the set of all possible F-representations of p. Let*

$$S = \{\mathrm{lm}(H) : H \in \mathcal{H}\}.$$

Then S has a smallest element with respect to $\prec$.

PROOF: $S \subset \mathbb{S}$, which is well ordered by $\prec$. □

Definition 11.29: We call the smallest element of S the **signature of** p, denoted by $\mathrm{sig}(p)$.

Now let's consider how the ordering behaves on some useful operations with F-representations. First, some notation.

Definition 11.30: If $t \in \mathbb{M}$ and $H, H' \in \mathcal{R}^m$, we define

$$tH = (th_1, \ldots, th_m) \text{ and } H + H' = \left(h_1 + h'_1, \ldots, h_m + h'_m\right).$$

In addition, we define $t\,\mathrm{sig}(p) = t\,(u\mathbf{F}_i) = (tu)\,\mathbf{F}_i$.

Lemma 11.31: *Let $p, q \in I$, H an F-representation of f, H' an F-representation of q, and $t, u \in \mathbb{M}$. Suppose $\tau = \operatorname{lm}(H)$ and $\upsilon = \operatorname{lm}(H')$. Each of the following holds.*

(A) tH *is an F-representation of tp;*

(B) $\operatorname{sig}(tp) \preceq t\tau = \operatorname{lm}(tH)$;

(C) if $t\tau \prec u\upsilon$, *then* $\operatorname{lm}\left(tH \pm uH'\right) = u\upsilon$;

(D) if $t\tau = u\upsilon$, *then there exists* $c \in \mathbb{F}$ *such that* $\operatorname{lm}\left(ctH + uH'\right) \prec t\tau$.

(E) if $\operatorname{Spol}(p,q) = atp - buq$ *for appropriate* $a, b \in \mathbb{F}$, *then* $\operatorname{sig}(\operatorname{Spol}(p,q)) \preceq \max(t\tau, u\upsilon)$;

(F) if H'' is an F-representation of p and $\operatorname{lm}\left(H''\right) \prec \operatorname{lm}(H)$, *then there exists a syzygy* $Z \in \mathcal{R}^m$ *such that*

- $H'' + Z = H$ *and*
- $\operatorname{lm}(Z) = \operatorname{lm}(H)$;

and

(G) if H'' is an F-representation of p such that $\operatorname{lm}\left(H''\right) = \operatorname{sig}(p)$, *then* $\operatorname{lm}\left(H''\right) < \operatorname{lm}(H)$ *if and only if there exists a nonzero syzygy Z such that* $H'' + Z = H$ *and* $\operatorname{lm}(Z) = \operatorname{lm}(H)$.

It is important to note that even if $t\tau = \operatorname{lm}(tH)$, that does not imply that $t\tau = \operatorname{sig}(tp)$ even if $\tau = \operatorname{sig}(p)$.

PROOF: (A) Since H is an F-representation of p, we know that $p = \sum h_i f_i$. By the distributive and associative properties, $tp = t\sum h_i f_i = \sum[(th_i) f_i]$. Hence tH is an F-representation of tp.

(B) The definition of a signature implies that $\operatorname{sig}(tp) \preceq t\tau$. That $t\tau = \operatorname{lm}(tH)$ is a consequence of (A).

(C) Assume $t\tau \prec u\upsilon$. Write $\tau = v\mathbf{F}_i$ and $\upsilon = w\mathbf{F}_j$. By definition of the ordering $\prec$, either $i < j$ or $i = j$ and $\operatorname{lm}(h_i) \lessdot \operatorname{lm}\left(h'_j\right)$. Either way, $\operatorname{lm}\left(tH \pm uH'\right)$ is $u\operatorname{lm}\left(h'_j\right)\mathbf{F}_j = u\upsilon$.

(D) Assume $t\tau = u\upsilon$. Let $a = \operatorname{lc}(H)$, $b = \operatorname{lc}\left(H'\right)$, and $c = b/a$. Then $\operatorname{lm}(tH) = t\tau = u\upsilon = \operatorname{lm}\left(uH'\right)$, and $c\operatorname{lc}(tH) = \operatorname{lc}\left(uH'\right)$. Together, these imply that the leading monomials of ctH and uH' cancel in the subtraction $ctH - uH'$. Hence $\operatorname{lm}\left(ctH - uH'\right) \prec t\tau$.

(E) follows from (B), (C), and (D).

(F) Assume that H'' is an F-representation of p and $\operatorname{lm}\left(H''\right) \prec \operatorname{lm}(H)$. Then

$$0 = p - p = \sum h_i f_i - \sum h''_i f_i = \sum \left(h_i - h''_i\right) f_i.$$

Let $Z = \left(h_1 - h''_1, \ldots, h_m - h''_m\right)$. By definition, Z is a sygyzy. In addition, $\operatorname{lm}\left(H''\right) \prec \operatorname{lm}(H)$ and (C) imply that $\operatorname{lm}(Z) = \operatorname{lm}(H)$.

(G) One direction follows from (F); the other is routine. □

We saw in previous sections that if we considered critical pairs by ascending lcm, we were able to take advantage of previous computations to reduce substantially the amount of work

needed to compute a Gröbner basis. It turns out that we can likewise reduce the amount of work substantially if we proceed by ascending signature. This will depend on an important fact.

Definition 11.32: Let $p \in I$, and H an S-representation of p. If $\operatorname{lm}(h_k)\operatorname{sig}(g_k) \preceq \operatorname{lm}(p)$ for each k, then we say that H is a **signature-compatible representation** of p, or a **sig-representation** for short.

Lemma 11.33: *Let $\tau \in \mathbb{S}$, and suppose that every S-polynomial of $G \subsetneq I$ with signature smaller than τ has a sig-representation. Let $p, q \in I$ and $t, u \in \mathbb{M}$ such that $u\operatorname{sig}(q) \preceq t\operatorname{sig}(p) = \tau$, $\operatorname{Spol}(p,q) = \operatorname{lc}(q)\,tp - \operatorname{lc}(p)\,uq$. Suppose that one of the following holds:*
(A) $\operatorname{sig}(tp) = \operatorname{sig}(uq)$*; or*
(B) $t\operatorname{sig}(p) \neq \operatorname{sig}(\operatorname{Spol}(p,q))$.
Then $\operatorname{Spol}(p,q)$ *has a sig-representation.*

PROOF: (A) Let H and H' be F-representations of p and q (respectively) such that $\operatorname{lm}(H) = \operatorname{sig}(p)$ and $\operatorname{lm}(H') = \operatorname{sig}(q)$. By Lemma 11.31(D), there exists $c \in \mathbb{F}$ satisfying the property $\operatorname{lm}(ctH + uH') \prec \operatorname{lm}(ctH)$; in other words, $\operatorname{sig}(ctp + uq) \prec \operatorname{sig}(tp)$. Let H'' be an F-representation of $ctp + uq$ such that $\operatorname{lm}(H'') = \operatorname{sig}(ctp + uq)$; by hypothesis, all top-cancellations of the sum

$$h''_1 f_1 + \cdots + h''_m f_m$$

have sig-representations. The fact that the top-cancellations have signature smaller than τ implies that we can rewrite these top-cancellations repeatedly as long as they exist. Each rewriting leads to smaller leading monomials, and signatures no larger than those of the top-cancellations. Since the monomial ordering is a well ordering, we cannot rewrite these top-cancellations indefinitely. Hence this process of rewriting eventually terminates with a sig-representation of $ctp + uq$. If $ctp + uq$ is a scalar multiple of $\operatorname{Spol}(p,q)$, then we are done; notice $\operatorname{sig}(\operatorname{Spol}(p,q)) \prec t\operatorname{sig}(p)$.

If $ctp + uq$ is not a scalar multiple of $\operatorname{Spol}(p,q)$, then $\operatorname{sig}(\operatorname{Spol}(p,q)) = t\operatorname{sig}(p) = \tau$. Consider the fact that $c\operatorname{Spol}(p,q) = \operatorname{lc}(q)(ctp + uq) - (c\operatorname{lc}(p) + \operatorname{lc}(q))\,uq$. One summand on the right hand side is a scalar multiple of q, so it has a sig-representation no larger than $u\operatorname{sig}(q) \prec \tau$. The previous paragraph showed that $ctp + uq$ has a sig-representation smaller than τ. The sum of these sig-representations is also a sig-representation no larger than τ. Hence the left hand side has an F-representation H''' with $\operatorname{lm}(H''') \preceq \tau$.

(B) By part (A), we know that if $u\operatorname{sig}(q) = t\operatorname{sig}(p)$, then $\operatorname{Spol}(p,q)$ has a sig-representation. Assume therefore that $u\operatorname{sig}(q) \prec t\operatorname{sig}(p) = \tau$. Since $t\operatorname{sig}(p) \neq \operatorname{sig}(tp)$, Lemma 11.31 implies that $\operatorname{sig}(tp) \prec t\operatorname{sig}(p) = \tau$. Likewise, $\operatorname{sig}(uq) \preceq u\operatorname{sig}(q) \prec \tau$, so

$$\operatorname{sig}(\operatorname{Spol}(p,q)) \preceq \max(\operatorname{sig}(tp), \operatorname{sig}(uq)) \prec \tau.$$

The hypothesis implies that $\operatorname{Spol}(p,q)$ has a sig-representation. □

To compute a Gröbner basis using signatures, we have to reduce polynomials in such a way that we have a good estimate of the signature. To do this, we cannot allow a reduction

Algorithm 13. Signature-based algorithm to compute a Gröbner basis

inputs
  $F \subsetneq \mathcal{R}$
outputs
  $G \subsetneq \mathcal{R}$, a Gröbner basis of $\langle F \rangle$
do
  Let $G = \{(\mathbf{F}_i, f_i)\}_{i=1}^{m}$
  Let $\mathcal{S} = \left\{ \operatorname{lm}\left(f_j\right) \mathbf{F}_i : 1 \leq j < i \right\}_{i=1}^{m}$
  Let $P = \left\{ (\upsilon, p, q) : (\sigma, p), (\tau, q) \in G \text{ and } \upsilon \text{ is the expected signature of Spol}\,(p,q) \right\}$
  repeat while $P \neq \emptyset$
    Select any $(\sigma, p, q) \in P$ such that τ is minimal
    Let $S = \operatorname{Spol}(p,q)$
    if $\exists\, (\tau, g) \in G$, $t \in \mathbb{M}$ such that $t\tau = \sigma$ and $t \operatorname{lm}(g) \leq \operatorname{lm}(S)$
      if σ is not a monomial multiuple of any $\tau \in \mathcal{S}$
        Top-reduce S to r over G in such a way that $\operatorname{sig}(r) \preceq \sigma$
        if $r \neq 0$ and r is not sig-redundant to G
          for $(\tau, g) \in G$
            if $g \neq 0$ and $t\sigma \neq u\tau$, where t and u are the monomials needed to construct $\operatorname{Spol}(r,g)$
              Add (υ, r, g) to P, where υ is the expected signature of $\operatorname{Spol}(r,g)$
        else
          Add σ to $\mathcal{S}$
  return $\{ g : (\tau, g \in G) \text{ and } g \neq 0 \}$

$r - tg$ if $\operatorname{sig}(r) \preceq t\operatorname{sig}(g)$; otherwise, we have no way to recuperate $\operatorname{sig}(r)$. Thus, a signature-based algorithm to compute a Gröbner basis can sometimes add redundant polynomials to the basis. Recall that termination of the Gröbner basis algorithms studied so far follows from the property of those algorithms that r was not added to a basis if it was redundant. This presents us with a problem. The solution looks like a natural generalization, but it took several years before someone devised it.

Definition 11.34: Let $G = \{(\tau_k, g_k)\}_{k=1}^{\ell}$ for some $\ell \in \mathbb{N}^+$, $g_k \in I$, and $\tau_k \in \mathbb{S}$, satisfying $\tau_k = \operatorname{sig}(g_k)$ for each k. We say that (σ, r) is **signature-redundant**, or **sig-redundant**, if there exists $(\tau, g) \in G$ such that $\tau \mid \sigma$ and $\operatorname{lm}(g) \mid \operatorname{lm}(r)$.

Algorithm 13 uses these ideas to compute a Gröbner basis of an ideal.

Theorem 11.35: *Algorithm 13 terminates correctly.*

PROOF: To see why the algorithm terminates, let $\mathbb{M}'$ be the set of variables in $x_1, \ldots, x_n$ *and* $x_{n+1}, \ldots, x_n$, and define two functions

- $\psi : \mathbb{M} \to \mathbb{M}'$ by $\psi\left(x_1^{\alpha_1} \cdots x_n^{\alpha_n}\right) = x_{n+1}^{\alpha_1} \cdots x_{2n}^{\alpha_n}$, and
- $\varphi : G \to \left(\mathbb{M}'\right)^m$ by $\varphi\left(u\mathbf{F}_i, g\right) = \left(u \cdot \psi\left(\operatorname{lm}(g)\right)\right)\mathbf{F}_i$.

Notice that the variable shift imposed by ψ implies that $\varphi\left(u\mathbf{F}_i, g\right)$ divides $\varphi\left(u'\mathbf{F}_i, g'\right)$ if and only if $u \mid u'$ and $\operatorname{lm}(g) \mid \operatorname{lm}\left(g'\right)$. This is true if and only if $\left(u'\mathbf{F}_i, g'\right)$ is sig-redundant with $\left(u\mathbf{F}_i, g\right)$, which contradicts how the algorithm works! Let J be the ideal generated by $\varphi(G)$ in $\left(\mathbb{M}'\right)^m$. As we just saw, adding elements to G implies that we expand some component of J. However, Proposition 8.34 and Definition 8.32 imply that the components of J can expand only finitely many times. Hence the algorithm can add only finitely many elements to G, which implies that it terminates.

For correctness, we need to show that the output satisfies the criteria of Lemma 11.33. Lines 12, 13, and 17 are the only ones that could cause a problem.

For line 12, suppose $(\tau, g) \in G$ and $t \in \mathbb{M}$ satisfy $t\tau = \sigma$ and $t\operatorname{lm}(g) \leq \operatorname{lm}(\operatorname{Spol}(p,q))$. Let $H, H' \in \mathcal{R}^m$ be F-representations of $S = \operatorname{Spol}(p,q)$ and g, respectively. We can choose H and H' such that $\operatorname{lm}(H) = \sigma$ and $\operatorname{lm}\left(H'\right) = \tau$. By Lemma 11.31, there exists $c \in \mathbb{F}$ such that $\operatorname{sig}(cS + tg) \prec \sigma$. On the other hand, $t\operatorname{lm}(g) < \operatorname{lm}(S)$ implies that $\operatorname{lm}(cS + tg) = \operatorname{lm}(S)$. The algorithm proceeds by ascending signature, so $cS + tg$ has a sig-representation H'' (over G, not F). Thus,

$$cS + tg = \sum h_k'' g_k \quad \Longrightarrow \quad S = -c^{-1} tg + \sum \left(c^{-1} h_k''\right) g_k$$

Every monomial of H'' is, by definition of a sig-representation, smaller than $\operatorname{lm}(cS + tg) = \operatorname{lm}(S)$. In addition, $\operatorname{sig}(tg) \preceq \sigma$, and $\operatorname{sig}\left(h_k'' g_k\right) \prec \sigma$ for each k. Define

$$\widehat{h}_k = \begin{cases} c^{-1}\widehat{h}_k, & g \neq g_k; \\ c^{-1}\left(\widehat{h}_k - t\right), & g = g_k. \end{cases}$$

Then $\widehat{H} = \left(\widehat{h}_1, \ldots, \widehat{h}_{\#G}\right)$ is a sig-representation of $\operatorname{Spol}(p,q)$.

For line 13, inspection of the algorithm shows that either $\tau = \operatorname{lm}\left(f_j\right)\mathbf{F}_i$ for some $j < i$, or $\left(\tau, \widehat{p}, \widehat{q}\right)$ was selected from P, and the algorithm reduced $\operatorname{Spol}\left(\widehat{p}, \widehat{q}\right)$ to zero. In the first case, suppose $\sigma = u\mathbf{F}_i$. Let $H \in \mathcal{R}^m$ an F-representation of $\operatorname{Spol}(p,q)$ such that $\operatorname{lm}(H) = \sigma$, and $t \in \mathbb{M}$ such that $t\operatorname{lm}\left(f_j\right)\mathbf{F}_i = \sigma$. Let $Z \in \mathcal{R}^m$ such that

$$z_k = \begin{cases} f_i, & k = j; \\ -f_j, & k = i; \\ 0, & \text{otherwise.} \end{cases}$$

Observe that Z is a syzygy, since $\sum z_\ell f_\ell = f_i f_j + \left(-f_j\right) f_i = 0$. In addition, $j < i$ so $\operatorname{lm}(Z) =$

$\operatorname{lm}\left(f_j\right)\mathbf{F}_i$. Thus

$$\operatorname{Spol}(p,q) = \operatorname{Spol}(p,q) + t\sum z_\ell f_\ell = \operatorname{Spol}(p,q) + \sum (t z_\ell) f_\ell.$$

The right hand side has signature smaller than σ (look at $H + Z$), so the left hand side must, as well. By Lemma 11.33, $\operatorname{Spol}(p,q)$ has a sig-representation.

In the second case, we have some $(\tau, \widehat{p}, \widehat{q})$ selected from P whose S-polynomial reduced to zero, and some $t \in \mathbb{M}$ such that $t\tau = \sigma$. Since the reduction respects the signature τ, there exists a sig-representation H of $\operatorname{Spol}(\widehat{p}, \widehat{q})$; that is,

$$\operatorname{Spol}(\widehat{p}, \widehat{q}) = \sum h_\ell g_\ell$$

and $\operatorname{sig}(h_\ell g_\ell) \prec \tau$ for each $\ell = 1, \ldots, \#G$. Thus $\operatorname{Spol}(\widehat{p}, \widehat{q}) - \sum h_\ell g_\ell = 0$. This implies the existence of a syzygy $Z \in \mathcal{R}^m$ such that $\operatorname{lm}(Z) = \operatorname{sig}\left(\operatorname{Spol}(\widehat{p}, \widehat{q}) - \sum h_\ell g_\ell\right) = \tau$. Thus

$$\operatorname{Spol}(p,q) = \operatorname{Spol}(p,q) - t\sum z_\ell f_\ell = \operatorname{Spol}(p,q) - \sum (t z_\ell) f_\ell,$$

but the right side clearly has signature smaller than σ, so the left hand side must, as well. By Lemma 11.33, $\operatorname{Spol}(p,q)$ has a sig-representation.[30]

For line 17, let $(\tau, g) \in G$ such that $\tau \mid \sigma$ and $\operatorname{lm}(g) \mid \operatorname{lm}(r)$. Let $t, u \in \mathbb{M}$ such that $t\tau = \sigma$ and $u\operatorname{lm}(g) = \operatorname{lm}(r)$. If $u < t$, then $u\tau \prec \sigma$, which contradicts the hypothesis that (σ, r) completed a reduction that respects the signature. Otherwise, $t \leq u$, which implies that $t\tau = \sigma$ and $t\operatorname{lm}(g) \leq \operatorname{lm}(r) \leq \operatorname{lm}(\operatorname{Spol}(p,q))$. In this case, an argument similar to the one for line 12 applies. □

[30] Notice that both cases for line 13 use syzygies. This is why $\mathcal{S}$ has that name: $\mathcal{S}$ for syzygy.

Appendices

0

Where can I go from here?

Advanced group theory

Galois theory [Rot98], representation theory, other topics [AF05, Rot06]

Advanced ring theory

Commutative algebra [GPS05], algebraic geometry [CLO97, CLO98], non-commutative algebra

Applications

General [LP98], coding theory, cryptography, computational algebra [vzGG99]

Hints to Exercises

Hints to Chapter 1

Exercise 1.21: Since you have to prove something for any subset of $\mathbb{Z}$, give it a name: let S be any subset of $\mathbb{Z}$. Then explain why any two elements $a, b \in S$ satisfy $a < b$, $a = b$, or $a > b$. If you think about the definition of a subset in the right way, your proof will be a lot shorter than the proof of Theorem 1.15.

Exercise 1.24: Try to show that $a - b = 0$.

Exercise 1.25: Use the definition of $<$.

Exercise 1.27: Use Exercise 1.26(c).

Exercise 1.28: Let m, n be two smallest elements of S. Since m is a smallest element of S, what do you know about m and n? Likewise, since n is a smallest element of S, what do you know about m and n? Then...

Exercise 1.29: Pick an example $n, d \in \mathbb{Z}$ and look at the resulting M. Which value of q gives you an element of $\mathbb{N}$ as well? If $n \in \mathbb{N}$ then you can easily identify such q. If $n < 0$ it takes a little more work.

Exercise 1.30: Here, "smallest" doesn't mean what you think of as smallest; it means smallest with respect to the definition. That is, you have to explain why there does *not* exist $a \in \mathbb{N}$ such that for all other $b \in \mathbb{N}$, we have $a > b$.

Exercise 1.31: This question is really asking you to find a new ordering $\prec$ of $\mathbb{Q}$ that is a linear ordering *and* that behaves the same on $\mathbb{Z}$ as $<$. To define $\prec$, choose $p, q \in \mathbb{Q}$. By definition, there exist $a, b, c, d \in \mathbb{Z}$ such that $p = a/b$ and $q = c/d$. What condition can you place on $ad - bc$ that would (a) order p and q, and (b) remain compatible with $<$ in $\mathbb{Z}$ in case $p, q \in \mathbb{Z}$ as well?

Exercise 1.50: Don't confuse what you have to do here, or what the elements are. You have to work with elements of $P(S)$; these are *subsets of* S. So, if I choose $X \in P(S)$, I know that $X \subseteq S$. Notice that I use capital letters for X, even though it is an element of $P(S)$, precisely because it is a set. This isn't something you *have* to do, strictly speaking, but you might find it helpful to select an element of X to prove at least one of the properties of a monoid, and it looks more natural to select $x \in X$ than to select $a \in x$, even if this latter x is a set.

Exercise 1.53: To show closure, you have to explain how we know that the set specified in the definition of lcm has a minimum.

Exercise 1.68: By Definition 1.3, you have to show that

- for any monoid M, $M \cong M$ (reflexive);
- for any two monoids M and N, if $M \cong N$, then also $N \cong M$ (symmetric); and

- for any three monoids M, N, and P, if $M \cong N$ and $N \cong P$, then $M \cong P$ (transitive).

In the first case, you have to find an isomorphism $f : M \longrightarrow M$. In the second, you have to assume that there exist isomorphisms $f : M \longrightarrow N$, then show that there exists an isomorphism $f : N \longrightarrow M$.

Hints to Chapter 2

Exercise 2.14: Remember that $-$ means the additive inverse. So, you have to show that the additive inverse of $-x$ is x.

Exercise 2.16: Use substitution.

Exercise 2.17: Work with arbitrary elements of $\mathbb{R}^{2\times 2}$. The structure of such elements is

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad \text{where } a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{R}.$$

Exercise 2.21: At least one such monoid appears in the exercises to this section.

Exercise 2.25: You probably did this in linear algebra, or saw it done. Work with arbitrary elements of $\mathbb{R}^{m\times m}$, which have the structure

$$A = \left(a_{i,j}\right)_{i=1\ldots m, j=1\ldots m}.$$

Exercise 2.77: You will need the condition that $16a^3 = 27c^2$.

Exercise 2.78: For closure, it suffices to show that each line between two distinct, finite points of the curve intersects the curve a third time, possibly at P_∞.

Exercise 2.79: You may want to use a computer algebra system to help with this. In the appendix to this section we show how you can do it with the computer algebra system Sage.

Exercise 2.27:

(a) Try $m = 2$, and find two invertible matrices A, B such that $(AB)\left(A^{-1}B^{-1}\right) \neq I_2$.

(b) Use the associative property to help simplify the expression $(ab)\left(b^{-1}a^{-1}\right)$.

Exercise 2.33: Exercise 2.27 on page 32 is similar.

Exercise 2.34: You may assume that composition of functions is associative in this problem.

(a) Use the fact that $(F \circ F)(P) = F(F(P))$ to show that $(F \circ F)(P) = I(P)$, and repeat with the other functions.

(b) One of closure, identity, or inverse fails. Which?

(c) Add elements to G that are lacking, until all the properties are now satisfied.

(d) A clever argument would avoid a brute force computation.

Exercise 2.80: This goes a lot faster if you work with approximate numbers.

Exercise 2.59: Use the product notation as we did.

Exercise 2.60: Use Theorem 2.56.

Exercise 2.61: Look back at Exercise 2.30 on page 32.

Exercise 2.64: Use denominators to show that no matter what you choose for $x \in \mathbb{Q}$, there is some $y \in \mathbb{Q}$ such that $y \notin \langle x \rangle$.

Exercise 2.65: One possibility is to exploit $\det(AB) = \det A \cdot \det B$. It helps to know that $\mathbb{R}$ is not cyclic (which may not be obvious, but should make sense from Exercise 2.64).

Exercise 2.43: To rewrite products so that ρ never precedes φ, use Corollary 2.40. To show that D_3 satisfies the properties of a group, you may use the fact that D_3 is a subset of $\mathrm{GL}(2)$, the multiplicative group of 2×2 invertiable matrices. Thus D_3 "inherits" certain properties of $\mathrm{GL}(2)$, but which ones? For the others, simple inspection of the multiplication table should suffice.

Exercise 2.45:

(a) You may use the property that $|P - Q|^2 = |P|^2 + |Q|^2 - 2P \cdot Q$, where $|X|$ indicates the distance of X from the origin, and $|X - Y|$ indicates the distance between X and Y.

(c) Use the hint from part (a), along with the result in part (a), to show that the distance between the vectors is zero. Also use the property of dot products that for any vector X, $X \cdot X = |X|^2$. Don't use part (b).

Exercise 2.46: Let $P = (p_1, p_2)$ be an arbitrary point in $\mathbb{R}^2$, and assume that ρ leaves it stationary. You can represent P by a vector. The equation $\rho \cdot \vec{P} = \vec{P}$ gives you a system of two linear equations in two variables; you can solve this system for p_1 and p_2.

Exercise 2.47: Repeat what you did in Exercise 2.46. This time the system of linear equations will have infinitely many solutions. You know from linear algebra that in $\mathbb{R}^2$ this describes a line. Solve one of the equations for p_2 to obtain the equation of this line.

Hints to Chapter 3

Exercise 3.13: Start with the smallest possible subgroup, then add elements one at a time. Don't forget the adjective "proper" subgroup.

Exercise 3.15: Look at what L has in common with H from Example 3.8.

Exercise 3.19: Use Exercise 2.64 on page 47.

Exercise 3.21: Look at Exercise 3.18 on page 58.

Exercise 3.37: For (CE1), you have to show that two sets are equal. Follow the structure of the proof for Theorem 3.28 on page 61. Take an arbitrary element of eH, and show that it also an element of H; that gives $eH \subseteq H$. Then take an arbitrary element of H, and show that it is an element of eH; that gives $eH \supseteq H$. The two inclusions give $eH = H$.

As for (CE2) and (CE3), you can prove them in a manner similar to that of (CE1), or you can explain how they are actually consequences of (CE1).

Exercise 3.50: Use Corollary 3.46 on page 66.

Exercise 3.51: See Exercises 2.61 on page 47 and 3.50.

Exercise 3.69: Theorem 3.57 tells us that the subgroup of an abelian group is normal. If you can show that $D_m(\mathbb{R})$ is abelian, then you are finished.

Exercise 3.71: It is evident from the definition that $Z(G) \subseteq G$. You must show first that $Z(G) < G$. Then you must show that $Z(G) \triangleleft G$. Make sure that you separate these steps and justify each one carefully!

Exercise 3.72: First you must show that $H \subseteq N_G(H)$. Then you must show that $H < N_G(H)$. Finally you must show that $H \triangleleft N_G(H)$. Make sure that you separate these steps and justify each one carefully!

Exercise 3.73: List the two left cosets, then the two right cosets. What does a partition mean? Given that, what sets must be equal?

Exercise 3.74(c): The "hard" way is to show that for all $g \in G$, $g[G,G] = [G,G]g$. This requires you to show that two sets are equal. Any element of $[G,G]$ has the form $[x,y]$ for some $x,y \in G$. At some point, you will have to show that $g[x,y] = [w,z]g$ for some $w,x \in G$. This is an existence proof, and it suffices to construct w and z that satisfy the equation. To construct them, think about conjugation.

An "easier" way uses the result of Exercise 3.67, showing that $gG'g^{-1} = G'$ for any $g \in G$. Exercise 2.36 should help you see why $gG'g^{-1} \subseteq G'$; to show the reverse direction, show why any $g' \in G'$ has the form $g^{-1}[x^g, y^g]g$ for any $g \in G$, so $gG'g^{-1} \supseteq G'$.

Exercise 3.85: Use Lemma 3.29 on page 62.

Hints to Chapter 4

Exercise 4.17(b): Generalize the isomorphism of (a).

Exercise 4.32: Use the Subgroup Theorem along with the properties of a homomorphism.

Exercise 4.24: For a homomorphism function, think about the equation that describes the points on L.

Exercise 4.25: Since it's a corollary to Theorem 4.10, you should use that theorem.

Exercise 4.28: Use induction on the positive powers of g; use a theorem for the nonpositive powers of g.

Exercise 4.29(b): Let $G = \mathbb{Z}_2$ and $H = D_3$; find a homomorphism from G to H.

Exercise 4.30: Recall that

$$f(A) = \{y \in H : f(x) = y \ \exists x \in A\},$$

and use the Subgroup Theorem.

Exercise 4.31(b): See the last part of Exercise 4.29.

Exercise 4.32: Denote $K = \ker f$. Show that $gKg^{-1} = K$ for arbitrary $g \in G$; then Exercise 3.67 applies. Showing that $gKg^{-1} \subseteq K$ is routine. To show that $gKg^{-1} \supseteq K$, let $k \in K$; by closure, $g^{-1}kg = x$ for some $x \in G$. Show that $x \in K$, then rewrite the definition of x to obtain $k \in gKg^{-1}$.

Exercise 4.48(a): Consider $f : \mathbb{R}^2 \to \mathbb{R}$ by $f(a) = b$ where the point $a = (a_1, a_2)$ lies on the line $y = x + b$.

Exercise 4.49(b): You already know the answer from Exercise 3.65 on page 71; find a homomorphism f from Q_8 to that group such that $\ker f = \langle -\mathbf{1} \rangle$.

Exercise 4.61: Use some of the ideas from Example 4.51(c), as well as the Subgroup Theorem.

Exercise 4.63: We can think of D_3 as generated by the elements ρ and φ, and each of these generates a non-trivial cyclic subgroup. Any automorphism α is therefore determined by these generators, so you can find all automorphisms α by finding all possible results for $\alpha(\rho)$ and $\alpha(\varphi)$, then examining that carefully.

Hints to Chapter 5

Exercise 5.27: Life will probably be easier if you convert it to cycle notation first.

Exercise 5.30: List the six elements of S_3 as $\begin{pmatrix} 1 \end{pmatrix}$, α, α^2, β, $\alpha\beta$, $\alpha^2\beta$, using the previous exercises both to justify and to simplify this task.

Exercise 5.34: Try computing $\alpha \circ \beta$ and $\beta \circ \alpha$.

Exercise 5.31: Show that f is an isomorphism either exhaustively (this requires $6 \times 6 = 36$ checks for each possible value of $f\left(\rho^a \varphi^b\right)$), or by a clever argument, perhaps using using the Isomorphism Theorem (since $D_3 / \{\iota\} \cong D_3$).

Exercise 3.108: There are one subgroup of order 1, three subgroups of order 2, one subgroup of order 3, and one subgroup of order 6. From Exercise 5.31 on page 112, you know that $S_3 \cong D_3$, and some subgroups of D_3 appear in Example 3.9 on page 56 and Exercise 3.18 on page 58.

Exercise 5.65: Lemma 5.54 tells us that any permutation can be written as a product of cycles, so it will suffice to show that any cycle can be written as a product of transpositions. For that, take an arbitrary cycle $\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$ and write it as a product of transpositions, as suggested by Example 5.53. Be sure to explain why this product does in fact equal α.

Exercise 5.66: You can do this by showing that any transposition is its own inverse. Take an arbitrary transposition $\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix}$ and show that $\alpha^2 = \iota$.

Exercise 5.67: Let α and β be arbitrary cycles. Consider the four possible cases where α and β are even or odd.

Exercise 5.68: See a previous exercise about subgroups or cosets.

Exercise 5.72: Use the same strategy as that of the proof of Theorem 5.71: find the permutation σ^{-1} that corresponds to the current confiuration, and decide whether $\sigma^{-1} \in A_{16}$. If not, you know the answer is no. If so, you must still check that it can be written as a product of transpositions that satisfy the rules of the puzzle.

Hints to Chapter 6

Exercise 6.21: At least you know that $\gcd(16,33) = 1$, so you can apply the Chinese Remainder Theorem to the first two equations and find a solution in $\mathbb{Z}_{16\cdot 33}$. Now you have to extend your solution so that it also solves the third equation; use your knowledge of cosets to do that.

Exercise 6.25: Since $d \in S$, we can write $d = am + bn$ for some $a, b \in \mathbb{Z}$. Show first that every common divisor of m, n is also a divisor of d. Then show that d is a divisor of m and n. For this last part, use the Division Theorem to divide m by d, and show that if the remainder is not zero, then d is not the smallest element of M.

Exercise 6.43: Use the properties of prime numbers.

Exercise 6.57: Consider Lemma 6.33 on page 144.

Exercise 6.60(c): Using the Extended Euclidean Algorithm might make this go faster. The proof of the RSA algorithm outlines how to use it.

Exercise 6.61:

(b) That largest number should come from encrypting ZZZZ.

(d) Using the Extended Euclidean Algorithm might make this go faster. The proof of the RSA algorithm outlines how to use it.

Exercise 6.62: There are a couple of ways to argue this. The best way for you is to explain why there exist a, b such that $ap + bq = 1$. Next, explain why there exist integers d_1, d_2 such that $m = d_1 a$ and $m = d_2 b$. Observe that $m = m \cdot 1 = m \cdot (ap + bq)$. Put all these facts together to show that $ab \mid m$.

Hints to Chapter 7

Exercise 7.9: The cases where $n = 0$ and $n = 1$ can be disposed of rather quickly; the case where $n \neq 0, 1$ is similar to (a).

Exercise 7.11:

(a) This is short, but not trivial. You need to show that $(-r)s + rs = 0_R$. Try using the distributive property.

(b) You need to show that $-1_R \cdot r + r = 0$. Try using a proof similar to part (a), but work in the additive identity as well.

Exercise 7.12: Proceed by contradiction. Show that if $r \in R$ and $r \neq 0, 1$, then something goes terribly wrong with multiplication in the ring.

Exercise 7.13: Use the result of Exercise 7.12.

Exercise 7.14: You already know that $(B, \oplus)$ is an additive group, so it remains to decide whether $\wedge$ satisfies the requirements of multiplication in a ring.

Exercise 7.24: Use the definition of equality in this set given in Example 7.18. For the first simplification rule, show the equalities separately; that is, show first that $(ac)/(bc) = a/b$; then show that $(ca)/(cb) = a/b$.

Exercise 7.25: For the latter part, try to find fg such that f and g are not even defined, let alone an element of $\mathrm{Frac}(R)$.

Exercise 7.35: Proceed by induction on $\deg f$. We did *not* say that r was unique.

Exercise 7.48: $\mathbb{Z}[x]$ is a subring of what Euclidean domain? But don't be too careless–if you can find the gcd in that Euclidean domain, how can you go from there back to a gcd in $\mathbb{Z}[x]$?

Exercise 7.49: Since it's a field, you should never encounter a remainder, so finding a valuation function should be easy.

Exercise 7.50: There are two parts to this problem. The first is to find a "good" valuation function. The second is to show that you can actually divide elements of the ring. You should be able to do both if you read the proof of Theorem 7.39 carefully.

Exercise 7.51: For correctness, you will want to show something similar to Theorem 6.13 on page 134.

Exercise 7.52(a,iii): A system of equations could help with this latter division.

Hints to Chapter 8

Exercise 8.17: Use the Division Theorem for Integers (Theorem 1.19).

Exercise 8.24: For part (b), consider ideals of $\mathbb{Z}$.

Exercise 8.19: The Extended Euclidean Algorithm (Theorem 6.13 on page 134) would be useful.

Exercise 8.39: Use the Ideal Theorem.

Exercise 8.38: Show that if there exists $f \in \mathbb{F}[x,y]$ such that $x, y \in \langle f \rangle$, then $f = 1$ and $\langle f \rangle = \mathbb{F}[x,y]$. To show that $f = 1$, consider the degrees of x and y necessary to find $p, q \in \mathbb{F}[x,y]$ such that $x = pf$ and $y = qf$.

Exercise 8.47: Follow the argument of Example 8.43.

Exercise 8.61:

(c) Let g have the form $cx + d$ where $c, d \in \mathbb{C}$ are unknown. Try to solve for c, d. You will need to reduce the polynomial fg by an appropriate multiple of $x^2 + 1$ (this preserves the representation $(fg) + I$ but lowers the degree) and solve a system of two linear equations in the two unknowns c, d.

(e) Use the fact that $x^2 + 1$ factors in $\mathbb{C}[x]$ to find a zero divisor in $\mathbb{C}[x]/\langle x^2 + 1 \rangle$.

Exercise 8.62: Try the contrapositive. If $\mathbb{F}[x]/\langle f \rangle$ is not a field, what does Theorem 8.55 tell you? By Theorem 7.50, $\mathbb{F}[x]$ is a Euclidean domain, so you can find a greatest common divisor

of f and a polynomial g that is not in $\langle f \rangle$ (but where is g located?). From this gcd, we obtain a factorization of f.

Or, follow the strategy of Exercise 8.61 (but this will be very, very ugly).

Exercise 8.63:

(a) Look at the previous problem.

(b) Notice that

$$y\left(x^2+y^2-4\right)+I=I$$

and $x\left(xy-1\right)+I=I$. This is related to the idea of the *subtraction polynomials* in later chapters.

Exercise 8.72(d): Proceed by induction on n.

Exercise 8.73: Rewrite an abitrary element of the ring using the multiplicative identity, then apply the commutative property of the ring.

Exercise 8.77: Think of a fraction field over an appropriate ring.

Exercise 8.87: Use strategies similar to those used to prove Theorem 4.10 on page 84.

Exercise 8.89: Follow Example 8.86 on page 211.

Exercise 8.90: Multiply two polynomials of degree at least two, and multiply two matrices of the form given, to see what the polynomial map should be.

Exercise 8.91(d): Think about $i=\sqrt{-1}$.

Exercise 8.92: Showing that φ is multiplicative should be straightforward. To show that φ is additive, use the Binomial Theorem

$$(x+y)^n=\sum_{i=0}^{n}\binom{n}{i}x^n y^{n-i}$$

along with the fact that p is irreducible.

Hints to Chapter 9

Exercise 9.12: You could do this by proving that it is a subring of $\mathbb{C}$. Keep in mind that $\left(\sqrt{-5}\right)\left(\sqrt{-5}\right)=-5$.

Hints to Chapter 10

Exercise 10.61(b): Use part (a).

Exercise 10.62(c): Don't forget to explain why $\langle G\rangle=\left\langle G_{\text{minimal}}\right\rangle$! It is essential that the S-polynomials of these redundant elements top-reduce to zero. Lemma 10.54 is also useful.

Index

0

References

[AF05] Marlow Anderson and Todd Feil. *A First Course in Abstract Algebra*. Chapman and Hall/CRC, second edition, 2005.

[AP] Alberto Arri and John Perry. The F5 Criterion revised. Submitted to the *Journal of Symbolic Computation*, 2009, preprint online at `arxiv.org/abs/1012.3664`.

[Bah08] Tavmjong Bah. *Inkscape: Guide to a Vector Drawing Program*. Prentice-Hall, second edition, 2008. Retrieved from `www.inkscape.org`.

[Bri] Rogério Brito. The `algorithms` bundle. Retrieved 16 October 2008 from `http://www.ctan.org/tex-archive/macros/latex/contrib/algorithms/`. Version 0.1.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalem Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal)*. PhD thesis, Mathematical Insitute, University of Innsbruck, Austria, 1965. English translation published in the Journal of Symbolic Computation (2006) 475–511.

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag New York, Inc., New York, second edition, 1997.

[CLO98] David Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. Springer-Verlag New York, Inc., New York, 1998.

[EP10] Christian Eder and John Perry. F5C: A variant of Faugère's F5 algorithm with reduced Gröbner bases. *Journal of Symbolic Computation*, 45(12):1442–1458, 2010.

[EP11] Christian Eder and John Perry. Signature-based algorithms to compute Gröbner bases. In *Proceedings of the International Symposium on Symbolic and Algebraic Manipulation*, 2011.

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In *International Symposium on Symbolic and Algebraic Computation Symposium - ISSAC 2002, Villeneuve*

d'Ascq, France, pages 75–82, Jul 2002. Revised version downloaded from `http://fgbrs.lip6.fr/jcf/Publications/index.html`.

[GGV10] Shuhong Gao, Yinhua Guan, and Frank Volny. A new incremental algorithm for computing Groebner bases. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*. ACM Press, 2010.

[GPS05] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005. `http://www.singular.uni-kl.de`.

[Grä04] George Grätzer. *Math into LaTeX*. Birkhäuser, Boston, third edition, 2004.

[HA88] Abraham P. Hillman and Gerald L. Alexanderson. *A First Undergraduate Course in Absract Algebra*. Wadsworth Publishing Company, Belmont, California, fourth edition, 1988.

[Knu84] Donald Knuth. *The TeXbook*. Addison-Wesley Professional, spi edition, 1984.

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra*, volume 1. Springer-Verlag, Berlin - Heidelberg - New York, 2000.

[Lam86] Leslie Lamport. *LaTeX: a Document Preparation System*. Addison-Wesley Publishing Company, 1986.

[Lau03] Niels Lauritzen. *Concrete Abstract Algebra: from Numbers to Gröbner Bases*. Cambridge University Press, Cambridge, 2003.

[LP98] Rudolf Lidl and Günter Pilz. *Applied Abstract Algebra*. Springer-Verlag, New York, second edition edition, 1998.

[Lyx] Lyx Team. *Lyx*, 2008–. Retrieved too many times to count from `http://www.lyx.org`.

[Pic06] Paul Pichaureau. *The mathdesign package*, 2006. Retrieved from `http://www.ctan.org/tex-archive/help/Catalogue/entries/mathdesign.h`

[Pip07] Sebastian Pipping. *ccBeamer*, 2007. Retrieved from `http://www.hartwork.org/cgi-bin/download.cgi?file=CCBEAMER`.

[RO08] Sebastian Rahtz and Heiko Oberdiek. *Hypertext marks in LaTeX: a manual for* `hyperref`, 2008. Retrieved 21 April 2009 from `http://www.tug.org/applications/hyperref/manual.html`.

[Rot98] Joseph Rotman. *Galois Theory*. Springer-Verlag, New York, second edition, 1998.

[Rot06] Joseph J. Rotman. *A First Course in Abtract Algebra with Applications*. Pearson Education, Inc., New Jersey, third edition, 2006.

[Soc02] Americal Mathematical Society. *User's Guide for the* `amsmath` *Package*, version 2.0 edition, 2002. Retrieved 21 April 2009 from `http://www.ams.org/tex/amslatex.html`.

[Ste08] William Stein. *Sage: Open Source Mathematical Software (Version 3.1.1)*. The Sage Group, 2008. `http://www.sagemath.org`.

[vzGG99] Joachim von zur Gathen and Jurgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, 1999.