# Notes on Abstract Algebra

John Perry

University of Southern Mississippi
john.perry@usm.edu

Copyright 2009 John Perry
www.math.usm.edu/perry/
Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States
You are free:

- to Share—to copy, distribute and transmit the work
- to Remix—to adapt the work

Under the following conditions:

- Attribution—You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
- Noncommercial—You may not use this work for commercial purposes.
- Share Alike—If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

With the understanding that:

- Waiver—Any of the above conditions can be waived if you get permission from the copyright holder.
- Other Rights—In no way are any of the following rights affected by the license:
  - Your fair dealing or fair use rights;
  - Apart from the remix rights granted under this license, the author's moral rights;
  - Rights other persons may have either in the work itself or in how the work is used, such as publicity or privacy rights.
- Notice—For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page:

  http://creativecommons.org/licenses/by-nc-sa/3.0/us/legalcode

# Contents

## Reference sheet for notation

| | |
|---|---|
| $[r]$ | the element $r+n\mathbb{Z}$ of $\mathbb{Z}_n$, page 57 |
| $\langle g\rangle$ | the group (or ideal) generated by $g$, page 31 |
| $]$ | $[G,G]$, page 55 |
| $]$ | $[x,y]$, page 31 |
| $A_3$ | the alternating group on three elements, page 53 |
| $A:=B$ | $A$ is defined to be $B$, page 22 |
| $A\triangleleft G$ | for $G$ a group, $A$ is a normal subgroup of $G$, page 53 |
| $A\triangleleft I$ | for $I$ a ring, $A$ is an ideal of $I$., page 147 |
| $\mathbb{C}$ | the complex numbers $\{a+bi:\ a,b\in\mathbb{C}$ and $i=\sqrt{-1}\}$, page 9 |
| $\mathrm{Conj}_a(G)$ | the group of conjugations of $G$ by $a$, page 74 |
| $\mathrm{conj}_g(x)$ | the automorphism of conjugation by $g$, page 74 |
| $D_3$ | the symmetries of a triangle, page 34 |
| $d\mid n$ | $d$ divides $n$, page 16 |
| $\deg f$ | the degree of the polynomial $f$, page 135 |
| $D_n$ | the dihedral group of symmetries of a regular polygon with $n$ sides, page 87 |
| $D_n(\mathbb{R})$ | the set of all diagonal matrices whose values along the diagonal is constant, page 44 |
| $d\mathbb{Z}$ | the set of integer multiples of $d$, page 41 |
| $f(G)$ | for $f$ a homomorphism and $G$ a group (or ring), the image of $G$, page 62 |
| $\mathbb{F}$ | an arbitrary field, page 133 |
| $\mathrm{Frac}(R)$ | the set of fractions of a commutative ring $R$, page 131 |
| $G/A$ | the set of left cosets of $A$, page 50 |
| $G\backslash A$ | the set of right cosets of $A$, page 50 |
| $gA$ | the left coset of $A$ with $g$, page 47 |
| $G\cong H$ | $G$ is isomorphic to $H$, page 62 |
| $\mathrm{GL}_m(\mathbb{R})$ | the general linear group of invertible matrices, page 26 |
| $\prod_{i=1}^n G_i$ | the ordered $n$-tuples of $G_1$, $G_2$, …, $G_n$, page 22 |
| $G\times H$ | the ordered pairs of elements of $G$ and $H$, page 22 |
| $g^z$ | for $G$ a group and $g,z\in G$, the conjugation of $g$ by $z$, or $zgz^{-1}$, page 31 |
| $H<G$ | for $G$ a group, $H$ is a subgroup of $G$, page 41 |
| $I_n$ | the identity matrix of dimension $n\times n$, page 11 |
| $\ker f$ | the kernel of the homomorphism $f$, page 71 |
| $\mathrm{lm}(p)$ | the leading monomial of the polynomial $p$, page 176 |
| $\mathrm{lv}(p)$ | the leading variable of a linear polynomial $p$, page 170 |
| $\mathbb{M}$ | the set of all monomials over $\mathbf{x}=(x_1,x_2,\ldots,x_n)$, page 177 |
| $\mathbb{N}^+$ | the positive integers, page 9 |
| $N_G(H)$ | the normalizer of a subgroup $H$ of $G$, page 55 |
| $\mathbb{N}$ | the natural or counting numbers $\{0,1,2,3\ldots\}$, page 9 |

| | |
|---|---|
| $\operatorname{ord}(x)$ | the order of $x$, page 32 |
| $P_\infty$ | the point at infinity on an elliptic curve, page 23 |
| $Q_8$ | the group of quaternions, page 31 |
| $\mathbb{Q}$ | the rational numbers $\{\frac{a}{b} : a, b \in \mathbb{Z}$ and $b \neq 0\}$, page 9 |
| $R/A$ | for $R$ a ring and $A$ an ideal subring of $R$, $R/A$ is the quotient ring of $R$ with respect to $A$, page 153 |
| $\langle r_1, r_2, \ldots, r_m \rangle$ | the ideal generated by $r_1, r_2, \ldots, r_m$, page 149 |
| $\mathbb{R}$ | the real numbers, those that measure any length along a line, page 9 |
| $\mathbb{R}^{m\times m}$ | $m \times m$ matrices with real coefficients, page 10 |
| $\mathbb{R}[x]$ | polynomials in one variable with real coefficients, page 10 |
| $\mathbb{R}[x_1, x_2, \ldots, x_n]$ | polynomials in $n$ variables with real coefficients, page 10 |
| $R[x_1, x_2, \ldots, x_n]$ | the ring of polynomials whose coefficients are in the ground ring $R$, page 135 |
| $\operatorname{swp} \alpha$ | the sign function of a cycle or permutation, page 96 |
| $S_n$ | the group of all permutations of a list of $n$ elements, page 85 |
| $S \times T$ | the Cartesian product of the sets $S$ and $T$, page 12 |
| $\operatorname{tts}(p)$ | the trailing terms of $p$, page 201 |
| $Z(G)$ | centralizer of a group $G$, page 55 |
| $\mathbb{Z}_n^*$ | the set of elements of $\mathbb{Z}_n$ that are *not* zero divisors, page 114 |
| $\mathbb{Z}/n\mathbb{Z}$ | quotient group (resp. ring) of $\mathbb{Z}$ modulo the subgroup (resp. ideal) $n\mathbb{Z}$, page 56 |
| $\mathbb{Z}$ | the integers $\{\ldots, -1, 0, 1, 2, \ldots\}$, page 9 |
| $\mathbb{Z}_n$ | the quotient group $\mathbb{Z}/n\mathbb{Z}$, page 56 |

## A few acknowledgements

These notes are inspired from some of my favorite algebra texts: [**AF05**, **CLO97**, **HA88**, **Lau03**, **LP98**, **Rot06**]. However, the connection may not be obvious.

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 and 9.

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 good algebra professors; in chronological order, they were:

- 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 turn out bad in practice should not be blamed on any of the individuals or sources named above. The errors are mine and mine alone. *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 [**Lyx09**] (and therefore LaTeX [**Lam86**, **Grä04**]), along with the packages
    - `cc-beamer` [**Pip07**],
    - `hyperref` [**RO08**],
    - AMS-LaTeX[**Soc02**],
    - `mathdesign` [**Pic06**], and
    - `algorithms` (modified slightly from version 2006/06/02) [**Bri**].
- Inkscape [**Bah08**].

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

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

CHAPTER 1

# Patterns and anti-patterns

## 1.1. THREE INTERESTING PROBLEMS

We'd like to motivate this study of algebra with three problems that we hope you will find interesting. We also provide "general" solutions. What might surprise you is that in this class, what interests us are not the solutions, but *why the solutions to these problems work*. You don't yet know enough to explain this. One can compare the situation to walking through a museum with a tour guide. The guide 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 its original owner.

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 $\alpha$.

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 same card you place on the table in rows of four; likewise the last card must remain last. Ask your friend again what column the card is in; call that number $\beta$.

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 $x$th card. This will be the card your friend chose.

Mastering this trick isn't hard, and takes only a little practice. To understand *why* it works requires a marvelous result called the *Chinese Remainder Theorem*, so named because many centuries ago the Chinese military used this technique to count the number of casualties of a battle.[1] We cover the Chinese Remainder Theorem later in this course.

INTERNET COMMERCE. You go online to check your bank account. Before you can gain access to your account, your computer must send your login name and password to the bank. Likewise, your bank sends a lot of information from its computers to yours, things like your account number and balance. You'd rather keep such sensitive information secret from all the other computers through which the information passes on the internet, but how?

The solution is called *public-key cryptography*. Your computer tells the bank's computer how to send it a message, and the bank's computer tells your computer how to send it a message. One key—a special number used to encrypt the message—is therefore public. Anyone in the world can see it. What's more, anyone in the world can look up the method used to decrypt the message.

[1] I asked Dr. Ding what the Chinese call this theorem. He showed me one of his books; I couldn't read it, but he says they call it Sun Tzu's Theorem. At first I thought that he meant the author of the *Art of War*. Later I learned that this mathematical Sun Tzu was a different person.

How on earth is this safe? To use the decryption method, snoopers also need a *hidden key,* a special number related to the public key. Hidden? 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. ***What?!?*** you exclaim. Yes: a snooper can determine your hidden key and decrypt the messages *using procedures that would factor* $21 = 3 \cdot 7$.

*How on earth is this safe?!?* Although the problem to solve is "simple", the size of the integers in use now is about 40 digits. Believe it or not, even a 40 digit integer takes far too long to factor! The world's fastest computers won't be fast enough to do this for many years, if not decades. So your internet commerce is completely safe.

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 25. As with the twelve-hour clock, when we hit the integer 26, we reset to 1; when we hit the integer 27, we reset to 2; and in general for any number that does not lie between 1 and 25, we divide by 25 and take the remainder. For example,

$$20 \cdot 3 + 8 = 68 \rightsquigarrow 18.$$

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 $\{1, 2, \ldots, 25\}$ 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?*

As the problems show, abstract 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.

## 1.2. COMMON PATTERNS

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

- numbers, of which you have seen
  - the **natural numbers** $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, also written $\mathbb{Z}_{\geq 0}$; with which we can easily associate
    - ⋆ the **positive integers** $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$;
    - ⋆ the **integers** $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$;[2] and
    - ⋆ the **rational numbers** $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\right\}$, which the Pythagoreans believed to be the only possible numbers;
  - 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

[2] The integers are denoted by $\mathbb{Z}$ from the German word *Zählen*.

   - 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 especially useful for representing certain kinds of objects. Natural numbers can represent objects that we count: two apples, or twenty planks of flooring. Real numbers can represent objects that we measure, such as the length of the hypotenuse of a right triangle.

In each set described above, you can perform arithmetic: add, subtract, multiply, and (in most cases) divide. Have you ever noticed that you perform these operations differently in each set?

EXAMPLE 1.1. The natural number 2 can represent a basket of 2 tomatoes; the natural number 10 can represent a basket of ten tomatoes. Adding the two numbers represents counting how many tomatoes are in both baskets: 10+2=12.

Adding two polynomials is somewhat similar, but requires a different method for simplification. The polynomial $f = 2x+3y$ can represent the amount of money earned when tomatoes ($x$) and cucumbers ($y$) are sold on a day where their respective prices are \$2 and \$3 apiece. On another day, the prices may change to \$1 and \$2.50, respectively, so the polynomial $g = x+2.5y$ represents the amount of money earned on that day. Adding the two polynomials gives $f+g$, which represents the amount of money earned if we sell the same number of tomatoes and cucumbers on both days. To determine a simplified representation of $f+g$, apply the distributive property:

$$f+g = (2x+3y)+(x+2.5y) = (2+1)x+(3+2.5)y = 3x+5.5y.$$

Adding two rational numbers is quite involved. Let $x,y\in\mathbb{Q}$. Then $x=a/b$ and $y=c/d$ for certain integers $a,b,c,d$ where $b,d\neq 0$. We have

$$x+y=\frac{a}{b}+\frac{c}{d}=\frac{ad}{bd}+\frac{bc}{bd}=\frac{ad+bc}{bd}.$$

Here we had to compute a common denominator in order to add the two rational numbers. This is conceptually different from adding integers or adding polynomials. Students often dislike fractions and want instead to add

$$\frac{a}{b}+\frac{c}{d}=\frac{a+c}{b+d}.$$

You might be tempted to say, "That's wrong!" and in general you're right, because the real-world objects that fractions model don't behave this way.

However, if someone wanted to model a different real-world phenomenon using the notation of fractions, he might find that adding fractions the "wrong" way is actually *right*. Mathematicians do consider this second version of addition wrong, but *only because it does not correspond to the real-world phenomena that fractions usually represent.* Make sure you understand this point: adding fractions in the second way described above is wrong because of what fractions represent. ◇

EXAMPLE 1.2. How do you divide $x^5-3x^3+1$ by $x-2$? In high school, you should have learned two ways: long polynomial division, and synthetic division. Both of them tell you the same answer, but in a different way. Synthetic division is faster, but it only applies to linear divisors like $x-2$, and not to higher degrees. Long polynomial division works like long integer division, but differences exist. ◇

Despite the fact that we perform the operations differently in each set, they still preserve some common properties. These properties have nothing to do with the choice of *how to simplify a given operation*. They are intrinsic to the operation itself, or to the structure of the objects of the set.

For example:

(1) Addition is always **commutative**. That is, $x+y=y+x$ for any $x,y$ in any set.
(2) Multiplication is *not* always commutative. For example,
$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}=\begin{pmatrix} 2 & 3 \\ 2 & 0 \end{pmatrix}\neq\begin{pmatrix} 2 & 2 \\ 3 & 0 \end{pmatrix}=\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$
(3) Both operations are always **associative**. That is, $x+(y+z)=(x+y)+z$ and $x(yz)=(xy)z$ for any $x,y,z$ in any set.
(4) Multiplication is **distributive** over addition. That is, $x(y+z)=xy+xz$ no matter which set contains $x,y,z$.
(5) Each set has additive and multiplicative **identities**. That is, each set has two special elements, written $0$ and $1$, such that $0+x=x$ and $1\cdot x=x\cdot 1=x$, for every value of $x$.[3]
(6) Each set has **additive inverses**. That is, for any set and for any $x$ in that set, we can identify an element $y$ such that $x+y=0$. Usually we write $-x$ for this element.
(7) Not every set contains **multiplicative inverses** for its non-zero elements. For polynomials, only non-zero constant polynomials like 4 or -8 have multiplicative inverses. Polynomials such as $x^2$ do not have inverses *that are also polynomial;* although $1/x^2$ is a multiplicative inverse, it is not a polynomial. With matrices the situation is even worse; many matrices have no inverse in *any* set.
(8) In every set specified, $-1\times x=-x$ and $0\times x=0$. But not every set obeys the **zero product property**,
$$\text{if } xy=0 \text{ then } x=0 \text{ or } y=0.$$
Here again it is the matrices that misbehave:
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\mathbf{0}.$$
(9) In some sets you have learned how to **divide** with remainder. Even though non-constant polynomials don't have multiplicative inverses, you can still divide them. But you don't generally divide matrices.

Not very long ago, mathematicians set about asking themselves how they could organize the common principles of these sets and operations as abstractly, simply, and generically as possible. This abstraction turned out to be very, *very* useful. If I prove some property about the integers, then I only have a result about integers. If someone comes and asks whether that property is also true about matrices, the only answer I have without further effort is, "I don't know." It might be easy to show that the property is true, but it might be hard.

If, on the other hand, I prove something about any set that shares certain properties with the integers, and if the set of matrices shares those properties, then I can answer without any further effort, "Yes!"

This is the beauty of abstract algebra.

---

[3] For square matrices we actually write $I_n$, where $n$ is the dimension of the matrix.

EXERCISES.

EXERCISE 1.3. For each set $S$ listed below, find a real-world phenomenon that the elements of $S$ represent.

(a) $\mathbb{Z}$
(b) $\mathbb{Q}$
(c) $\mathbb{R}[x,y]$

EXERCISE 1.4. Give a detailed example of a real-world phenomenon where

$$\frac{a}{b}+\frac{c}{d}\neq\frac{a+c}{b+d}.$$

By "real-world phenomenon", I mean that you should not merely add two fractions in the ordinary manner, but describe the problem using objects that you use every day (or at least once a month).

EXERCISE 1.5. Let $a,b,c,d\in\mathbb{N}^+$ and assume that $\frac{a}{b}<\frac{c}{d}$. Prove that

- $\frac{a}{b}<\frac{a+c}{b+d}<\frac{c}{d}$;
- $\frac{a}{b}<\frac{a}{b}+\frac{c}{d}$; and
- $\frac{c}{d}<\frac{a}{b}+\frac{c}{d}$.

As you see, $\frac{a+c}{b+d}\neq\frac{a}{b}+\frac{c}{d}$ in general. Verify this assertion by choosing different values for $a,b,c,d$. *Hint:* You can try a proof by contradiction.

## 1.3. SOME FACTS ABOUT THE INTEGERS

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.[4]

We review some basic facts. Some you may have seen in high-school algebra; others you won't. Some that you did see you probably didn't see with the emphasis that we want in this course: *why* something is true.

DEFINITION 1.6 (Cartesian product, relation). Let $S$ and $T$ be two sets. The **Cartesian product of $S$ and $T$** is the set

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

A **relation on the sets $S$ and $T$** is any subset of $S\times T$. ◇

EXAMPLE 1.7. 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

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

is a relation on $S$ and $T$. ◇

[4]Named after the mathematician and philosopher René Descartes, who inaugurated modern philosophy and claimed to have spent a moment wondering even whether he existed. He concluded instead, *Cogito, ergo sum*: I am thinking about something, so I must exist. It's usually translated more snappily as: I think, therefore I am.

One of the most fundamental relations occurs with the set of sets.[5]

DEFINITION 1.8. 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 $A \subsetneq B$.[6] ◇

NOTATION. Notice what the notation means: both $\mathbb{N} \subseteq \mathbb{Z}$ and $\mathbb{N} \subsetneq \mathbb{Z}$ are true.

It is possible to construct $\mathbb{Z}$ using a minimal number of assumptions, but that is beyond the scope of this course.[7] 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 1.9. 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* $>$.

The relations $\leq$ and $\subseteq$ have something in common: just as both $\mathbb{N} \subseteq \mathbb{Z}$ and $\mathbb{N} \subsetneq \mathbb{Z}$ are true, both $3 \leq 5$ and $3 < 5$ are true. However, there is one important difference between the two relations. Given two distinct integers (like 3 and 5) you have always been able to order them. You *cannot* always order any two distinct sets. 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? If so, such a property would merit with a name.

DEFINITION 1.10 (linear ordering). Let $S$ be any set. A **linear ordering** on $S$ is a relation $\sim$ where for any $a, b \in S$ exactly one of the following holds:

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

So $\subseteq$ is *not* a linear ordering, since

$$\{a, b\} \nsubseteq \{c, d\},\ \{a, b\} \neq \{c, d\},\ \text{and}\ \{c, d\} \nsubseteq \{a, b\}.$$

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

THEOREM 1.11. *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 you know from before. Try to identify where these assumptions 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 (for now, 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.

---

[5] Talking about the "set of sets" leads to a paradox, usually resolved by introducing the concept of *classes*. We ignore that here, since the intuitive notion suffices.

[6] 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.

[7] 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.

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 $\mathbb{Z}$.[8]

- 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 $\mathbb{N}$.[9] 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. We can also extend them to $\mathbb{C}$ and $\mathbb{R}^{m \times m}$, but I haven't seen it in pracitce, and we don't need that anyway.

That said, this relation behaves differently in $\mathbb{N}$ than it does in $\mathbb{Z}$.

DEFINITION 1.12 (well-ordering property). Let $S$ be a set and $\prec$ a linear ordering on $S$. We say that $\prec$ is a **well-ordering** if

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

EXAMPLE 1.13. 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 $a$. Observe that

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

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

*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.*[10] It is an assumption about the natural numbers. This is why we state it as a principle (or axiom, if you prefer).

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

[8]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.

[9]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.

[10]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.

THEOREM 1.14 (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 1.15 (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: $d > 0$, and $d < 0$. First we consider $d > 0$. 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 1.22 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 $d > 0$, so $0 \leq r - d < r$. Rewrite property (D1) 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 $r - d \in S$. Since $0 \leq r - d$, we know that $r - d \in \mathbb{N}$ also, 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 $0 \leq r' \leq r < d$. Then $r' = n - q'd \in S$. Since $r$ is the smallest element of $S$, $r' = r$. Rewriting this as $n - q'd = n - qd$ and applying the properties of arithmetic yields $q = q'$.

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

DEFINITION 1.16 (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 write $d \nmid n$. ◈

EXERCISES.

EXERCISE 1.17. Show that we can order any subset of $\mathbb{Z}$ linearly. *Hint:* 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 1.11.

EXERCISE 1.18. Identify the quotient and remainder when dividing:

(a) 10 by $-5$;
(b) $-5$ by 10;
(c) $-10$ by $-5$.

EXERCISE 1.19. Let $a, b \in \mathbb{Z}$, and assume that both $a \leq b$ and $b \leq a$ . Prove that $a = b$. *Hint:* Try to show that $a - b = 0$.

EXERCISE 1.20. Let $a, b \in \mathbb{N}$ and assume that $a < b$. Let $d = b - a$. Show that $d < b$. *Hint:* Use the definition.

EXERCISE 1.21. Let $S \subset \mathbb{N}$. We know from the well-ordering property that $S$ has a smallest element. Prove that this smallest element is unique. *Hint:* 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 1.22. Let $n, d \in \mathbb{Z}$, where $d > 0$. Define $M = \{n - qd : q \in \mathbb{Z}\}$. Prove that $M \cap \mathbb{N} \neq \emptyset$. *Hint:* (a) If $n > 0$ then you can pretty easily identify a $q$ that finds an element of the intersection $M \cap \mathbb{N}$. (It helps that $d > 0$ also.) (b) Otherwise $n \leq 0$; use (a) with the set $M' = \{|n| - qd : q \in \mathbb{Z}\}$ to find $q$ such that $|n| - qd \in \mathbb{N}$. Use this to find $q' \in \mathbb{Z}$ such that $n - q'd \in \mathbb{N}$.

EXERCISE 1.23. Show that $>$ is not a well-ordering of $\mathbb{N}$. *Hint:* 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 1.24. Show that the ordering $<$ of $\mathbb{Z}$ can be generalized "naturally" to an ordering $<$ of $\mathbb{Q}$ that is also a linear ordering. *Hint:* 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 1.25. Define an ordering $\prec$ on the set of monomials $\{x^a : a \in \mathbb{N}\}$ such that $\prec$ is both a linear ordering and a total ordering.

# Part 1

# An introduction to group theory

CHAPTER 2

# Groups

There are many structures in algebra, and some disagreement about where to start.

- Some authors prefer rings, arguing that the structure of a ring is most familiar to students, as are the classical examples. However, the structure of rings is more complicated than the structure of a group, and the classical examples of rings are also additive groups.
- Other authors prefer monoids and semigroups for their logical simplicity. In this case, the structure seems to be too specialized, and the examples chosen are often not as familiar to the students as the usual ones.

So we will start with a simple structure, but not in its full generality.

A *group* is a simple algebraic structure that applies to a large number of useful phenomena. We characterize a group by three things: a set of objects, an operation on the elements of that set, and certain properties that operation satisfies.

From a pedagogical point of view, the simplest kind of groups are probably the additive groups, so we start by describing those (Section 2.1). To illustrate the power of this structure, we then describe an additive group that you have never met before, but has received a great deal of attention in recent decades, the *elliptic cuves* (Section 2.2). We then look at a kind of group that is structurally simpler than additive groups, multiplicative groups (Section 2.3).[1] From there we generalize to generic groups (Section 2.4), where the operation can be very different from addition and subtraction. This allows us to describe two special kinds of groups, the cyclic groups (Section 2.5) and an important group called $D_3$ (Section 2.6).

## 2.1. COMMON STRUCTURES FOR ADDITION

Many sets in mathematics, such as those listed in Chapter 1.2, allow addition of their elements; others allow multiplication. Some allow both. We saw that while addition was commutative for all the examples listed, multiplication was not. Both are examples of a common relation called an operation.

DEFINITION 2.1. Let $S$ and $T$ be sets. An **binary operation from $S$ to $T$** is a map $f : S \times S \to T$. If $S = T$, we say that $f$ is a binary operation **on** $S$. In addition, we say that $f$ is **closed** if $T = S$ and $f(a, b)$ is defined for all $a, b \in S$. $\diamondsuit$

EXAMPLE 2.2. Addition of the natural numbers is a map $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Hence addition is a binary operation on $\mathbb{N}$. Since addition is defined for all natural numbers, 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 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.

[1] Although multiplicative groups are structurally simpler than additive groups, you are not as used to working with the more interesting examples of multiplicative groups. This is the reason that we start with additive groups.

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

We now use some of the properties we associate with addition to define a common structure for addition.

DEFINITION 2.3. Let $G$ be a set, and $+$ a binary operation on $G$. The pair $(G,+)$ is an **additive group**, and $+$ is an **addition**, if $(G,+)$ satisfies the following properties.

(AG1) Addition is closed.
(AG2) Addition is associative; that is, $x+(y+z)=(x+y)+z$ for all $x,y,z \in G$.
(AG3) There exists an element $z \in G$ such that $x+z=x$ for all $x \in G$. We call $z$ the **zero element** or the **additive identity**, and generally write $0$ to represent it.
(AG4) For every $x \in G$ there exists an element $y \in G$ such that $x+y=0$. Normally we write $-x$ for this element and call it the **additive inverse**.
(AG5) Addition is commutative; that is, $x+y=y+x$ for all $x,y \in G$. ◊

NOTATION. It is tiresome to write $x+(-y)$ all the time, so we write $x-y$ instead.

We may also refer to an additive group as a **group under addition**. The operation is usually understood from context, so we usually write $G$ rather than $(G,+)$. We will sometimes write $(G,+)$ when we want to emphasize the operation, especially if the operation does not fit the normal intuition of addition (see Exercises 2.13 and 2.14 below) and when we discuss groups under multiplication later.

EXAMPLE 2.4. Certainly $\mathbb{Z}$ is an additive group. Why?

(AG1) Adding two integers gives another integer.
(AG2) Addition of integers is associative.
(AG3) The additive identity is the number $0$.
(AG4) Every integer has an additive inverse.
(AG5) Addition of integers is commutative. ◊

The same holds true for many of the sets we identified in Chapter 1.2, using the ordinary definition of addition in that set. However, $\mathbb{N}$ is not an additive group. Why not? Although $\mathbb{N}$ is closed, and addition of natural numbers is associative and commutative, no positive natural number has an additive inverse in $\mathbb{N}$.

The definition of additive groups allows us to investigate "generic" additive groups, and to formulate conclusions based on these arbitrary groups. 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".) We won't replicate their achievement in this course, but we do want to to take a few steps in this area. First we need a definition.

DEFINITION 2.5. Let $S$ be any set. If there is a finite number of elements in $S$, then $|S|$ denotes that number, and we 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, without stating a precise number.

For any additive group $(G,+)$ the **order of** $G$ is the size of $G$. A group has finite order if $|G|<\infty$ and infinite order if $|G|=\infty$. ◊

We can now completely classify all finite groups of order two. We will do this by building the addition table for a "generic" group of order two. As a consequence, we show that no matter how you define the set and its addition, every group of order 2 behaves exactly the same way: there is only one structure possible for its addition table.

EXAMPLE 2.6. Every additive group of order two has the same addition table. To see this, let $G$ be an arbitrary additive group of order two. By property (AG3), it has to have a zero element, so $G = \{0, a\}$ where $0$ represents that zero element.

We did *not* say that $0$ represents the *only* zero element. For all we know, $a$ might also be a zero element. The group could have two zero elements! In fact, this is not the case; a group can have only one zero element. Why?

Suppose, by way of contradiction, that $a$ is also a zero element. Since $0$ is a zero element, property (AG3) tells us that $a + 0 = a$. Since $a$ is a zero element, $0 + a = 0$. The commutative property (AG5) tells us that $a + 0 = 0 + a$, and by substitution we have $0 = a$. Thus $G = \{0\}$, but this contradicts the definition of $G$ as a group of order two! So $a$ cannot be a zero element.

Now we build the addition table. We *have* to assign $a + a = 0$. *Why?*

- To satisfy (AG3), we must have $0 + 0 = 0$, $0 + a = a$, and $a + 0 = a$.
- To satisfy (AG4), $a$ must have an additive inverse. The inverse isn't $0$, so it must be $a$ itself! That is, $-a = a$. (Read that as, "the additive inverse of $a$ is $a$.") So $a + (-a) = a + a = 0$.

This leads to the following table.

| $+$ | $0$ | $a$ |
|---|---|---|
| $0$ | $0$ | $a$ |
| $a$ | $a$ | $0$ |

The only assumption we made about $G$ is that it was a group of order two. That means that we have completely determined the addition table of all groups of order two! ◇

Example 2.6 includes a proof of an important fact that we should highlight:

PROPOSITION 2.7. *Every additive group $G$ contains a unique zero element.*

We will prove this lemma differently from the example. "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 for the Division Theorem (Theorem 1.15 on page 15).

PROOF. Let $G$ be an additive group. By property (AG3), $G$ must contain at least one zero element. If $|G| = 1$, then $G = \{0\}$, and we are done. Otherwise, let $z \in G$ and assume $z$ satisfies (AG3); that is, $g + z = g$ for all $g \in G$.

By (AG3), $0 + z = 0$ and $z + 0 = z$. By (AG5), $0 + z = z + 0$, and substitution implies that $0 = z$. Hence the zero element of $G$ is unique. Since $G$ was arbitrary, *every* additive group has a unique zero element. □

The following fact looks obvious—but remember, we're talking about elements of *any* additive group, not only the numbers you have always used.

PROPOSITION 2.8. *Let $G$ be an additive group and $x \in G$. Then $-(-x) = x$.*

Proposition 2.8 is saying that the additive inverse of the additive inverse of $x$ is $x$ itself; that is, if $y$ is the additive inverse of $x$, then $x$ is the additive inverse of $y$.

PROOF. You prove it! See Exercise 2.10. □

In Example 2.6, the structure of a group compels certain assignments for addition. Similarly, we can infer an important conclusion for additive groups of finite order.

THEOREM 2.9. *Let $G$ be an additive group of finite order, and let $a, b \in G$. Then $a$ appears exactly once in any row or column of the addition table that is headed by $b$.*

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 addition table headed by $b$ any time there exists $c \in G$ such that $b + c = a$. Let $c, d \in G$ such that $b + c = a$ and $b + d = a$. (We have *not* assumed that $c \neq d$.) Since $a = a$, substitution implies that $b + c = b + d$. Properties (AG1), (AG4), and (AG3) give us

$$-b + (b + d) = (-b + b) + d = 0 + d = d.$$

Along with substitution, they also give us

$$-b + (b + d) = -b + (b + c) = (-b + b) + c = 0 + c = c.$$

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 addition 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 $n - 1$ additions are defined, which contradicts either the assumption that addition is an operation (that $b + x$ is defined for all $x \in G$) or closure (that $b + x \in G$ for all $x \in G$). Hence $a$ must appear at least once. $\square$

EXERCISES.

EXERCISE 2.10. Explain why $-(-x) = x$. *Hint:* Remember that $-$ means the additive inverse. So, you have to show that the additive inverse of $-x$ is $x$.

EXERCISE 2.11. Let $G$ be an additive group, and $x, y, z \in G$. Show that if $x + z = y + z$, then $x = y$. *Hint:* Use substitution.

EXERCISE 2.12. Show in detail that $\mathbb{R}^{2\times 2}$ is an additive group. *Hint:* 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 2.13. 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 $(B, \vee)$ an additive group? If so, explain how it justifies each property. Identify the zero element, and for each non-zero element identify its additive inverse. If it is not, explain why not.

EXERCISE 2.14. Consider the set $B$ from Exercise 2.13 with the operation $\oplus$ where

$$F \oplus F = F$$
$$F \oplus T = T$$
$$T \oplus F = T$$
$$T \oplus T = F.$$

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

Is $(B, \oplus)$ an additive group? If so, explain how it justifies each property. Identify the zero element, and for each non-zero element identify its additive inverse. If it is not, explain why not.

EXERCISE 2.15. Define $\mathbb{Z} \times \mathbb{Z}$ to be the set of all ordered pairs whose elements are integers; that is,

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

Addition in $\mathbb{Z} \times \mathbb{Z}$ works in the following way. For any $x, y \in \mathbb{Z} \times \mathbb{Z}$, write $x = (a,b)$ and $y = (c,d)$; then

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

Show that $\mathbb{Z} \times \mathbb{Z}$ is an additive group.

EXERCISE 2.16. Let $G$ and $H$ be additive groups, and define

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

Addition in $G \times H$ works in the following way. For any $x, y \in G \times H$, write $x = (a,b)$ and $y = (c,d)$ and then

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

Show that $G \times H$ is an additive group.

*Note:* The symbol $+$ may have different meanings for $G$ and $H$. For example, the first group might be $\mathbb{Z}$ while the second group might be $\mathbb{R}^{m \times m}$.

EXERCISE 2.17. Let $n \in \mathbb{N}^+$. Let $G_1, G_2, \ldots, G_n$ be additive groups, and define

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

Addition in this set works as follows. For any $x, y \in \prod_{i=1}^{n} G_i$, write $x = (a_1, a_2, \ldots, a_n)$ and $y = (b_1, b_2, \ldots, b_n)$ and then

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

Show that $\prod_{i=1}^{n} G_i$ is an additive group.

EXERCISE 2.18. Let $m \in \mathbb{N}^+$. Show in detail that $\mathbb{R}^{m \times m}$ is a group under addition. *Hint:* 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 2.19. Show that every additive group of order 3 has the same structure.

EXERCISE 2.20. *Not* every additive group of order 4 has the same structure, because there are two addition 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.

## 2.2. ELLIPTIC CURVES

An excellent example of how additive 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 2.21. Let $a, b \in \mathbb{R}$ such that $16a^3 \neq 27b^2$. We say that $E \subset \mathbb{R}^2$ is an **elliptic curve** if

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

where $P_\infty$ 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 2.22. 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 2.1 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 $\ell$ at $P$. It turns out that $\ell$ 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 $\ell$ determined by $P$ and $Q$. It turns out that $\ell$ 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 2.2 shows the addition of $P = \left(2, -\sqrt{6}\right)$ and $Q = (0,0)$; the line intersects $E$ at $S = \left(-1/2, \sqrt{6}/4\right)$, so $P + Q = \left(-1/2, -\sqrt{6}/4\right)$. $\diamondsuit$

FIGURE 2.1. A plot of the elliptic curve $y^2 = x^3 - x$.

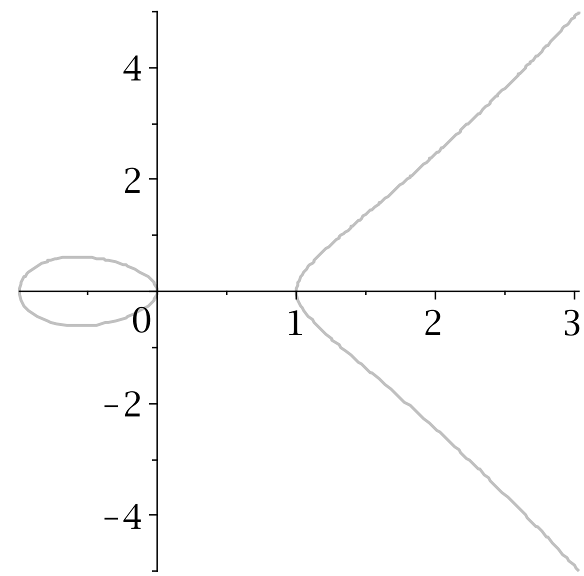
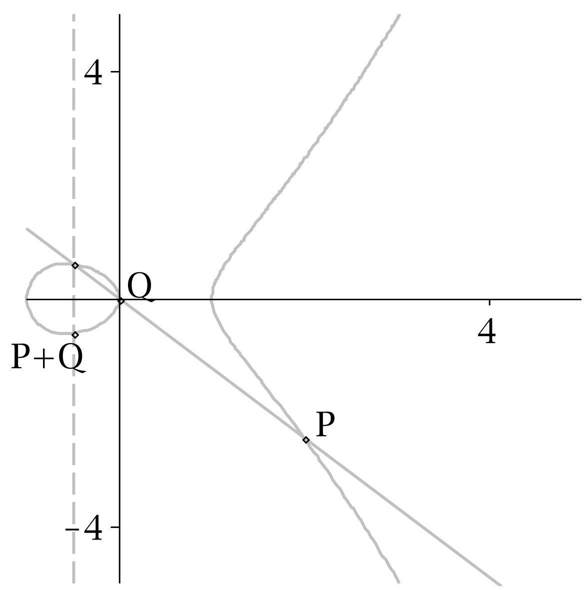



FIGURE 2.2. Addition on an elliptic curve




EXERCISES.

EXERCISE 2.23. Let $E$ be an arbitrary elliptic curve. Show that $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) \neq (0,0)$ for any point on $E$. *Hint:* You will need the condition that $16a^3 = 27c^2$.

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 2.24. Show that $E$ is an additive group under the addition defined above, with

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

*Hint:* 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 $P_\infty$.

EXERCISE 2.25. Choose different values for $a$ and $b$ to generate another elliptic curve. Graph it, and illustrate each kind of addition.

*Hint:* 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.

APPENDIX: BASIC ELLIPTIC CURVES WITH SAGE. Sage computes elliptic curves of the form

$$y^2 + a_{1,1}xy + a_{0,1}y = x^3 + a_{2,0}x^2 + a_{1,0}x + a_{0,0} \tag{2.2.1}$$

using the command

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

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 $P_\infty$; but
- if $c = 1$, then substituting $x = a$ and $y = b$ *must* satisfy equation 2.2.1.

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 2.2 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)
```

This point corresponds to $P + Q$ as shown in Figure 2.2. To see this visually, create the plot using the following sequence of commands.

[2]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.

```
# 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
```

## 2.3. Common structures for multiplication

We saw in Section 1.2 that multiplication, unlike addition, is not always commutative. So *multiplicative groups* will have a structure similar to additive groups, but lack the commutative property.

Definition 2.26. Let $G$ be a set, and $\times$ a binary operation on $G$ to itself. The pair $(G,\times)$ is a **multiplicative group**, and $\times$ is a **multiplication**, if $(G,\times)$ satisfies the following properties.

(MG1) Multiplication is closed; that is, $x \times y \in G$ for all $x, y \in G$.

(MG2) Multiplication is associative; that is, $x \times (y \times z) = (x \times y) \times z$ for all $x, y, z \in G$.

(MG3) There exists an element $1 \in G$ such that $x \times 1 = x = 1 \times x$ for all $x \in G$. We call this element the **identity**.

(MG4) For every $x \in G$ there exists an element $y \in G$ such that $x \times y = e = y \times x$. Normally we write $x^{-1}$ for this element, and call it the **multiplicative inverse**. ◇

We may also refer to a multiplicative group as a **group under multiplication**.

Notation. We usually write $x \cdot y$ or even just $xy$ in place of $x \times y$.

Remark 2.27. The statements of (MG3) and (MG4) may seem odd, inasmuch as they imply that sometimes $x \times 1 \neq 1 \times x$ and $x \times y \neq y \times x$, but since we are not assuming the commutative property, this is important at first. We will show eventually that this is not necessary.

Even with this more restricted idea of multiplication, $\mathbb{R}^{m\times m}$ is not a group. However, we can now construct a group using a large subset of $\mathbb{R}^{m\times m}$.

Definition 2.28. The **general linear group of degree** $n$ is the set of invertible matrices of dimension $n \times n$.

Notation. We write $\mathrm{GL}_m(\mathbb{R})$ for the general linear group of degree $n$.

EXAMPLE 2.29. $\mathrm{GL}_m(\mathbb{R})$ is a multiplicative group. We leave much of the proof to the exercises, but the properties (MG1)–(MG4) are generally reviewed in linear algebra.

EXAMPLE 2.30. Every multiplicative group of order 2 has the same multiplication table. To see this, let $G$ be an arbitrary multiplicative group of order two. Then $G = \{1, a\}$. The properties of a multiplicative group imply that $a \times a = 1$, just as the properties of an additive group implied that $a + a = 0$ in the multiplication table of Example 2.6 on page 20. Thus the multiplication table look like:

| $\times$ | $1$ | $a$ |
|---|---|---|
| $1$ | $1$ | $a$ |
| $a$ | $a$ | $1$ |

The only assumption we made about $G$ is that it was a multiplicative group of order two. That means that we have completely determined the addition table of all multiplicative groups of order two! ◇

The structure of the multiplication table of a group of order two is *identical* to the structure of the addition table in Example 2.6. This suggests that there is no meaningful difference between additive and multiplicative groups of size two. Likewise, you will find in Exercises 2.37 and 2.38 that the multiplication tables for groups of order 3 and 4 are identical to the structure of the addition tables in Exercises 2.19 and 2.20: even the multiplication is commutative.

At this point a question arises:

*Although multiplication was not commutative in* $\mathrm{GL}_m(\mathbb{R})$,

*could it be commutative in every* ***finite*** *multiplicative group?*

The answer is no. In Exercise 2.47, you will meet a group of order 8 whose multiplication is not commutative.

Since multiplicative groups of orders 2, 3, and 4 must be commutative, but multiplicative groups of order 8 need not be commutative, a new question arises:

*Is multiplication necessarily commutative*

*in multiplicative groups of order 5, 6, or 7?*

The answer is, “it depends.” We delay the details until later.

You have now encountered additive and multiplicative groups. The only difference we have seen between them so far is that multiplication need not be commutative. Both Proposition 2.8 and Theorem 2.9 have parallels for multiplicative groups, and we could state them, but it is time to exploit the power of abstraction a little further.

EXERCISES.

EXERCISE 2.31. Let $m \in \mathbb{N}^+$. Explain why $\mathrm{GL}_m(\mathbb{R})$ satisfies properties (MG3) and (MG4) of the definition of a multiplicative group.

EXERCISE 2.32. Let $m \in \mathbb{N}^+$ and $G = \mathrm{GL}_m(\mathbb{R})$.

(a) Show that there exist $a, b \in G$ such that $(ab)^{-1} \neq a^{-1}b^{-1}$. *Hint:* Try $m = 2$, and find two invertible matrices $A, B$ such that $(AB)(A^{-1}B^{-1}) \neq I_2$.
(b) Show that for any $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$. *Hint:* Use the associative property to help simplify the expression $(ab)(b^{-1}a^{-1})$.

EXERCISE 2.33. 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 properties (MG1)–(MG4).

EXERCISE 2.34. 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 2.35. Show that $\mathbb{Q}^* \times \mathbb{Q}^*$ is a multiplicative group, where for all $x, y \in \mathbb{Q}^* \times \mathbb{Q}^*$ we have

$$xy = (x_1 y_1, x_2 y_2).$$

EXERCISE 2.36. Explain why $\mathbb{Z}$ is not a multiplicative group.

EXERCISE 2.37. Show that every multiplicative group of order 3 has the same multiplication table, and that this structure is in fact identical to that of an additive group of order 3.

EXERCISE 2.38. Show that there are only two possible multiplication tables for multiplicative groups of order 4, and that these correspond to the groups found in Exercise 2.20.

## 2.4. GENERIC GROUPS

Until now, we have defined groups using arbitrary sets, but specific operations: either addition, or multiplication. We now generalize the notion of a group to both arbitrary sets and arbitrary operations. The new definition will incorporate the principles of additive and multiplicative groups without forcing either into the mold of the other.

Our criteria for a "generic" group will incorporate the properties common to both additive and multiplicative groups, nothing more and nothing less. Additive groups satisfy all the properties of multiplicative groups, but add a commutative property; multiplicative groups, on the other hand, do *not* satisfy all the properties of additive groups. So a generic group should satisfy at least all the properties of a multiplicative group, but not necessarily all the properties of an additive group.

DEFINITION 2.39. Let $G$ be a set, and $\circ$ a binary operation on $G$. For convenience denote $x \circ y$ as $xy$. The pair $(G, \circ)$ is a **group under the operation** $\circ$ if $(G, \circ)$ satisfies the following properties.

(G1) The operation is closed; that is, $xy \in G$ for all $x, y \in G$.
(G2) The operation is associative; that is, $x(yz) = (xy)z$ for all $x, y, z \in G$.
(G3) There exists an element $e \in G$ such $xe = ex = x$ for all $x \in G$. We call this element the **identity**.
(G4) For every $x \in G$ there exists an element $y \in G$ such that $xy = yx = e$. Normally we write $x^{-1}$ for this element.

We say that $(G, \circ)$ is an **abelian group**[3] if it also satisfies

(G5) The operation is commutative; that is, $xy = yx$ for all $x, y \in G$. ◇

NOTATION. In Definition 2.39, the symbol $\circ$ is a placeholder for any operation. It can stand for addition, for multiplication, or for other operations that we have not yet considered. We adopt the following conventions:

[3]Named after Niels Abel, a Norwegian high school mathematics teacher who helped found group theory.

- If all we know is 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. For example, in Definition 2.39, as well as later, the symbol $\circ$ is provided for the operation, but we wrote $xy$ instead of $x \circ y$.
- We reserve the symbol $+$ exclusively for abelian group; *however,*
  - in some abelian groups we use multiplicative notation, and write $xy$.

Definition 2.39 allows us to classify both additive and multiplicative groups as generic groups. Additive groups are guaranteed to be abelian, while multiplicative groups are sometimes abelian, sometimes not. For this reason, from now on we generally abandon the designation "additive" group, preferring "abelian".

We can now generalize Proposition 2.8 and Theorem 2.9 as promised. The proofs are very easy—one needs merely rewrite them using the notation for a general group—so we leave that to the exercises.

Notice that we change the name of the operation from "addition" in Theorem 2.9 to the generic term "operation" in Theorem 2.41.

LEMMA 2.40. *Let $G$ be a group and $x \in G$. Then $\left(x^{-1}\right)^{-1} = x$.*

THEOREM 2.41. *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 operation table that is headed by $b$.*

The following lemma may look obviously true, but its proof isn't, and the result is important. It's better to make sure "obvious" things are true than to assume that they are, so we'll make sure of that now.

THEOREM 2.42. *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.*

The proof is similar to that of Proposition 2.7.

PROOF. Let $G$ be a group. Suppose now that $e$ 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

$$ei = e.$$

By substitution,

$$e = i.$$

We chose an arbitrary left identity of $G$ and an arbitrary right identity of $G$, 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.

A similar strategy shows that the inverse of an element is both two-sided and unique. 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,

$$xy = e.$$

Certainly $ex = x$, so substitution gives us

$$(xy)x = ex$$
$$x(yx) = x.$$

Since $w$ is a left inverse, $wx = e$, and substitution gives

$$w(x(yx)) = wx$$
$$(wx)(yx) = wx$$
$$e(yx) = e$$
$$yx = e.$$

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

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

Apply the associative property of $G$ to obtain

$$(yx)y = (yx)z.$$

Since $y$ is an inverse of $x$,

$$ey = ez.$$

Since $e$ is the identity of $G$,

$$y = z.$$

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

EXERCISES.

EXERCISE 2.43. 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 $(ab)^{-1} = b^{-1}a^{-1}$. *Hint:* Use Exercise 2.32.

EXERCISE 2.44. Prove Lemma 2.40.

EXERCISE 2.45. Prove Theorem 2.41.

EXERCISE 2.46. Let $G_1, G_2, \ldots, G_n$ be groups. Show that $G = G_1 \times G_2 \times \cdots \times G_n$ is also a group, where for all $x, y \in G$ we have

$$xy = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

EXERCISE 2.47. 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 multiplication table of $Q_8$.
(c) Show that $Q_8$ is a group under matrix multiplication.
(d) Explain why $Q_8$ is not an abelian group.

EXERCISE 2.48. 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 for $x$ and $y$ in a group $G$, the commutator of $x$ and $y$ 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 $[x,y]^z = [x^z, y^z]$.

## 2.5. CYCLIC GROUPS

At this point you can make an acquaintance with an important class of groups. Groups in this class have a nice, appealing structure.

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

$$g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g$$

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

$$g^{10}$$

instead. We likewise define $g^{-10}$ to represent

$$g^{-1} \cdot g^{-1} \cdot g^{-1} \cdot g^{-1} \cdot g^{-1} \cdot g^{-1} \cdot g^{-1} \cdot g^{-1} \cdot g^{-1} \cdot g^{-1}.$$

For consistency we need

$$g^0 = g^{10} g^{-10} = e.$$

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

- $g^n$ means to perform the group operation on $n$ copies of $g$;
- $g^{-n}$ means to perform the group operation on $n$ copies of $g^{-1}$;
- $g^0 = e$.

In abelian groups we write $ng$, $(-n)\,g$, and $0g$ for the same.

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 $G$. ◇

In other words, a cyclic group has the form $\{\ldots, g^{-2}, g^{-1}, e, g^1, g^2, \ldots\}$ where $g^0 = e$. If the group is abelian, we 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.

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 $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Here is another example from $\mathrm{GL}_m(\mathbb{R})$.

EXAMPLE 2.51. Let
$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$
It turns out that $G$ is a group, and that the second and third matrices both generate the group. For example,
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \diamond$$

The size of a cyclic group will prove useful later.

DEFINITION 2.52. Let $G$ be a group, and $g \in G$. We say that the **order** of $g$ is $\operatorname{ord}(g) = |\langle g \rangle|$. If $\operatorname{ord}(g) = \infty$, we say that $g$ has **infinite order**. ◇

If the order of a group is finite, then we have many different ways to represent the same element. Taking the matrix we examined in Example 2.51, we can write
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^8 = \cdots$$
and
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-4} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-8} = \cdots.$$
In addition,
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^3 \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}.$$
So it would seem that if the order of an element $G$ is $n \in \mathbb{N}$, then we can write
$$G = \left\{ e, g, g^2, \ldots, g^{n-1} \right\}.$$
The examples we have looked at so far suggest this, but they are only examples. To prove it in general, we have to show that for a generic cyclic group $\langle g \rangle$ with $\operatorname{ord}(g) = n$,

- $g^n = e$, and
- if $a, b \in \mathbb{Z}$ and $n \mid (a - b)$, then $g^a = g^b$.

THEOREM 2.53. *Suppose that $G$ is a group, $g \in G$, and* $\operatorname{ord}(g) = n$*, where $n \neq \infty$. Each of the following holds.*

*(A)* $g^n = e$.
*(B)* *$n$ is the smallest positive integer $d$ such that $g^d = e$.*
*(C)* *If $a, b \in \mathbb{Z}$ and $n \mid (a-b)$, then $g^a = g^b$.*

We are not yet ready to prove Theorem 2.53. First we need a lemma which happens to be a useful tool even for non-cyclic groups.

LEMMA 2.54. *Let $G$ be a group, $g \in G$, and $\operatorname{ord}(g) = n$. For all $a, b \in \mathbb{N}$ such that $0 \leq a < b < n$, we have $g^a \neq g^b$.*

PROOF. Let $H = \langle g \rangle$. By hypothesis, $\operatorname{ord}(g) = n$, so $|H| = n$.

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 2.57, we can write

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

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 $d \leq b - a$. By Exercise 1.20, $b > d$, so $n > b > d > 0$.

We can now list $d$ distinct elements of $H$:

$$g, g^2, g^3, \ldots, g^d = e. \tag{2.5.1}$$

Since $d < n$ and $|H| = n$, this list omits $d - n$ elements of $H$. Let $x$ be one such element. Since $H = \langle g \rangle$, we can express $x = g^c$ for some $c \in \mathbb{Z}$. If $c = 0$, then $x = g^0 = e$. But we already listed that above: $g^d = e$, so $c \neq 0$.

Let $q, r$ be the result from applying the Division Theorem to division of $c$ by $d$. Then $g^c = g^{qd+r}$. By Exercise 2.57,

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

By the Division Theorem, $0 \leq r < d$, we have already listed $g^r$. This contradicts the assumption that $g^c = g^r$ was not listed. Hence if $0 \leq a < b < n$, then $g^a \neq g^b$. □

Now we can use the lemma prove Theorem 2.53.

PROOF OF THEOREM 2.53. Let $H = \langle g \rangle$. By hypothesis, $\operatorname{ord}(g) = n$, so $|H| = n$.

If $n = 1$ then $H = \{e\} = \langle e \rangle$, and the theorem is trivial. Assume therefore that $n > 1$.

Since $H$ is a group, $e \in H$; since $H = \langle g \rangle$, some power of $g$ generates $e$. 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 $d$. Since $H$ contains $n$ elements, $1 < d \leq n$. But $d < n$ contradicts Lemma 2.54 (with $a = 0$ and $b = d$). Hence $d = n$, and $g^n = e$, and we have shown (A).

We have also shown (B). Why? $d$ was the smallest element of $S$.

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

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

and we have shown (C). □

EXERCISES.

EXERCISE 2.55. In Exercise 2.47 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 2.56. Recall from Section 2.2 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 $E$. *Hint:* This goes a lot faster if you work with approximate numbers.

EXERCISE 2.57. Let $G$ be a group, and $x \in G$. Explain why for all $m, n \in \mathbb{Z}$,

(a) $x^{mn} = (x^m)^n$;
(b) $x^{-m} = (x^m)^{-1}$;
(c) $x^{-(mn)} = (x^m)^{-n}$;
(d) $x^{-(mn)} = \left(x^{-m}\right)^n$.

*Hint:* Once you show (a), you can use it to explain the rest.

EXERCISE 2.58. Let $G$ be a group, and $g \in G$. Assume $\operatorname{ord}(g) = d$. Show that $g^n = e$ if and only if $d \mid n$. *Hint:* Use Theorem 2.53.

EXERCISE 2.59. Show that any group of 3 elements is cyclic. *Hint:* Look back at Exercise 2.19 on page 22.

EXERCISE 2.60. Is the Klein 4-group (Exercise 2.20 on page 23) cyclic? What about the cyclic group of order 4?

EXERCISE 2.61. Show that $Q_8$ is not cyclic.

EXERCISE 2.62. Show that $\mathbb{Q}$ is not cyclic. *Hint:* 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 2.63. Use a fact from linear algebra to explain why $\mathrm{GL}_m(\mathbb{R})$ is not cyclic.

EXERCISE 2.64. Explain why every cyclic group is abelian.

## 2.6. THE SYMMETRIES OF A TRIANGLE

We conclude this first chapter with a very important group, called $D_3$. It derives from the symmetries of a triangle. What is interesting about this group is that *it is not abelian.* You already know that groups of order 2, 3, and 4 are abelian; in Section 3.3 you will why a group of order 5 must also be abelian. Thus $D_3$ is the smallest non-abelian group.

Draw an equilateral triangle in $\mathbb{R}^2$, with its center at the origin. What distance-preserving functions map $\mathbb{R}^2$ to itself, while mapping points on the triangle back onto 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, *without moving the origin?* (By distance, we mean the usual, Euclidean measure,

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

(2) Which of these functions map points on the triangle back onto the triangle?

Lemma 2.65 answers the first question. The assumption that we not move the origin makes sense in the context of the triangle, because if we preserve distances, the origin will have to stay fixed as well.

LEMMA 2.65. *Let* $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$. *If*

- $\alpha(0,0) = (0,0)$, *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* $\alpha$ *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.)

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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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

$$(\cos t - s_1)^2 + (\sin t - s_2)^2 = 2. \tag{2.6.1}$$

We can simplify (2.6.1) to obtain

$$-2(s_1 \cos t + s_2 \sin t) + \left(s_1^2 + s_2^2\right) = 1. \tag{2.6.2}$$

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 (2.6.2), we find that

$$\begin{aligned}-2\left(s_1\cos t+s_2\sin t\right)+s_1^2+s_2^2&=1\\ -2\left(s_1\cos t+s_2\sin t\right)+1&=1\\ -2\left(s_1\cos t+s_2\sin t\right)&=0\\ s_1\cos t&=-s_2\sin t.\end{aligned}\tag{2.6.3}$$

At this point we can see that $s_1=\sin t$ and $s_2=\cos t$ would solve the problem. 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 (2.6.3) 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 (2.6.3), 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 2.70) that $\alpha$ 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

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

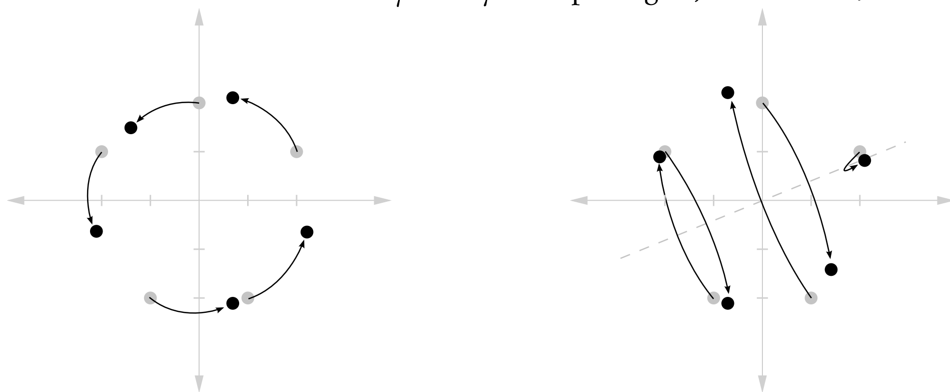
The lemma names the first of these forms $\varphi$ and the second $\rho$. □

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

EXAMPLE 2.66. Consider the set of points $\mathcal{S}=\{(0,2),(\pm2,1),(\pm1,-2)\}$; these form 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 2.1. Actions of $\rho$ and $\varphi$ on a pentagon, with $t = \pi/4$



$\rho$ $\varphi$

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

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

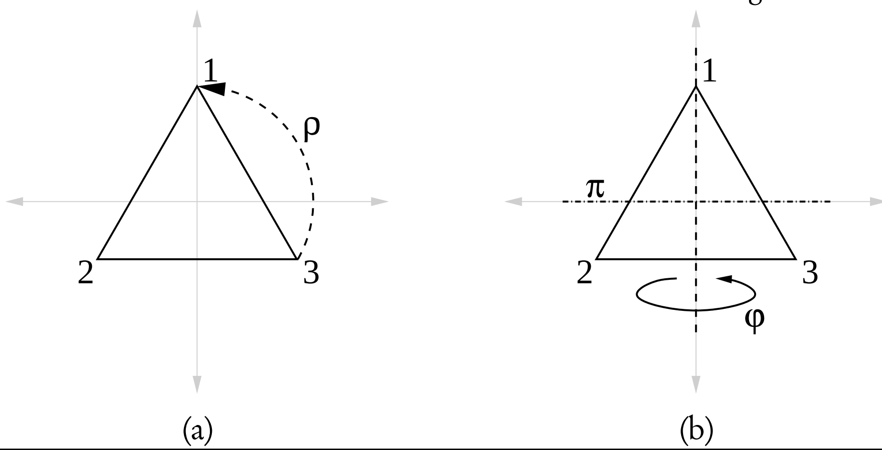
This is shown in Figure 2.1 . The line of reflection for $\varphi$ has slope $\left(1 - \cos\frac{\pi}{4}\right) / \sin\frac{\pi}{4}$. (You will show this in Exercise 2.72) $\diamond$

The second questions asks which of the matrices described by Lemma 2.65 also preserve the triangle.

- The first solution ($\rho$) 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 2.2(a).) Let $\iota$ correspond to $t = 0$, the identity rotation; notice that

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

FIGURE 2.2. Rotation and reflection of the triangle




which is what we would expect for the identity. We can let $\rho$ correspond to a counterclockwise 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 $\rho^2$; 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 ($\varphi$) 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 2.2(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 $\varphi$ and $\rho$. (Why? See Exercise 2.69.)

We have the following interesting consequence.

COROLLARY 2.67. *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 2.67? 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 $\varphi\rho \neq \rho\varphi$.

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.

EXERCISES.

EXERCISE 2.68. The multiplication table for $D_3$ has at least this structure:

| $\circ$ | $\iota$ | $\varphi$ | $\rho$ | $\rho^2$ | $\rho\varphi$ | $\rho^2\varphi$ |
|---|---|---|---|---|---|---|
| $\iota$ | $\iota$ | $\varphi$ | $\rho$ | $\rho^2$ | $\rho\varphi$ | $\rho^2\varphi$ |
| $\varphi$ | $\varphi$ | | $\rho^2\varphi$ | | | |
| $\rho$ | $\rho$ | $\rho\varphi$ | | | | |
| $\rho^2$ | $\rho^2$ | | | | | |
| $\rho\varphi$ | $\rho\varphi$ | | | | | |
| $\rho^2\varphi$ | $\rho^2\varphi$ | | | | | |

Complete the multiplication table, writing every element in the form $\rho^m\varphi^n$, never with $\varphi$ before $\rho$. Explain how $D_3$ satisfies the properties of a group. *Hint:* To rewrite products so that $\rho$ never precedes $\varphi$, use Corollary 2.67. To show that $D_3$ satisfies the properties of a group, you may use the fact that $D_3$ is a subset of GL(2), the multiplicative group of $2\times 2$ invertiable matrices. Thus $D_3$ "inherits" certain properties of GL(2), but which ones? For the others, simple inspection of the multiplication table should suffice.

EXERCISE 2.69. 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 2.70. Show that any function $\alpha$ satisfying the requirements of Theorem 2.65 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 $\mathbb{R}^2$. *Hint:* 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 $Y$.

(b) Show that $\alpha(1,0)\cdot\alpha(0,1) = 0$.

(c) Show that $\alpha((a,0)+(0,b)) = a\alpha(1,0) + b\alpha(0,1)$. *Hint:* 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).

(d) Show that $\alpha(aP) = a\alpha(P)$.
(e) Show that $\alpha(P+Q) = \alpha(P) + \alpha(Q)$.

EXERCISE 2.71. Show that the only point in $\mathbb{R}^2$ left stationary by $\rho$ is the origin. That is, if $\rho(P) = P$, then $P = (0,0)$. *Hint:* Let $P = (p_1, p_2)$ be an arbitrary point in $\mathbb{R}^2$, and assume that $\rho$ 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 2.72. Show that the only points in $\mathbb{R}^2$ left stationary by $\varphi$ lie along the line whose slope is $(1-\cos t)/\sin t$. *Hint:* Repeat what you did in Exercise 2.71. 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.

CHAPTER 3

# Subgroups and Quotient Groups

A subset of a group is not necessarily a group; for example, $\{2,4\} \subset \mathbb{Z}$, but $\{2,4\}$ doesn't satisfy any of the properties of an additive group. Some subsets of groups are 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 marvelous new mathematical worlds. They enable a special class of subgroups called *quotient groups*, (Sections 3.4), one of which is a very natural, very useful tool (Section 3.5).

## 3.1. SUBGROUPS

DEFINITION 3.1. Let $G$ be a group and $H \subseteq G$ a nonempty subset. 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. If $H$ is a subgroup of $G$ then we write $H < G$.

EXAMPLE 3.2. Check that the following statements are true by verifying that properties (G1)–(G4) 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 of properties (G1)–(G4) is burdensome. 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, that its subgroups would be abelian, so we shouldn't have to check (G5) either. So which properties *must* we check to decide whether a subset is a subgroup?

To start with, we can eliminate (G2) and (G5) from consideration. In fact, the operation remains associative and commutative for any subgroup.

LEMMA 3.3. *Let $G$ be a group and $H \subseteq G$. Then $H$ satisfies the associative property (G2) of a group. In addition, if $G$ is abelian, then $H$ satisfies the commutative property (G5) of an abelian group.*

Be careful: Lemma 3.3 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 3.3 *does* imply that if we want to prove that a subset of a group is also a subgroup, then we do not have to prove the associative and commutative properties, (G2) and (G5). We need to prove only that the subsets have an identity, have inverses, and are closed under the operation.

LEMMA 3.4. *Let $H \subseteq G$ be nonempty. The following are equivalent:*
*(A) $H < G$;*
*(B) $H$ satisfies (G1), (G3), and (G4).*

PROOF. By definition of a group, (A) implies (B). The assumption that $H$ is nonempty is essential, since otherwise $H$ would not have an identity element, so it could not satisfy (G3).

It remains to show that (B) implies (A). Assume (B). Then $H$ satisfies (G1), (G3), and (G4). Lemma 3.3 shows us that $H$ also satisfies (G2). Hence $H$ is a group, from which we have (A). □

Lemma 3.4 has reduced the number of requirements for a subgroup from four to three. Three is still too many; amazingly, we can simplify this 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. Observe that if $G$ were an abelian group, we would write $x - y$ instead of $xy^{-1}$.

PROOF. Assume (A). Let $x, y \in H$. By (A), $H$ is a group; from (G4) we have $y^{-1} \in H$, and from (G1) we have $xy^{-1} \in H$. Thus (A) implies (B).

Conversely, assume (B). By Lemma 3.4, we need to show only that $H$ satisfies (G1), (G3), and (G4). We do this slightly out of order:

(G3): Let $x \in H$. By (B), $e = x \cdot x^{-1} \in H$.[1]
(G4): Let $x \in H$. Since $H$ satisfies (G3), $e \in H$. By (B), $x^{-1} = e \cdot x^{-1} \in H$.
(G1): Let $x, y \in H$. Since $H$ satisfies (G4), $y^{-1} \in H$. By (B), $xy = x \cdot \left(y^{-1}\right)^{-1} \in H$.

Since $H$ satisfies (G1), (G3), and (G4), $H < G$. □

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 3.6. Let $d \in \mathbb{Z}$. We claim that $d\mathbb{Z} < \mathbb{Z}$. *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

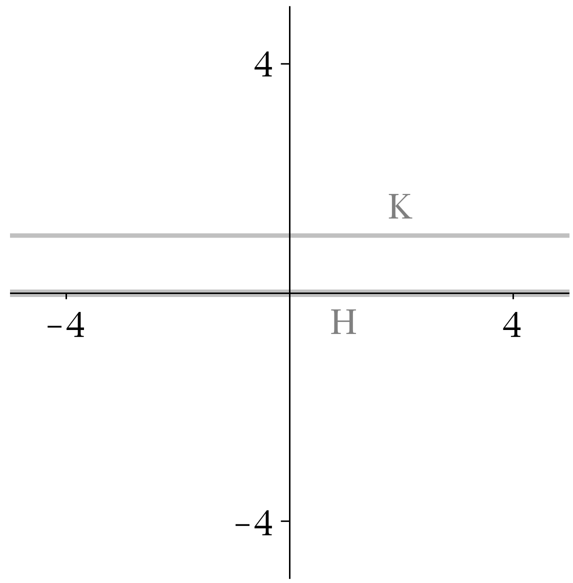
$$x - y = x + (-y) = dm + d(-n) = d(m + (-n)) = d(m - n).$$

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.

[1]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 3.7




---

EXAMPLE 3.7. 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

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

You showed in Exercise 2.16 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 3.13. $\diamondsuit$

Examples 3.6 and 3.7 give us examples of how the Subgroup Theorem verifies subgroups of *abelian* groups. Two interesting examples of nonabelian subgroups appear in $D_3$.

EXAMPLE 3.8. Recall $D_3$ from Section 2.6. Both $H = \{\iota, \varphi\}$ and $K = \{\iota, \rho, \rho^2\}$ are subgroups of $D_3$. *Why?* Use the Subgroup Theorem, exploiting the fact that both $H$ and $K$ are cyclic groups: $H = \langle \varphi \rangle$ and $K = \langle \rho \rangle$.

For $H$: Let $x, y \in H$. Since $H = \langle \varphi \rangle$, $x = \varphi^m$ and $y = \varphi^n$ for some $m, n \in \mathbb{Z}$. Applying Exercise 2.57 on page 34, $xy^{-1} = \varphi^m \varphi^{-n} = \varphi^{m-n} \in \langle \varphi \rangle = H$. By the Subgroups Theorem, $H < D_3$.

For $K$: Repeat the argument for $H$, using $\rho$ instead of $\varphi$. ◇

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 1.15 on page 15).

THEOREM 3.9. *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 $H$. Because $H \subseteq G$, every element $x \in H$ can be written in the form $x = g^i$ for some $i \in \mathbb{Z}$. A good candidate would be the smallest positive power of $g$ in $H$, if one exists. Let $S = \left\{ i \in \mathbb{N}^+ : g^i \in H \right\}$. From the well-ordering of $\mathbb{N}$, there exists a smallest element of $S$; call it $d$, and assign $h = g^d$.

We have found a candidate; 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 2.57 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 (G1) and the existence of inverses (G4), 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 3.10. Recall from Example 2.50 on page 32 that $\mathbb{Z}$ is cyclic; in fact $\mathbb{Z} = \langle 1 \rangle$. By Theorem 3.9, $d\mathbb{Z}$ is cyclic. In fact, $d\mathbb{Z} = \langle d \rangle$. Can you find another generator of $d\mathbb{Z}$? ◇

EXERCISES.

EXERCISE 3.11. Show that even though the Klein 4-group is not cyclic, each of its proper subgroups is cyclic (see Exercises 2.20 on page 23 and 2.60 on page 34). *Hint:* Start with the smallest possible subgroup, then add elements one at a time. Don't forget the adjective "proper" subgroup.

EXERCISE 3.12.

(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 2.18, 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 2.28, the operation here is multiplication.)

EXERCISE 3.13. Let $G = \mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$, with addition defined as in Exercise 2.16 and Example 3.7. 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. *Hint:* Look at what $L$ has in common with $H$ from Example 3.7.

EXERCISE 3.14. Let $G$ be any group and $g \in G$. Show that $\langle g \rangle < G$.

EXERCISE 3.15. 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 3.16. 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 3.15?

EXERCISE 3.17. Explain why $\mathbb{R}$ cannot be cyclic. *Hint:* Use Exercise 2.62 on page 34.

EXERCISE 3.18. 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 3.19. 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 $G$. *Hint:* Look at Exercise 3.16

## 3.2. COSETS

Recall the Division Theorem (Theorem 1.15 on page 15). 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

$$\begin{aligned} A &= \{\ldots, -4, 0, 4, 8, \ldots\} \\ B &= \{\ldots, -3, 1, 5, 9, \ldots\} \\ C &= \{\ldots, -2, 2, 6, 10, \ldots\} \\ D &= \{\ldots, -1, 3, 7, 11, \ldots\}. \end{aligned} \tag{3.2.1}$$

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 3.20. 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
- the 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 3.21. Let $\mathcal{B} = \{A, B, C, D\}$ where $A$, $B$, $C$, and $D$ are defined as in (3.21). 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.

Re-examine this phenomenon using the vocabulary of groups. In the example above, you might have noticed that $A = 4\mathbb{Z}$. (If not, look back at the definition of $4\mathbb{Z}$ on page 41.) So, $A < \mathbb{Z}$. Meanwhile, 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 $x \in A$. Define
$$1 + A := \{1 + x : x \in A\},$$
then set
$$B = 1 + A.$$
Likewise, set $C = 2 + A$ and $D = 3 + A$.

What about $0 + A$? Clearly $0 + A = A$; in fact $x + A = A$ for every $x \in A$:
$$\begin{aligned} &\vdots \\ -4 + A &= \{\ldots, -8, -4, 0, 4, \ldots\} = A \\ 0 + A &= \{\ldots, -4, 0, 4, 8, \ldots\} = A \\ 4 + A &= \{\ldots, 0, 4, 8, 16, \ldots\} = A \\ &\vdots \end{aligned}$$

So

$$\cdots = -4 + A = A = 0 + A = 4 + A = 8 + A = \cdots.$$

Pursuing this further, you can check that

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

and so forth. Interestingly, all of these sets are the same as $B$! Notice that $1 + B = 5 + B$ and $1 - 5 = -4 \in A$. The same holds for $C$: $C = 2 + A$ and $C = 10 + A$, 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.

Mathematicians love to generalize any phenomena they observe, and this is no exception. How can we generalize this to arbitrary subgroups?

DEFINITION 3.22. 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 abelian subgroup, we write the coset of $A$ with $g$ as

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

In general, left cosets and right cosets are not equal, partly because the operation might not commute.

EXAMPLE 3.23. Recall the group $D_3$ from Section 2.6 and the subgroup $H = \{\iota, \varphi\}$ from Example 3.8. 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 $\rho H \neq H\rho$. $\diamond$

Sometimes, the left coset and the right coset *are* equal. This is always true in abelian groups, as illustrated by Example 3.24.

EXAMPLE 3.24. Consider the subgroup $H = \{(a, 0) : a \in \mathbb{R}\}$ of $\mathbb{R}^2$ from Exercise 3.13. 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 3.13. 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 $\mathbb{R}^2$? $\diamond$

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 commute*, but *whether sets 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 3.25. Let $K = \{\iota, \rho, \rho^2\}$; certainly $K < D_3$. In this case, $\alpha K = K\alpha$ for all $\alpha \in D_3$:

| $\alpha$ | $\alpha K$ | $K\alpha$ |
|---|---|---|
| $\iota$ | $K$ | $K$ |
| $\varphi$ | $\{\varphi, \varphi\rho, \varphi\rho^2\} = \{\varphi, \rho\varphi, \rho^2\varphi\}$ | $\{\varphi, \rho\varphi, \rho^2\varphi\}$ |
| $\rho$ | $K$ | $K$ |
| $\rho^2$ | $K$ | $K$ |
| $\rho\varphi$ | $\{\rho\varphi, (\rho\varphi)\rho, (\rho\varphi)\rho^2\} = \{\rho\varphi, \varphi, \rho^2\varphi\}$ | $\{\rho\varphi, \varphi, \rho^2\varphi\}$ |
| $\rho^2\varphi$ | $\{\rho^2\varphi, (\rho^2\varphi)\rho, (\rho^2\varphi)\rho^2\} = \{\rho^2\varphi, \rho\varphi, \varphi\}$ | $\{\rho^2\varphi, \rho\varphi, \varphi\}$ |

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

We can now explain why cosets of a subgroup partition a group.

THEOREM 3.26. *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 $G$. □

Before we finish, we should observe two facts about cosets that parallel facts about $A$ in the example at the beginning of the section. These facts allow us to decide when two cosets are equal.

LEMMA 3.27 (Equality of cosets). *Let $G$ be a group and $H < G$. We have (CE1), (CE2), and (CE2), where:*

*(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 $a, b \in H$, $a + H = b + G$ if and only if $a - b \in H$.

PROOF. You do it! See Exercise 3.33. □

EXERCISES.

EXERCISE 3.28. Let $\{e, a, b, a+b\}$ be the Klein 4-group. (See Exercises 2.20 on page 23, 2.60 on page 34, and 3.11 on page 44.) Compute the cosets of $\langle a \rangle$.

EXERCISE 3.29. In Exercise 3.16 on page 45, 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 3.30. Recall the subgroup $L$ of $\mathbb{R}^2$ from Exercise 3.13 on page 45.

(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 3.31. Recall $D_n(\mathbb{R})$ from Exercise 3.12 on page 44. 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 3.32. In the proof of Theorem 3.26 on the preceding page, we stated that "A similar argument shows that $xA \supseteq yA$." Give this argument.

EXERCISE 3.33. Prove Lemma 3.27 on the previous page. *Hint:* For (CE1), you have to show that two sets are equal. Follow the structure of the proof for Theorem 3.26 on the preceding page. 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).

## 3.3. LAGRANGE'S THEOREM AND THE ORDER OF AN ELEMENT OF A GROUP

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. 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 $G \backslash A$ for the set of all right cosets of $A$ (but not as often):

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

EXAMPLE 3.34. Let $G = \mathbb{Z}$ and $A = 4\mathbb{Z}$. We saw in Example 3.21 that

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

We actually "waved our hands" in Example 3.21. 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, $q + r \in \mathbb{Z}$. If we write $m$ in place of $4(q + r)$, 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. $\diamond$

EXAMPLE 3.35. Let $G = D_3$ and $H = \{\iota, \varphi\}$ as in Example 3.25. Then

$$G/K = D_3/\langle\varphi\rangle = \left\{K, \rho A, \rho^2 A\right\}.$$

Likewise, if $K = \left\{\iota, \rho, \rho^2\right\}$ as in Example 3.25, then

$$G/K = D_3/\langle\rho\rangle = \{K, \varphi A\}. \diamond$$

EXAMPLE 3.36. Let $H < \mathbb{R}^2$ be as in Example 3.7 on page 43; 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? $\diamond$

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 3.37 (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 3.26 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 3.38. *The order of a subgroup divides the order of a group.*

EXAMPLE 3.39. Let $G$ be the Klein 4-group (see Exercises 2.20 on page 23, 2.60 on page 34, and 3.11 on page 44). Every subgroup of the Klein 4-group is cyclic, and has order 1, 2, or 4. As predicted by Corollary 3.38, 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 3.16 on page 45 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 3.40. *In a finite group $G$, the order of any element divides the order of a group.*

PROOF. You do it! See Exercise 3.41. □

EXERCISES.

EXERCISE 3.41. Prove Corollary 3.40.

EXERCISE 3.42. Suppose that a group $G$ has order 8, but is not cyclic. Show that $g^4 = e$ for all $g \in G$.

EXERCISE 3.43. Suppose that a group has five elements. Will it be cyclic? *Hint:* Use Corollary 3.40.

EXERCISE 3.44. Find a sufficient (but not necessary) condition on the order of a group that guarantees that the group is cyclic. *Hint:* See Exercises 2.59 on page 34 and 3.43.

## 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 map defined above would not be an operation if two different representations of $gA$ gave us two different answers.

EXAMPLE 3.45. Recall the subgroup $A = 4\mathbb{Z}$ of $\mathbb{Z}$. Let $B, C, D \in \mathbb{Z}/A$, so $B = b + \mathbb{Z}$, $C = c + \mathbb{Z}$, and $D = d + \mathbb{Z}$ 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 3.27, 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 $B + C = D + C$. $\diamondsuit$

So the operation was well-defined here. This procedure looks promising, doesn't it? However, 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 $4m$. Example 3.46 shows how it can go wrong.

EXAMPLE 3.46. Recall $A = \langle \varphi \rangle < D_3$ from Example 3.35. 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 $\rho A = \left\{\rho\varphi, \rho\varphi^2\right\}$ 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:

$$((\rho\varphi)A)\left(\rho^2 A\right) = \left((\rho\varphi)\rho^2\right)A = \left(\rho\left(\varphi\rho^2\right)\right)A = (\rho(\rho\varphi))A = \left(\rho^2\varphi\right)A \neq A. \diamondsuit$$

So the procedure described at the beginning of this section does *not* always result in an operation on cosets of non-abelian groups. Can we identify a condition on a subgroup that would guarantee that the procedure results in an operation?

The key in Example 3.45 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 3.47. Let $A < G$. If

$$gA = Ag$$

for every $g \in G$, then $A$ is a **normal subgroup** of $G$.

NOTATION. We write $A \triangleleft G$ to indicate that $A$ is a normal subgroup of $G$.

An easy generalization of the argument of Example 3.45 shows the following Theorem.

THEOREM 3.48. *Let $G$ be an abelian group, and $H < G$. Then $H \triangleleft G$.*

PROOF. You do it! See Exercise 3.54. □

We now present our first non-abelian normal subgroup.

EXAMPLE 3.49. 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,

| $\sigma$ | $\sigma A_3$ | $A_3\sigma$ |
|---|---|---|
| $\iota$ | $A_3$ | $A_3$ |
| $\rho$ | $A_3$ | $A_3$ |
| $\rho^2$ | $A_3$ | $A_3$ |
| $\varphi$ | $\varphi A_3 = \{\varphi, \varphi\rho, \varphi\rho^2\} = \{\varphi, \rho^2\varphi, \rho\varphi\} = A_3\varphi$ | $A_3\varphi = \varphi A_3$ |
| $\rho\varphi$ | $\{\rho\varphi, (\rho\varphi)\rho, (\rho\varphi)\rho^2\} = \{\rho\varphi, \varphi, \rho^2\varphi\} = \varphi A_3$ | $\varphi A_3$ |
| $\rho^2\varphi$ | $\{\rho^2\varphi, (\rho^2\varphi)\rho, (\rho^2\varphi)\rho^2\} = \{\rho^2\varphi, \rho\varphi, \varphi\} = \varphi A_3$ | $\varphi A_3$ |

(We have left out some details of the computation. You should check them very carefully, using extensively the fact that $\varphi\rho = \rho^2\varphi$.) 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

| $\circ$ | $A_3$ | $\varphi A_3$ |
|---|---|---|
| $A_3$ | $A_3$ | $\varphi A_3$ |
| $\varphi A_3$ | $\varphi A_3$ | $A_3$ |

Compare the operation table of $D_3/A_3$ to those of Examples 2.6 on page 20 and 2.30 on page 27.)
◇

As we wanted, normal subgroups allow us to turn the set of cosets into a group $G/A$.

THEOREM 3.50. *Let $G$ be a group. If $A \triangleleft G$, then $G/A$ is a group.*

PROOF. We show that $G/A$ satisfies properties (G1)–(G4) of a group.

(G1): Closure follows from the fact that multiplication of cosets is well-defined when $A \triangleleft G$, as discussed earlier in this section: 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.

(G2): The associative property follows from the associative property of the elements of the group. 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,

$$(XY)Z = ((g_1g_2)A)(g_3A).$$

Let $h = g_1g_2$, so $(g_1g_2)A = hA$. By substitution and the definition of coset multiplication,

$$\begin{aligned}(XY)Z &= (hA)(g_3A) \\ &= (hg_3)A \\ &= ((g_1g_2)g_3)A.\end{aligned}$$

By the associative property of the group $G$, $(g_1g_2)g_3 = g_1(g_2g_3)$. By substitution, and reveresing the previous steps, we find that

$$\begin{aligned}(XY)Z &= (g_1(g_2g_3))A \\ &= (g_1A)((g_2g_3)A) \\ &= (g_1A)[(g_2A)(g_3A)] \\ &= X(YZ).\end{aligned}$$

Since $(XY)Z = X(YZ)$ and $X,Y,Z$ were arbitrary in $G/A$, coset multiplication is associative.

(G3): 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 3.27 on page 48 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 $G/A$.

(G4): 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,

$$XY = (gA)\left(g^{-1}A\right) = \left(gg^{-1}\right)A = eA = A.$$

Hence $X$ has an inverse in $G/A$. Since $X$ was arbitrary in $G/A$, every element of $G/A$ has an inverse.

□

We need a definition for this new kind of group.

DEFINITION 3.51. 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.

EXERCISES.

EXERCISE 3.52. 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 3.53. 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 3.54. Let $G$ be an abelian subgroup. Explain why for any $H < G$ we know that $H \triangleleft G$.

EXERCISE 3.55. Recall the subgroup $L$ of $\mathbb{R}^2$ from Exercises 3.13 on page 45 and 3.30 on page 49.
(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 3.56. Explain why every subgroup of $D_m(\mathbb{R})$ is normal. (*Hint:* Theorem 3.48 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 3.57. Show that $Q_8$ is not a normal subgroup of $\mathrm{GL}_m(\mathbb{R})$.

EXERCISE 3.58. Let $G$ be a group. Define the **centralizer** of $G$ as

$$Z(G) = \{g \in G : xg = gx \ \forall x \in G\}.$$

Show that $Z(G) \triangleleft G$. *Hint:* 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 3.59. Let $G$ be a group, and $H < G$. Define the **normalizer** of $H$ as

$$N_G(H) = \{g \in G : gH = Hg\}.$$

Show that $H \triangleleft N_G(H)$. *Hint:* 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 3.60. 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 $A \triangleleft G$. *Hint:* List the two left cosets, then the two right cosets. What does a partition mean? Given that, what sets must be equal?

EXERCISE 3.61. Recall from Exercise 2.48 on page 31 the commutator of two elements of a group. Let $[G,G]$commutator subgroup of a group $G$ denote the intersection of all subgroups of $G$ that contain a commutator.
(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 $G$. *Hint:* You need 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.

## 3.5. "CLOCKWORK" GROUPS

By Theorem 3.48, 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 3.62. 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. It is common to write $\mathbb{Z}_n$ instead of $\mathbb{Z}/n\mathbb{Z}$.

This group has several different properties that are both interesting and powerful.

THEOREM 3.63. *$\mathbb{Z}_n$ is a finite group for every $n\in\mathbb{Z}$. In fact $\mathbb{Z}_n$ has $n$ elements corresponding to the remainders from division by $n$: $0, 1, 2, \ldots, n-1$.*

It should not surprise you that the proof of Theorem 3.63 relies 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 3.34 on page 50, so you might want to reread that.

PROOF. Let $n\in\mathbb{Z}$. To show that $\mathbb{Z}_n$ is finite, we will list its elements. Since $\mathbb{Z}_n$ is the set of cosets of $n\mathbb{Z}$, any element of $\mathbb{Z}_n$ has the form $a+n\mathbb{Z}$ for some $a\in\mathbb{Z}$.

Let $A\in n\mathbb{Z}$ and choose $a$ such that $A=a+n\mathbb{Z}$. Use the Division Theorem to find $q,r\in\mathbb{Z}$ such that $a=qn+r$ and $0\le r<n$. Applying substitution and properties of arithmetic,

$$\begin{aligned}
A &= a+n\mathbb{Z}\\
&= \{a+nz : z\in\mathbb{Z}\}\\
&= \{(qn+r)+nz : z\in\mathbb{Z}\}\\
&= \{r+n(q+z) : z\in\mathbb{Z}\}\\
&= \{r+m : m\in n\mathbb{Z}\}\\
&= r+n\mathbb{Z}.
\end{aligned}$$

Thus $A$ corresponds to a coset $r+n\mathbb{Z}$, where $r$ is a remainder from division by $n$. Since $A$ was arbitrary, *every* element of $\mathbb{Z}_n$ corresponds to a coset $r+n\mathbb{Z}$, where $r$ is a remainder from division by $n$. How many remainders are there? The possible values are $0, 1, \ldots, n-1$, so all the elements of $\mathbb{Z}_n$ are $n\mathbb{Z}$, $1+n\mathbb{Z}$, $2+n\mathbb{Z}$, $\ldots$, $(n-1)+n\mathbb{Z}$. It follows that $\mathbb{Z}_n$ is finite. $\square$

It is burdensome to write $a+n\mathbb{Z}$ whenever we want to discuss an element of $\mathbb{Z}_n$, so mathematicians usually adopt the following convention.

NOTATION. 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.

Since $\mathbb{Z}_n$ is finite, we can create the addition table for every $n \in \mathbb{Z}$. Since the representation of elements of $\mathbb{Z}_n$ is the remainder on division by $n$, we want $[a]_n + [b]_n = [r]_n$ where $0 \le r < n$. For small numbers this isn't too hard. In $\mathbb{Z}_3$ for example,

$$[1]_3 + [1]_3 = (1+3\mathbb{Z}) + (1+3\mathbb{Z}) = (1+1) + 3\mathbb{Z} = [2]_3 .$$

But what should we do with larger sums, such as $[1]_3 + [2]_3$? Although we *can* write $[3]_3$, we'd rather not, because 3 is not a valid remainder when we divide by 3.

LEMMA 3.64. *Let $[a]_n \in \mathbb{Z}_n$. Use the Division Theorem to choose $q, r \in \mathbb{Z}$ such that $a = qn + r$ and $0 \le r < n$. Then $[a]_n = [r]_n$.*

PROOF. By definition and substitution,

$$\begin{aligned}
[a]_n &= a + n\mathbb{Z} \\
&= (qn + r) + n\mathbb{Z} \\
&= \{(qn + r) + nd : d \in \mathbb{Z}\} \\
&= \{r + n(q + d) : d \in \mathbb{Z}\} \\
&= \{r + nm : m \in \mathbb{Z}\} \\
&= r + n\mathbb{Z} \\
&= [r]_n .
\end{aligned}$$

□

DEFINITION 3.65. We call $[r]_n$ in Lemma 3.64 the **canonical representation** of $[a]_n$.

LEMMA 3.66. *Let $d, n \in \mathbb{Z}$ and $[a]_n, [b]_n \in \mathbb{Z}_n$. Then*

$$[a]_n + [b]_n = [a+b]_n \qquad \textit{and} \qquad d\,[a]_n = [da]_n .$$

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 addition of $d$ copies of $[a]_n$, which the previous paragraph implies to be

$$\underbrace{[a]_n + [a]_n + \cdots + [a]_n}_{d \text{ times}} \quad = \quad [2a]_n + \underbrace{[a]_n + \cdots + [a]_n}_{d-2 \text{ times}} \quad = \quad \cdots \quad = [da]_n .$$

□

Lemmas 3.64 and 3.66 imply that each $\mathbb{Z}_n$ acts as a **"clockwork" group**. Why?

- To add $[a]_n$ and $[b]_n$, let $c = a + b$.
- If $c < n$, then you are done. After all, division of $c$ by $n$ gives $q = 0$ and $r = c$.
- Otherwise, $c \geq n$, 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 $15 - 3 = 12$ o’clock.

It should be clear from Examples 2.6 and 2.30 on pages 20 and 27 as well as Exercises 2.19 and 2.37 on pages 22 and 28 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 Exercises 2.20 and 2.38 on pages 23 and 28 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 3.67. Before building the table for $\mathbb{Z}_4$, recall that it is abelian. Use Lemma 3.66 on the preceding page to observe that

$$\begin{aligned}
[1] + [3] &= [0]\\
[2] + [2] &= [0]\\
[2] + [3] &= [1]\\
[3] + [1] &= [0]\\
[3] + [2] &= [1]\\
[3] + [3] &= [2].
\end{aligned}$$

The addition table is thus

| $+$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
|---|---|---|---|---|
| $[0]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| $[1]$ | $[1]$ | $[2]$ | $[3]$ | $[0]$ |
| $[2]$ | $[2]$ | $[3]$ | $[0]$ | $[1]$ |
| $[3]$ | $[3]$ | $[0]$ | $[1]$ | $[2]$ |

In the Klein 4-group, every element is its own inverse. That is *not* the case here, so it must be the cyclic group of order four, and in fact

$$\begin{aligned}
\langle [1] \rangle &= \{[1], [2], [3], [0]\} = \mathbb{Z}_4\\
\langle [3] \rangle &= \{[3], [2], [1], [0]\} = \mathbb{Z}_4.
\end{aligned}$$

Not every non-zero element generates $\mathbb{Z}_4$, however, since

$$\langle [2] \rangle = \{[2], [0]\}. \diamondsuit$$

The fact that $\mathbb{Z}_4$ was cyclic makes one wonder: is $\mathbb{Z}_n$ always cyclic? Yes!

THEOREM 3.68. *$\mathbb{Z}_n$ is cyclic for every $n \in \mathbb{Z}$.*

PROOF. Let $n \in \mathbb{Z}$. We claim that $\mathbb{Z}_n = \langle [1] \rangle$. *Why?* Let $x \in \mathbb{Z}_n$. Looking at Definition 2.49 on page 31, we need to show that $x = m[1]$ for some $m \in \mathbb{Z}$.

By Theorem 3.63, we can write $x = [r]$ for some $0 \leq r < n$. We proceed by induction on $r$.

*Inductive base:* If $r = 0$, then $x = [0] = 0 \cdot [1]$, so $x \in \langle [1] \rangle$.

*Inductive hypothesis:* Assume that for every $i = 0, 1, 2, \ldots, r - 1$ we know that if $x = [i]$ then $x = i[1] \in \langle [1] \rangle$.

*Inductive step:* Since $r < n$, it follows from Lemma 3.66 that

$$[r] = [r-1] + [1] = (r-1)[1] + [1] = r[1] \in \langle [1] \rangle .$$

By induction, $x = [r] \in \langle [1] \rangle$. □

We saw in Example 3.67 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 3.69. *Let $a, b, n \in \mathbb{Z}$ and assume that $n > 1$. 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 3.74. □

EXERCISES.

EXERCISE 3.70. As discussed in the text, 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 3.71. Write down the addition table for $\mathbb{Z}_5$. Which elements generate $\mathbb{Z}_5$?

EXERCISE 3.72. Write down the addition table for $\mathbb{Z}_6$. Which elements generate $\mathbb{Z}_6$?

EXERCISE 3.73. Compare the results of Example 3.67 and Exercises 3.70, 3.71, and 3.72. Formulate a conjecture as to which elements generate $\mathbb{Z}_n$. Do not try to prove your example.

EXERCISE 3.74. Prove Lemma 3.69. *Hint:* Use Lemma 3.27.

CHAPTER 4

# Isomorphisms

We have on occasion observed that different groups have the same addition or multiplication 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.

Group theorists describe such a relationship between two groups as *isomorphic*. We aren't ready to give a precise definition of the term, but we can provide an intuitive definition:

If two groups $G$ and $H$ have identical group structure,

we say that $G$ and $H$ are **isomorphic**.

To define isomorphism precisely, we need to reconsider another topic that you studied in the past, functions. 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 get an isomorphism from a *homomorphism* (a somewhat more general notion of an isomorphism) and its *kernel* (a subgroup with a special relationship to the homomorphism). Section 4.4 introduces a special kind of isomorphism, the *automorphism*, and groups of automorphisms.

## 4.1. FROM FUNCTIONS TO ISOMORPHISMS

Let $G$ and $H$ be groups. A mapping $f : G \to H$ is a **function** if for every input $x \in G$ the output $f(x)$ has precisely one value. 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 $\mathbb{Z}$, $\mathrm{GL}_m(\mathbb{R})$, etc. to groups. To the contrary; we will *specialize* the notion of a function in a way that tells us important information about the group.

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

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

Substituting $z$ for $xy$ suggests that we want the property

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

DEFINITION 4.1. Let $G,H$ be groups and $f : G \to H$ a function. We say that $f$ is a **group homomorphism**[1] from $G$ to $H$ if it satisfies the property that $f(x) f(y) = f(xy)$ for every $x,y \in G$. $\diamond$

NOTATION. 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

- $f(xy) = f(x) + f(y)$;
- $f(x+y) = f(x) f(y)$;
- $f(x \circ y) = f(x) \odot f(y)$;
- etc.

EXAMPLE 4.2. 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

$$\iota(gh) = gh = \iota(g)\iota(g).$$

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

$$f(x) + f(y) = 4x + 4y = 4(x+y) = f(x+y). \diamond$$

The homomorphism property should remind you of certain special functions and operations that you have studied in Linear Algebra or Calculus. Recall from Exercise 2.33 that $\mathbb{R}^+$, the set of all positive real numbers, is a multiplicative group.

EXAMPLE 4.3. Let $f : (\mathrm{GL}_m(\mathbb{R}), \times) \to (\mathbb{R}^+, \times)$ 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. $\diamond$

Let's look at a clockwork group that we studied in the previous section.

EXAMPLE 4.4. Let $n \in \mathbb{Z}$ such that $n > 1$, and let $f : (\mathbb{Z},+) \to (\mathbb{Z}_n,+)$ by the assignment $f(x) = [r]_n$ where $r$ is the remainder of the division of $x$ by $n$. We claim that $f$ is a homomorphism.

*Why?* Before giving a detailed, general explanation, let's look at an example. Suppose $n = 6$; then $f(-3) = [3]_6$ and $f(22) = [4]_6$. The operation in both the domain and the range is *addition*, so if $f$ is a homomorphism, then we should observe the homomorphism property. In the context of these *additive* sets, that property has the form $f(-3+22) = f(-3) + f(22)$. In fact,

$$\begin{aligned} f(-3+22) &= f(19) = [1] \\ f(-3) + f(22) &= [3] + [4] = (3+6\mathbb{Z}) + (4+6\mathbb{Z}) = 7+6\mathbb{Z} = 1+6\mathbb{Z} = [1]. \end{aligned}$$

This doesn't prove that $f$ is a homomorphism, but it does give a good sign. It also gives us a hint at the general case: we will have to argue that congruence classes such as [7] and [1] are equal.

In general, let $x,y \in \mathbb{Z}$. Write $[a] = f(x)$, $[b] = f(y)$, and $[c] = f(x+y)$. By definition of $a$, $b$, and $c$, there exist $q_x, q_y, q_{x+y} \in \mathbb{Z}$ such that $x = q_x n + a$, $y = q_y n + b$, $x + y = q_{x+y} n + c$,

[1]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.

and $0 \le a, b, c < n$. We need to show that $f(x+y) = f(x) + f(y)$, or in other words, $[c] = [a] + [b]$.

Let $[r] \in \mathbb{Z}_n$ such that $[a] + [b] = [r]$. In coset notation, $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = r + n\mathbb{Z}$. By definition of the quotient group, $(a+b) + n\mathbb{Z} = r + n\mathbb{Z}$. By Lemma 3.69 on page 59, $(a+b) - r \in n\mathbb{Z}$. By definition of $n\mathbb{Z}$, $n$ divides $(a+b) - r$. Let $d \in \mathbb{Z}$ such that $nd = (a+b) - r$.

We need to show that $f(x+y) = [c] = [r]$. That is, we need to show that two cosets are equal. We will try to apply Lemma 3.69, using the facts that $nd = (a+b) - r$, $x = q_x n + a$, $y = q_y n + b$, and $x + y = q_{x+y} n + c$. Observe that

$$\begin{aligned} nd &= (a+b) - r \\ &= \left((x - q_x n) + \left(y - q_y n\right)\right) - r \\ &= ((x+y) - r) - \left(q_x + q_y\right) n. \end{aligned}$$

Thus

$$n\left(d + q_x + q_y\right) = (x+y) - r.$$

By substitution,

$$\begin{aligned} n\left(d + q_x + q_y\right) &= \left(q_{x+y} n + c\right) - r \\ n\left(d + q_x + q_y - q_{x+y}\right) &= c - r. \end{aligned}$$

In other words, $n \mid (c - r)$. By Lemma 3.69, $[c] = [r]$. By substitution, $f(x+y) = [r] = f(x) + f(y)$. We conclude that $f$ is a homomorphism. ◇

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** $G$,

$$f(G) = \left\{h \in H : \exists g \in G \text{ such that } f(g) = h\right\}$$

act the same way as their preimages in $G$.

This does *not* imply that the *group structure* is the same. In Example 4.4, 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.

DEFINITION 4.5. Let $f : G \to H$ be a homomorphism of groups. If $f$ is one-to-one and onto, then $f$ is an **isomorphism**[2] and the groups $G$ and $H$ are **isomorphic**.[3] ◇

NOTATION. If the groups $G$ and $H$ are isomorphic, we write $G \cong H$.

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, along with two examples.

[2]The word comes Greek words that mean *identical shape*.

[3]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.

DEFINITION 4.6. 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 $S$.

EXAMPLE 4.7. Recall the homomorphisms of Example 4.2,

$$\iota : G \to G \quad \text{by} \quad \iota(g) = g \qquad \text{and} \qquad f : \mathbb{Z} \to 2\mathbb{Z} \quad \text{by} \quad f(x) = 4x.$$

First we show that $\iota$ 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 $\iota$, $g = h$. Since $g$ and $h$ were arbitrary in $G$, $\iota$ 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 $\iota$, $x = g$ does the job. Since $g$ was arbitrary in $G$, $\iota$ 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 4.8. Recall the homomorphism of Example 4.3,

$$f : \mathrm{GL}_m(\mathbb{R}) \to \mathbb{R}^+ \quad \text{by} \quad f(A) = |\det A|.$$

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 $0$, even though the matrices are unequal:

$$A = 0 = \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 0 & \\ & & & \ddots \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots \end{pmatrix}.$$

(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 $\mathbb{Z} \not\cong 2\mathbb{Z}$ and that $\mathbb{R}^+ \not\cong \mathbb{R}^{m \times n}$. *Why not?* In each case, we were considering only one of (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 4.9. *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* $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

Theorem 4.9 applies of course to isomorphisms as well. It should not surprise you that, if the operation's behavior is preserved, the identity is mapped to the identity, and inverses are mapped to inverses.

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 $f(x^{-1})$ is the identity, those two elements must be inverses! Hence $f(x^{-1})$ is the inverse of $f(x)$, which we write as

$$f\left(x^{-1}\right) = f(x)^{-1}.$$

□

COROLLARY 4.10. *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 4.18. □

The following theorem is similar to the previous one, but has a different proof.

THEOREM 4.11. *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 4.20. □

COROLLARY 4.12. *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 $n \in \mathbb{N}^+$ 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 4.11, $y = f(x) = f(g^n) = f(g)^n$. 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 4.11, $y = f(g^n)$. 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 conclude by showing that the isomorphism relations satisfies three important, and useful properties.

THEOREM 4.13. *The 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 $\iota$ be the identity homomorphism from Example 4.2. We showed in Example 4.7 that $\iota$ 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 4.19, $f^{-1}$ 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 $G \cong K$. 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 $G \cong K$. □

EXERCISES.

EXERCISE 4.14.
(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 $n$. *Hint:* Generalize the isomorphism of (a).

EXERCISE 4.15. Show that $\mathbb{Z}_2$ is isomorphic to the group of order two from Example 2.30 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 4.16. Show that $\mathbb{Z}_2$ is isomorphic to the Boolean xor group of Exercise 2.14 on page 22. *Caution!* Remember to denote the operation in the Boolean xor group correctly.

EXERCISE 4.17. Recall the subgroup $L$ of $\mathbb{R}^2$ from Exercises 3.13 on page 45, 3.30 on page 49, and 3.55 on page 55. Show that $L \cong \mathbb{R}$. *Hint:* For a homomorphism function, think about the equation that describes the points on $L$.

EXERCISE 4.18. Prove Corollary 4.10. *Hint:* Since it's a corollary to Theorem 4.9, you should use that theorem.

EXERCISE 4.19. 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 4.20. Prove Theorem 4.11. *Hint:* Use induction on the positive powers of $g$; use a theorem for the nonpositive powers of $g$.

EXERCISE 4.21. 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. *Hint:* Let $G = \mathbb{Z}_2$ and $H = D_3$; find a homomorphism from $G$ to $H$.

EXERCISE 4.22. Let $f : G \to H$ be a homomorphism of groups. Let $A < G$. Show that $f(A) < H$. *Hint:* Recall that

$$f(A) = \{y \in H : f(x) = y \ \exists x \in A\},$$

and use the Subgroup Theorem.

EXERCISE 4.23. 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. *Hint:* See the last part of Exercise 4.21.

## 4.2. CONSEQUENCES OF ISOMORPHISM

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

- $G$ 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 very well correspond to two different subgroups $B$ and $B'$ of $H$.

THEOREM 4.24. *Suppose that $G \cong H$ as groups. 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 4.21, $f(G)$ is abelian. Since $f$ is an isomorphism, and therefore onto, $f(G) = H$. Hence $H$ is abelian.

A similar argument shows that if $H$ is abelian, so is $G$. Hence $G$ is abelian iff $H$ is. □

THEOREM 4.25. *Suppose $G \cong H$ as groups. 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 4.11,

$$x = f(a) = f(g^n) = f(g)^n = h^n.$$

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.

A similar proof shows that if $H$ is cyclic, then so is $G$. □

THEOREM 4.26. *Suppose $G \cong H$ as groups. Every subgroup $A$ of $G$ is isomorphic to a subgroup $B$ of $H$. This correspondence is unique up to isomorphism. 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 4.22, $f(A) < H$.

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 $A \cong f(A)$. Uniqueness follows from the fact that $f$ is one-to-one.

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 $B \triangleleft H$.

A similar argument shows that if $B \triangleleft H$, then its preimage $A = f^{-1}(B)$ is normal in $G$, as claimed. □

THEOREM 4.27. *Suppose $G \cong H$ as groups. Every quotient group of $G$ is isomorphic to a quotient group of $H$.*

We use Lemma 3.27(CE3) on page 48 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. Let $X$ be a quotient group of $G$ defined by $G/A$, where $A \triangleleft G$. Let $A' = f(A)$; by Theorem 4.26 $A' \triangleleft H$, so $H/A'$ is a quotient group. We want to show that $G/A \cong H/A'$.

Let $f_A : G/A \to H/A'$ by

$$f_A(X) = f(g)A' \qquad \text{where} \qquad gA = X \in G/A.$$

We claim that $f_A$ is a well-defined homomorphism, and is one-to-one and onto.

*That $f_A$ is well-defined:* Let $X \in G/A$ and consider two representations $g_1A$ and $g_2A$ of $X$. Then

$$f_A(g_1A) = f(g_1)A' \quad \text{and} \quad f_A(g_2A) = f(g_2)A'.$$

We must show that the cosets $f_A(g_1)A'$ and $f_A(g_2)A'$ are equal in $H/A'$. By hypothesis, $g_1A = g_2A$. Lemma 3.27(CE3) implies that $g_2^{-1}g_1 \in A$. Recall that $f(A) = A'$; this implies that $f\left(g_2^{-1}g_1\right) \in A'$. The homomorphism property implies that

$$f(g_2)^{-1} f(g_1) = f\left(g_2^{-1}\right) f(g_1) = f\left(g_2^{-1}g_1\right) \in A'.$$

Lemma 3.27(CE3) again implies that $f(g_1)A' = f(g_2)A'$. In other words,

$$f_A(X) = f(g_1)A' = f(g_2)A'$$

so there is no ambiguity in the definition of $f_A$ as to the image of $X$ in $H/A'$; 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

$$\begin{aligned} f_A(XY) &= f_A((g_1A)\cdot(g_2A)) \\ &= f_A(g_1g_2 \cdot A) \\ &= f(g_1g_2)A' \\ &= (f(g_1)f(g_2))\cdot A' \\ &= f(g_1)A' \cdot f(g_2)A' \\ &= f_A(g_1A)\cdot f_A(g_2A) \\ &= f_A(X)\cdot f_A(Y) \end{aligned}$$

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 $H/A'$; 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 $X = g_1 A$ and $Y = g_2 A$. The definition of $f_A$ implies that

$$f(g_1) A' = f_A(X) = f_A(Y) = f(g_2) A',$$

so by Lemma 3.27(CE3) $f(g_2)^{-1} f(g_1) \in A'$. Recall that $A' = f(A)$, 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 3.27(CE3) again gives us $g_1 A = g_2 A$, and

$$X = g_1 A = g_2 A = Y.$$

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 4.28. □

EXERCISES.

EXERCISE 4.28. Show that the function $f_A$ defined in the proof of Theorem 4.27 is onto. *Hint:* It's quite a bit easier than the proof that $f_A$ is one-to-one.

EXERCISE 4.29. Recall from Exercise 2.55 on page 34 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 4.27 to determine the quotient group of $\mathbb{Z}_4$ to which $\langle \mathbf{i} \rangle / A$ is isomorphic.

EXERCISE 4.30. Recall from Exercise 4.17 on page 66 that the set

$$L = \left\{ x \in \mathbb{R}^2 : x = (a, a) \ \exists a \in \mathbb{R} \right\}$$

defined in Exercise 3.13 on page 45 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 $A$ of $L$ that corresponds to $\mathbb{Z} < \mathbb{R}$. What do this section's theorems imply that you can conclude about $A$ and $L/A$?
(e) Use the answer to (c) to describe $L/A$ intuitively. Choose an element of $L/A$ 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 4.31. Recall $A_3 = \{\iota, \rho, \rho^2\} \triangleleft D_3$ from Example 3.49. 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 $\mu$ 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 operation 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 $\mu$ is a homomorphism. The property of isomorphism follows from the facts that

- $\mu(A_3) \neq \mu(\varphi A_3)$, so $\mu$ is one-to-one, and
- both 0 and 1 have preimages, so $\mu$ is onto.

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 $\iota$, $\rho$, and $\rho^2$; $f$ 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* 2. $x \in A_3$ 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* 3. $x \notin A_3$ and $y \in A_3$.
An argument similar to the case above shows that $f(xy) = f(x) + f(y)$.

*Case* 4. $x, y \notin A_3$.
Inspection of the operation table of $D_3$ (Exercise 2.68 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 $\mathbb{Z}_2$.

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

$$\mu \circ \eta = f. \diamond$$

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 4.32. *Let $G$ be a group and $A \triangleleft G$. The function $\eta : G \to A$ by*

$$\eta(g) = gA$$

*is a homomorphism.*

PROOF. You do it! See Exercise 4.36. □

DEFINITION 4.33. We call the homomorphism $\eta$ of Lemma 4.32 the **natural homomorphism**.

We need another definition, related to something you should have seen in linear algebra. It will prove important in subsequent sections and chapters.

DEFINITION 4.34. 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 $\ker f$.

We now formalize the observation of Example 4.31.

THEOREM 4.35 (The Isomorphism Theorem). *Let $G$ and $H$ be groups, and $A \triangleleft G$. Let $\eta : G \to A$ 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 4.35 by the following diagram:

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\eta"'] & & H \\ & G/A \arrow[ur, "\mu"'] & \end{tikzcd}$$

The idea is that "the diagram commutes", or $f = \mu \circ \eta$.

PROOF. We are given $G, H, A$, and $\eta$. 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:

$$\mu(x) = \begin{cases} e_H, & x = A; \\ f(g), & x = gA \quad \exists g \notin A. \end{cases}$$

We claim that $\mu$ is an isomorphism from $G/A$ to $H$, and moreover that $f = \mu \circ \eta$.

Since the domain of $\mu$ consists of cosets which may have different representations, we must show first that $\mu$ is well-defined. Suppose that $X \in G/A$ has two different 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 3.27(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 $\mu$ 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

$$\mu(g'A) = f(g) \cdot e_H = f(g) = \mu(gA).$$

Hence $\mu(g'A) = \mu(gA)$ and $\mu(X)$ is well-defined.

Is $\mu$ 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

$$\mu(XY) = \mu((gA)(g'A)) = \mu((gg')A) = f(gg') = f(g)f(g') = \mu(gA)\mu(g'A).$$

Thus $\mu$ is a homomorphism.

Is $\mu$ 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

$$\begin{aligned} f\left(g^{-1}g'\right) &= f\left(g^{-1}\right)f(g') \\ &= f(g)^{-1}f(g') \\ &= \mu(gA)^{-1}\mu(g'A) \\ &= \mu(X)^{-1}\mu(Y) \\ &= \mu(Y)^{-1}\mu(Y) \\ &= e_H, \end{aligned}$$

so $g^{-1}g' \in \ker f$. It is given that $\ker f = A$, so $g^{-1}g' \in A$. Lemma 3.27(CE3) now tells us that $gA = g'A$, so $X = Y$. Thus $\mu$ is one-to-one.

Is $\mu$ 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 $\mu$ is onto.

We have shown that $\mu$ is an isomorphism; we still have to show that $f = \mu \circ \eta$, but the definition of $\mu$ makes this trivial: for any $g \in G$,

$$(\mu \circ \eta)(g) = \mu(\eta(g)) = \mu(gA) = f(g).$$

□

EXERCISES.

EXERCISE 4.36. Prove Lemma 4.32.

EXERCISE 4.37. Recall the normal subgroup $L$ of $\mathbb{R}^2$ from Exercises 3.13, 3.30, and 3.55 on pages 45, 49, and 55, respectively. In Exercise 4.17 on page 66 you found an explicit isomorphism $L \cong \mathbb{R}$.

(a) Use the Isomorphism Theorem to find an isomorphism $\mathbb{R}^2/L \cong \mathbb{R}$. *Hint:* Consider $f : \mathbb{R}^2 \to \mathbb{R}$ by $f(a) = b$ where the point $a = (a_1, a_2)$ lies on the line $y = x + b$.
(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 4.38. Recall the normal subgroup $\langle -\mathbf{1} \rangle$ of $Q_8$ from Exercises 2.47 on page 31 and 3.53 on page 55.

(a) Use Lagrange's Theorem to explain why $Q_8/\langle -\mathbf{1} \rangle$ has order 4.
(b) We know from Exercise 2.20 on page 23 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 $Q_8/\langle -\mathbf{1} \rangle$. *Hint:* You already know the answer from Exercise 3.53 on page 55; find a homomorphism $f$ from $Q_8$ to that group such that $\ker f = \langle -\mathbf{1} \rangle$.

## 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 4.39. Let $G$ be a group. If $f : G \to G$ is an isomorphism, then we call $f$ an **automorphism**.[4]

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 4.40.

(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 $\iota(g \cdot g') = g \cdot g' = \iota(g) \cdot \iota(g')$;

[4]The word comes Greek words that mean *self* and *shape*.

- 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 $\rho$ and on the right by $\rho^2$ 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 4.40(c) generalizes to an important automorphism.

Recall now the conjugation of one element of a group by another, introduced in Exercise 2.48 on page 31. By fixing the second element, we can turn this into a function on a group.

DEFINITION 4.41. Let $G$ be a group and $a \in G$. Define the function of **conjugation by** $a$ to be $\mathrm{conj}_a(x) = a^{-1}xa$. ◇

Conjugation by $a$ should look very similar to something you would have found useful in Exercise 3.61 on page 55.

In Example 4.40(c), we had $a = \rho$ and $\mathrm{conj}_a(x) = a^{-1}xa = \rho^2 x \rho$.

LEMMA 4.42. *Let $G$ be a group, and $a \in G$. Then $\mathrm{conj}_a$ is an automorphism. Moreover,*

$$\{\mathrm{conj}_a(g) : g \in G\} < G.$$

PROOF. You do it! See Exercise 4.50. □

The subgroup $\{\mathrm{conj}_a(g) : g \in G\}$ is important enough to identify by a special name.

DEFINITION 4.43. We say that $\{\mathrm{conj}_a(g) : g \in G\}$ is the **group of conjugations of** $G$ **by** $a$, and denote it by $\mathrm{Conj}_a(G)$. ◇

Conjugation of subgroups is *not* necessarily an automorphism; it is quite possible that for some $H < G$ and for some $a \in G \backslash H$ we do *not* have $H = \{\mathrm{conj}_a(h) : h \in H\}$. (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 $H = \{\mathrm{conj}_a(h) : h \in H\}$. You will explore this in the exercises.

Now it is time to identify the new group that we promised at the beginning of the chapter.

NOTATION. Write $\mathrm{Aut}(G)$ for the set of all automorphisms of $G$. In addition, we typically denote automorphisms by Greek letters, rather than Latin letters.

EXAMPLE 4.44. We compute $\mathrm{Aut}(\mathbb{Z}_4)$. Let $\alpha \in \mathrm{Aut}(\mathbb{Z}_4)$ be arbitrary; what do we know about $\alpha$? By definition, its range is $\mathbb{Z}_4$, and by Theorem 4.9 on page 64 we know that $\alpha(0) = 0$. Aside from that, we consider all the possibilities that preserve the isomorphism properties.

Recall from Theorem 3.68 on page 58 that $\mathbb{Z}_4$ is a cyclic group; in fact $\mathbb{Z}_4 = \langle 1 \rangle$. Corollary 4.12 on page 64 tells us that $\alpha(1)$ will tell us everything we want to know about $\alpha$. 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 $\alpha$ is the identity homomorphism $\iota$, 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 $\alpha$ is not one-to-one: by Theorem 4.9 on page 64, $\alpha(0) = 0 = \alpha(2)$! So we *cannot* have $\alpha(1) = 2$.

*Case* 4. Can we have $\alpha(1) = 3$? If so, then the homomorphism property implies that

$$\alpha(2) = \alpha(1+1) = \alpha(1) + \alpha(1) = 3 + 3 = 6 = 2; \text{ and}$$
$$\alpha(3) = \alpha(2+1) = \alpha(2) + \alpha(1) = 2 + 3 = 5 = 1.$$

In this case, $\alpha$ is both one-to-one *and* onto. We were careful to observe the homomorphism property when determining $\alpha$, so we know that $\alpha$ is a homomorphism. So we *can* have $\alpha(1) = 2$.

We found only two possible elements of $\operatorname{Aut}(\mathbb{Z}_4)$: the identity automorphism and the automorphism determined by $\alpha(1) = 3$. ◇

It turns out that $\operatorname{Aut}(G)$ is itself a group!

LEMMA 4.45. *For any group $G$,* $\operatorname{Aut}(G)$ *is a group under the operation of composition of functions.*

PROOF. Let $G$ be any group. We show that $\operatorname{Aut}(G)$ satisfies each of the group properties from Definition 2.39.

(G1) Let $\alpha, \theta \in \operatorname{Aut}(G)$. We must show that $\alpha \circ \theta \in \operatorname{Aut}(G)$ as well:
- the domain and range of $\alpha \circ \theta$ are both $G$ because the domain and range of both $\alpha$ and $\theta$ 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 $\alpha$ and $\theta$ to obtain

$$\begin{aligned}(\alpha \circ \theta)(g \cdot g') &= \alpha(\theta(g \cdot g')) \\ &= \alpha(\theta(g) \cdot \theta(g')) \\ &= \alpha(\theta(g)) \cdot \alpha(\theta(g')) \\ &= (\alpha \circ \theta)(g) \cdot (\alpha \circ \theta)(g');\end{aligned}$$

- $\alpha \circ \theta$ is *one-to-one* because $(\alpha \circ \theta)(g) = (\alpha \circ \theta)(g')$ implies $\alpha(\theta(g)) = \alpha(\theta(g'))$; since $\alpha$ is one-to-one we infer that $\theta(g) = \theta(g')$; since $\theta$ is one-to-one we conclude that $g = g'$; and
- $\alpha \circ \theta$ is *onto* because for any $z \in G$,
  - $\alpha$ is onto, so there exists $y \in G$ such that $\alpha(y) = z$, and
  - $\theta$ is onto, so there exists $x \in G$ such that $\theta(x) = y$, so
  - $(\alpha \circ \theta)(x) = \alpha(\theta(x)) = \alpha(y) = z$.

We have shown that $\alpha \circ \theta$ satisfies the properties of an automorphism; hence, $\alpha \circ \theta \in \operatorname{Aut}(G)$, and $\operatorname{Aut}(G)$ is closed under the composition of functions.

(G2) The associative property is sastisfied because the operation is composition of functions, which is associative.

(G3) Denote by $\iota$ the identity homomorphism; that is, $\iota(g) = g$ for all $g \in G$. We showed in Example 4.40(a) that $\iota$ is an automorphism, so $\iota \in \operatorname{Aut}(G)$. Let $f \in \operatorname{Aut}(G)$; 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 $\iota \circ f = f \circ \iota = f$.

(G2) Let $\alpha \in \operatorname{Aut}(G)$. Since $\alpha$ is an automorphism, it is an isomorphism. You showed in Exercise 4.19 that $\alpha^{-1}$ is also an isomorphism. The domain and range of $\alpha$ are both $G$, so the domain and range of $\alpha^{-1}$ are also both $G$. Hence $\alpha^{-1} \in \operatorname{Aut}(G)$.

□

Since $\operatorname{Aut}(G)$ is a group, we can compute $\operatorname{Aut}(\operatorname{Aut}(G))$. For finite groups, $|\operatorname{Aut}(G)| < |G|$ (we do not prove this here) so any chain of automorphism groups must eventually stop. In the exercises you will compute $\operatorname{Aut}(G)$ for some other groups.

EXAMPLE 4.46. Recall from Example 4.44 on page 74 that $\operatorname{Aut}(\mathbb{Z}_4)$ has only two elements. We saw early on that there is only one group of two elements, so $\operatorname{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$. ◇

EXERCISES.

EXERCISE 4.47. Show that $f(x) = x^2$ is an automorphism on the group $(\mathbb{R}^+, \times)$.

EXERCISE 4.48.

(a) List the elements of $\operatorname{Conj}_\rho(D_3)$.

(b) List the elements of $\operatorname{Conj}_\varphi(D_3)$.

(c) Will $\operatorname{Conj}_a(G)$ always be a *normal* subgroup of $G$?

EXERCISE 4.49. List the elements of $\operatorname{Conj}_{\mathbf{i}}(Q_8)$.

EXERCISE 4.50. Prove Lemma 4.42 on page 74 in two parts:

(a) Show first that $\operatorname{conj}_g$ is an automorphism.

(b) Show that $\left\{\operatorname{conj}_a(g) : g \in G\right\}$ is a group.

*Hint:* Use some of the ideas from Example 4.40 on page 73(c).

EXERCISE 4.51. Determine the automorphism group of the Klein 4-group.

EXERCISE 4.52. Determine the automorphism group of $D_3$. *Hint:* We can think of $D_3$ as generated by the elements $\rho$ and $\varphi$, and each of these generates a non-trivial cyclic subgroup. Any automorphism $\alpha$ is therefore determined by these generators, so you can find all automorphisms $\alpha$ by finding all possible results for $\alpha(\rho)$ and $\alpha(\varphi)$, then examining that carefully.

EXERCISE 4.53. Let $G$ be a group, $g \in G$, and $H < G$. Write $g^{-1}Hg = \left\{\operatorname{conj}_g(h) : h \in H\right\}$. Show that $H \triangleleft G$ iff for every $g \in G$ we have $H = g^{-1}Hg$. *Hint:* This problem requires you to show twice that two sets are equal.

CHAPTER 5

# Groups of permutations

This chapter introduces groups of permutations, a fundamental object of study in group theory. Section 5.2 introduces you to groups of permutations, but to get there you must first pass through Section 5.1, which tells you what a permutation is. 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; TABULAR NOTATION; CYCLE NOTATION

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 $\pi$ is one-to-one, and $\pi(i) = j$ is interpreted as "the $j$th element of the permuted list is the $i$th 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, $S$. $\diamondsuit$

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 $\alpha, \beta$ permutations of $V$. Let $\gamma = \alpha \circ \beta$. We claim that $\gamma$ is a permutation. To show this, we must show that $\gamma$ is a one-to-one function whose domain and range are both $V$. From the definition of $\alpha$ and $\beta$, it follows that the domain and range of $\gamma$ are both $V$; it remains to show that $\gamma$ is one-to-one. Let $x, y \in V$ and assume that $\gamma(x) = \gamma(y)$; by definition of $\gamma$,

$$\alpha(\beta(x)) = \alpha(\beta(y)).$$

Because they are permutations, $\alpha$ and $\beta$ are one-to-one functions. One-to-one functions have inverse functions. Applying them to the previous equation, we see that

$$\begin{aligned} \beta^{-1}\left(\alpha^{-1}(\alpha(\beta(x)))\right) &= \beta^{-1}\left(\alpha^{-1}(\alpha(\beta(y)))\right) \\ x &= y. \end{aligned}$$

Hence $\gamma$ is a one-to-one function. We already explained why its domain and range are both $V$, so $\gamma$ is a permutation. $\square$

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. 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 $\alpha(1) = \alpha_1$, $\alpha(2) = \alpha_2$, $\ldots$, $\alpha(n) = \alpha_n$. Again, $\alpha(i) = j$ indicates that the $j$th element of the permuted list is the $i$th element of the original list.

EXAMPLE 5.4. Recall $V$ and $\pi$ from Example 5.2. In tabular notation,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

because $\pi$ 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 $\pi$ looks similar to the table in Example 5.2.

We can also use $\pi$ to permute different lists, so long as the new lists have four elements:

$$\pi(3,2,1,4) = (4,3,1,2);$$
$$\pi(2,4,3,1) = (1,2,3,4);$$
$$\pi(a,b,c,d) = (d,a,c,b). \diamondsuit$$

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 5.5. A **cycle** is a vector

$$\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$$

that corresponds to the permutation where the entry in position $\alpha_1$ is moved to position $\alpha_2$; the entry in position $\alpha_2$ is moved to position $\alpha_3$, ... and the element in position $\alpha_n$ is moved to position $\alpha_1$. If a position is not listed in $\alpha$, 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

$$\iota = (1). \diamondsuit$$

The fact that the permutation $\alpha$ moves the entry in position $\alpha_n$ to position $\alpha_1$ is the reason that this is called a *cycle;* applying it repeatedly cycles the list of elements around, and on the $n$th application the list returns to its original order.

EXAMPLE 5.6. Recall $\pi$ from Example 5.4. 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 $\pi$ moves elements out of position 1, we start with

$$\pi = \begin{pmatrix} 1 & ? \end{pmatrix}.$$

The second entry in cycle notation tells us where $\pi$ moves the element whose position is that of the first entry. The first entry indicates position 1. From the tabular notation, we see that $\pi$ moves the element in position 1 to position 2, so

$$\pi = \begin{pmatrix} 1 & 2 & ? \end{pmatrix}.$$

The third entry of cycle notation tells us where $\pi$ moves the element whose position is that of the second entry. The second entry indicates position 2. From the tabular notation, we see that $\pi$ moves the element in position 2 to position 4, so

$$\pi = \begin{pmatrix} 1 & 2 & 4 & ? \end{pmatrix}.$$

The fourth entry of cycle notation tells us where $\pi$ moves the element whose position is that of the third entry. The third element indicates position 4. From the tabular notation, we see that $\pi$ moves the element in position 4 to position 1, so you might feel the temptation to write

$$\pi = \begin{pmatrix} 1 & 2 & 4 & 1 & ? \end{pmatrix},$$

but there is no need. Since we have now returned to the first element in the cycle, we close it:

$$\pi = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix}.$$

The cycle $\begin{pmatrix} 1 & 2 & 4 \end{pmatrix}$, 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 $\pi$. ◇

Not all permutations can be written as one cycle.

EXAMPLE 5.7. 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 5.8. 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 $\gamma$:

$$\gamma(V) = (4,1,3,2),$$

followed by $\beta$:

$$\beta(\gamma(V)) = (4,2,1,3).$$

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

$$\beta \circ \gamma = (\ 1\ \ 3\ \ 4\ ). \diamond$$

Another phenomenon occurs when each permutation moves elements that the other does not.

EXAMPLE 5.9. 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 $\beta$ operates only on the first and third elements of a list, and $\gamma$ operates only on the second and fourth elements of a list. The only way to write them is as the composition of two cycles,

$$\beta \circ \gamma = (\ 1\ \ 3\ ) \circ (\ 2\ \ 4\ ). \diamond$$

This motivates the following.

DEFINITION 5.10. We say that two cycles are **disjoint** if none of their entries are common.

Disjoint cycles enjoy an important property.

LEMMA 5.11. *Let $\alpha, \beta$ be two disjoint cycles. Then $\alpha \circ \beta = \beta \circ \alpha$.*

PROOF. Let $n \in \mathbb{N}^+$ be the largest entry in $\alpha$ or $\beta$. 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 $\alpha$. Recall that $\alpha$ and $\beta$ are disjoint. Since $i$ and $j$ are entries of $\alpha$, they cannot be entries of $\beta$. 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* 2. $\alpha(i) = i$.

*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 $\beta$. Recall that $\alpha$ and $\beta$ are disjoint. Since $j$ is an entry of $\beta$, it cannot be an entry of $\alpha$. By definition of cycle notation, $\alpha(j) = j$. Hence

$$(\alpha \circ \beta)(i) = \alpha(j) = j = (\beta \circ \alpha)(i).$$

In both cases, we had $(\alpha \circ \beta)(i) = (\beta \circ \alpha)(i)$. Since $i$ was arbitrary, $\alpha \circ \beta = \beta \circ \alpha$. □

NOTATION. 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

$$\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}.$$

By Lemma 5.11, we can also write this as

$$\begin{pmatrix} 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}.$$

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

$$\begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}$$

to either of

$$\begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 3 & 2 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 4 \end{pmatrix}.$$

The convention for writing a permutation in cycle form is the following:

(1) Rotate each cycle so 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 5.11, we know that they commute; write them in order from smallest first entry to largest first entry.

EXAMPLE 5.12. We return to Example 5.7, 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

$$\alpha = \begin{pmatrix} 1 & 2 \end{pmatrix} \ldots ?$$

Since $\alpha$ 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:

$$\alpha = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & ? \end{pmatrix}.$$

Since $\alpha$ moves the element in position 3 to position 4, we write

$$\alpha = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 & ? \end{pmatrix}.$$

Now $\alpha$ moves the element in position 4 to position 3, so we can close the second cycle:

$$\alpha = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}.$$

Now $\alpha$ moves no more entries, so the cycle notation is complete. $\diamondsuit$

We have come to the main result of this section.

THEOREM 5.13. *Every permutation can be written as a composition of cycles.*

The proof is constructive.

PROOF. Let $\pi$ 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 $\pi$ has at most $n$ elements; since $\pi$ is one-to-one, eventually $\pi^k(i_1) = i_1$ for some $k \leq n$. Let $\alpha^{(1)}$ be the cycle $\begin{pmatrix} i_1 & \pi(i_1) & \pi(\pi(i_1)) & \cdots & \pi^k(i_1) \end{pmatrix}$ where $\pi^{k+1}(i_1) = i_1$.

At this point, either every element of $V$ that is not stationary with respect to $\pi$ 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 $\pi$ and $i_2 \notin \alpha^{(1)}$, then generate the cycle $\alpha^{(2)}$ by $\begin{pmatrix} i_2 & \pi(i_2) & \pi(\pi(i_2)) & \cdots & \pi^\ell(i_2) \end{pmatrix}$ where as before $\pi^\ell(i_2) = i_2$.

Repeat this process until every non-stationary element of $V$ corresponds to a cycle, generating $\alpha^{(3)}, \ldots, \alpha^{(m)}$ 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 $\alpha$. 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, $\pi$ is a composition of cycles. Since $\pi$ was arbitrary, every permutation is a composition of cycles. $\square$

EXAMPLE 5.14. 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 5.13, we define the cycles

$$\begin{aligned}\alpha^{(1)} &= (\ 1\ \ 7\ )\\ \alpha^{(2)} &= (\ 2\ \ 5\ \ 4\ )\\ \alpha^{(3)} &= (\ 6\ \ 8\ ).\end{aligned}$$

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 $\alpha$ is 3, because $\pi(3) = 3$. Inspection verifies that

$$\pi = \alpha^{(1)}\alpha^{(2)}\alpha^{(3)}. \diamondsuit$$

We conclude with some examples of simplifying the composition of permutations.

EXAMPLE 5.15. 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, $\alpha$ and $\beta$ are not disjoint.

(1) We compute the cycle notation for $\gamma = \alpha \circ \beta$. We start with the smallest entry moved by either $\alpha$ or $\beta$:

$$\gamma = (\ 1\ \ ?\ ).$$

The notation $\alpha \circ \beta$ means to apply $\beta$ first, *then* $\alpha$. What does $\beta$ do with the entry in position 1? It moves it to position 3. Subsequently, $\alpha$ moves the entry in position 3 back to the entry in position 1. The next entry in the first cycle of $\gamma$ 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 $\alpha$ and $\beta$ also move other entries around. The next smallest entry moved by either $\alpha$ or $\beta$ is 2, so

$$\gamma = (\ 1\ )(\ 2\ \ ?\ ).$$

Now $\beta$ moves the entry in position 2 to the entry in position 4, and $\alpha$ moves the entry in position 4 to the entry in position 2. The next entry in the second cycle of $\gamma$ 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, $\beta$ moves the entry in position 3, so

$$\gamma = (\ 1\ )(\ 2\ )(\ 3\ \ ?\ ).$$

Where does $\beta$ move the entry in position 3? To the entry in position 2. Subsequently, $\alpha$ 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: $\beta$ moves the entry in position 4 to the entry in position 1, and $\alpha$ 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 $\gamma$ 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 $\alpha$ moves to 3, and $\beta$ then moves to 2. So we start with

$$\beta \circ \alpha = (\ 1\ \ 2\ \ ?\ ).$$

Next, $\alpha$ moves 2 to 4, and $\beta$ moves 4 to 1. This closes the first cycle:

$$\beta \circ \alpha = (\ 1\ \ 2\ )\ldots?$$

We start the next cycle with position 3: $\alpha$ moves it to position 1, which $\beta$ 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 $\gamma$ moves to 4, and then $\beta$ 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: $\gamma$ doesn't move it, and $\beta$ moves 2 to 4. We start with

$$\beta \circ \gamma = (\ 2\ \ 4\ \ ?\ ).$$

Next, $\gamma$ moves 4 to 1, and $\beta$ 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: $\gamma$ doesn't move it, and $\beta$ moves 3 to 2. The cycle is now complete:

$$\beta\circ\gamma=\left(\begin{array}{ccc}2&4&3\end{array}\right).\diamondsuit$$

EXERCISES.

EXERCISE 5.16. For the permutation

$$\alpha=\left(\begin{array}{cccccc}1&2&3&4&5&6\\1&5&2&4&6&3\end{array}\right),$$

(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 $\alpha$ in cycle notation.
(e) Write $\alpha$ as a piecewise function.

EXERCISE 5.17. For the permutation

$$\alpha=\left(\begin{array}{cccc}1&3&4&2\end{array}\right),$$

(a) Evaluate $\alpha(1,2,3,4)$.
(b) Evaluate $\alpha(1,4,3,2)$.
(c) Evaluate $\alpha(3,1,4,2)$.
(d) Write $\alpha$ in tabular notation.
(e) Write $\alpha$ as a piecewise function.

EXERCISE 5.18. Let $\alpha=\left(\begin{array}{cccc}1&2&3&4\end{array}\right)$, $\beta=\left(\begin{array}{cccc}1&4&3&2\end{array}\right)$, and $\gamma=\left(\begin{array}{cc}1&3\end{array}\right)$. Compute $\alpha\circ\beta$, $\alpha\circ\gamma$, $\beta\circ\gamma$, $\beta\circ\alpha$, $\gamma\circ\alpha$, $\gamma\circ\beta$, $\alpha^2$, $\beta^2$, and $\gamma^2$. (Here $\alpha^2=\alpha\circ\alpha$.) What are the inverses of $\alpha$, $\beta$, and $\gamma$?

EXERCISE 5.19. For

$$\alpha=\left(\begin{array}{cccc}1&2&3&4\\3&1&4&2\end{array}\right)$$

compute $\alpha^2$, $\alpha^3$, $\ldots$ until you reach the identity permutation. *Hint:* Life will probably be easier if you convert it to cycle notation first.

## 5.2. GROUPS OF PERMUTATIONS

In Section 5.1 we introduced permutations. For $n\geq 2$, denote by $S_n$ the set of all permutations of a list of $n$ elements. In this section we show that $S_n$ is a group for all $n\geq 2$.

EXAMPLE 5.20. For $n=2,3$ we have

$$S_2=\{(1),\left(\begin{array}{cc}1&2\end{array}\right)\}$$
$$S_3=\{(1),\left(\begin{array}{cc}1&2\end{array}\right),\left(\begin{array}{cc}1&3\end{array}\right),\left(\begin{array}{cc}2&3\end{array}\right),\left(\begin{array}{ccc}1&2&3\end{array}\right),\left(\begin{array}{ccc}1&3&2\end{array}\right)\}.\diamondsuit$$

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 in Section 5.1 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 5.21. *For all $n \geq 2$ $(S_n, \circ)$ is a group.*

NOTATION. 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 (G1)–(G4) under the operation of composition of functions:

(G1): For closure, we must show that the composition of two permutations is a permutation. This is precisely Lemma 5.3 on page 78.

(G2): The associative property follows from the fact that permutations are functions, and functions are associative.

(G3): The identity function $\iota$ 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 $\alpha \circ \iota = \alpha$.

(G4): Every one-to-one function has an inverse function, so every element of $S_n$ has an inverse element under composition.

□

EXERCISES.

EXERCISE 5.22. Show that all the elements of $S_3$ can be written as compositions of of the cycles $\alpha = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ and $\beta = \begin{pmatrix} 2 & 3 \end{pmatrix}$.

EXERCISE 5.23. For $\alpha$ and $\beta$ as defined in Exercise 5.22, 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 5.24. Write the operation table for $S_3$. *Hint:* List the six elements of $S_3$ as $\begin{pmatrix} 1 \end{pmatrix}$, $\alpha$, $\alpha^2$, $\beta$, $\alpha\beta$, $\alpha^2\beta$, using the previous exercises both to justify and to simplify this task.

EXERCISE 5.25. 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 5.26. How many elements are there of $S_4$? List them all using cycle notation.

EXERCISE 5.27. Compute the cyclic subgroup of $S_4$ generated by $\alpha = \begin{pmatrix} 1 & 3 & 4 & 2 \end{pmatrix}$. Compare your answer to that of Exercise 5.19.

EXERCISE 5.28. Let $\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix} \in S_n$. Show that we can write $\alpha^{-1}$ as

$$\beta = \begin{pmatrix} \alpha_1 & \alpha_n & \alpha_{n-1} & \cdots & \alpha_2 \end{pmatrix}.$$

For example, if $\alpha = \begin{pmatrix} 2 & 5 & 3 & 6 \end{pmatrix}$, $\alpha^{-1} = \begin{pmatrix} 2 & 6 & 3 & 5 \end{pmatrix}$. *Hint:* Try computing $\alpha \circ \beta$ and $\beta \circ \alpha$.

EXERCISE 5.29. In the textbook *God Created the Integers...* the famous theoretical physicist Stephen Hawking reprints, with commentary, some of the greatest mathematical results of all time. One of the excerpts 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

Hawking's explanation is **wrong**, and this exercise leads you towards an explanation as to why.[1]

(a) Find all six subgroups of $S_3$. *Hint:* 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 5.25 on the preceding page, you know that $S_3 \cong D_3$, and some subgroups of $D_3$ appear in Example 3.8 on page 43 and Exercise 3.16 on page 45.
(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 $S_3$?
(c) Why is Hawking's explanation of Galois' result "obviously" wrong?

## 5.3. DIHEDRAL GROUPS

In Section 2.6 we studied the symmetries of a triangle; we represented the group as the products of matrices $\rho$ and $\varphi$, derived from the symmetries of *rotation* and *reflection about the y-axis*. Figure 5.1 on the next page, a copy of Figure 2.2 on page 38, shows how $\rho$ and $\varphi$ correspond to the symmetries of an equilateral triangle centered at the origin. In Exercises 5.22–5.25 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 5.30. The **dihedral set** $D_n$ is the set of symmetries of a regular polygon with $n$ sides.

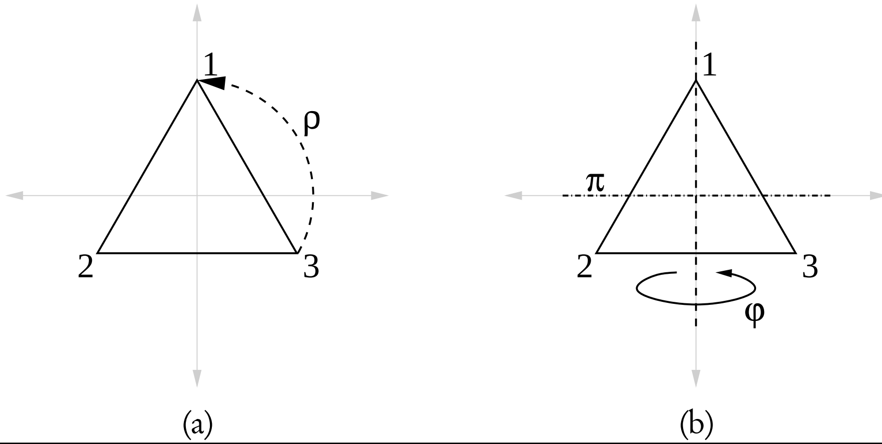
Is $D_n$ always a group?

THEOREM 5.31. *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 5.31 depends on the following proposition, which we accept without proof. We could prove it using an argument from matrices as in Section 2.6, but proving it requires more energy than is appropriate for this section.

[1]That said, the book is exceptionally good, and Hawking has contributed more to human understanding of the universe than I ever will. Probably Hawking was trying to simplify what Galois actually showed, and went too far: Galois was studying a certain class of normal subgroup called a **solvable group**.

FIGURE 5.1. Rotation and reflection of an equilateral triangle centered at the origin




PROPOSITION 5.32. *All the symmetries of a regular $n$-sided polygon can be generated by a composition of a power of the rotation $\rho$ of angle $2\pi/n$ and a power of the flip $\varphi$ across the $y$-axis. In addition, $\varphi^2 = \rho^n = \iota$ (the identity symmetry) and $\varphi\rho = \rho^{n-1}\varphi$.*

PROOF OF THEOREM 5.31. We must show that properties (G1)–(G4) are satisfied.

(G1): Closure follows from Proposition 5.32.

(G2): The associative property follows from the fact that permutations are functions, and the associative property applies to functions.

(G3): Certainly there exists an identity element $\iota \in D_n$, which corresponds to the identity symmetry where no vertex is moved.

(G4): 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 $\rho$ and $\varphi$ in Proposition 5.32, 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 5.33. 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 $\rho$ 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 $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$.

Application of $\varphi$ 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 $\begin{pmatrix} 2 & 3 \end{pmatrix}$.

In the context of the symmetries of the triangle, it looks as if we can say that $\rho = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ and $\varphi = \begin{pmatrix} 2 & 3 \end{pmatrix}$. Recall that $\rho$ and $\varphi$ generate all the symmetries of a triangle; likewise, these two cycles generate all the permutations of a list of three elements! (See Example 5.20 on page 85 and Exercise 2.68 on page 39.) ◇

We can do this with $D_4$ and $S_4$ as well.

EXAMPLE 5.34. 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

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

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 on the next page. We can also imagine other diagonals; but they can be shown to be superfluous, just as we show shortly that $\vartheta$ and $\psi$ are superflulous. There may be other symmetries of the square, but we'll stop here for the time being.

Is it possible to write $\psi$ as a composition of $\varphi$ and $\rho$? 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 2.6.

- Geometrically, $\rho$ moves $(1,2,3,4)$ to $(4,1,2,3)$; subsequently $\varphi$ moves $(4,1,2,3)$ to $(1,4,3,2)$; see Figure 5.3.
- We can use the tabular notation for $\psi$, $\varphi$, and $\rho$ 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

  $$\begin{aligned}(\varphi \circ \rho)(1,2,3,4) &= \varphi(\rho(1,2,3,4)) \\ &= \varphi(4,1,2,3) \\ &= (1,4,3,2).\end{aligned}$$

FIGURE 5.2. Rotation and reflection of a square centered at the origin

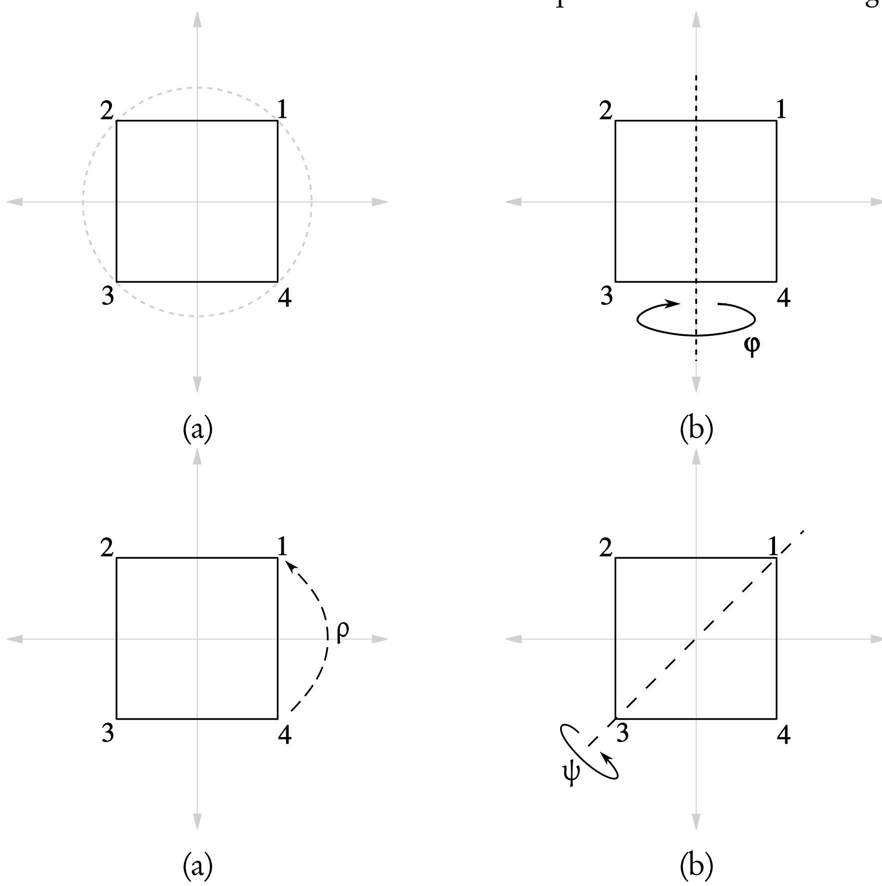
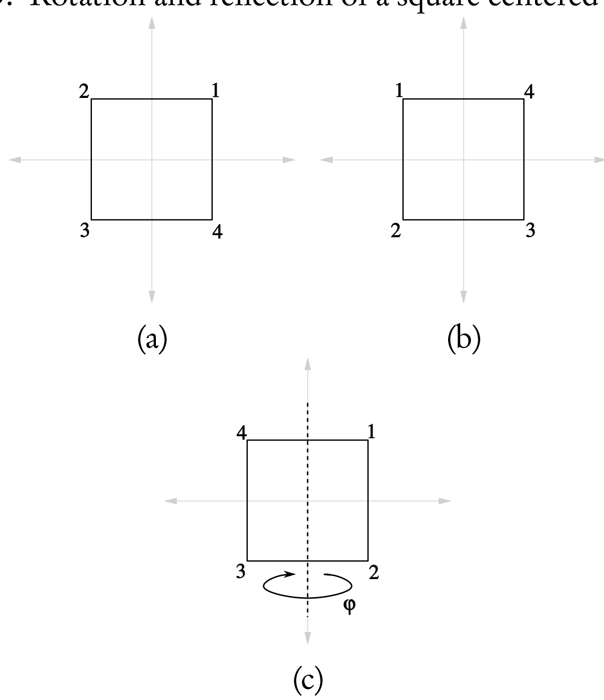



FIGURE 5.3. Rotation and reflection of a square centered at the origin



How did we get that last step? Look back at the tabular notation for $\varphi$: 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:

$$\begin{array}{ccccc} \mathbf{4}, & & 1, & 2, & 3 \\ & \searrow & & & \\ ?, & & \mathbf{4}, & ?, & ? \end{array}$$

The tabular notation for $\varphi$ also tells us to move the element in the second entry (1) to the first. Thus

$$\begin{array}{ccccc} 4, & & \mathbf{1}, & 2, & 3 \\ & & & & \\ \mathbf{1}, & & 4, & ?, & ? \end{array}$$

Likewise, $\varphi$ moves the element in the third entry (2) to the fourth, and vice-versa, giving us

$$\begin{array}{cccccc} 4, & & 1, & \mathbf{2}, & & \mathbf{3} \\ & & & & & \\ 1, & & 4, & \mathbf{3}, & & \mathbf{2} \end{array}$$

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 $\varphi$ and $\rho$ 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 $\rho$ after some power of $\varphi$. 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 $4! = 24$. $\diamond$

COROLLARY 5.35. *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.*

EXERCISES.

EXERCISE 5.36. Without using Corollary (5.35), show that $D_3 \cong S_3$. *Hint:* Define a homomorphism $f$ from $D_3$ to $S_3$ by deciding first the values of $f(\rho)$ and $f(\varphi)$. After that, you can 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 5.37. Write all eight elements of $D_4$ in cycle notation.

EXERCISE 5.38. Construct the composition table of $D_4$. Compare this result to that of Exercise 2.47.

EXERCISE 5.39. Show that the symmetries of any $n$-gon can be described as a power of $\rho$ and $\varphi$, where $\varphi$ is a flip about the $y$-axis and $\rho$ is a rotation of $2\pi/n$ radians.

## 5.4. CAYLEY'S REMARKABLE RESULT

The mathematician Arthur Cayley discovered a lovely fact about the permutation groups.

THEOREM 5.40 (Cayley's Theorem). *Every finite group of $n$ elements 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 5.41. 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

$$f(x) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \ell(x \cdot e) & \ell(x \cdot a) & \ell(x \cdot b) & \ell(x \cdot ab) \end{pmatrix}, \tag{5.4.1}$$

where $\ell(y)$ is the label that corresponds to $y$.

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 (5.4.1) 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 third row of the multiplication table), and filling in the labels for the entries in that row! Doing this or applying equation (5.4.1) 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 $\ell$ 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 $m$th 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 $z = x \cdot \ell^{-1}(m)$. Similar statement holds for how $f(y)$ and $f(xy)$ move $m$.

- Applying these facts, we observe that

$$\begin{aligned}(f(x)\circ f(y))(m) &= (f(x))(f(y)(m))\\ &= f(x)\left(\ell\left(y\cdot\ell^{-1}(m)\right)\right)\\ &= \ell\left(x\cdot\ell^{-1}\left(\ell\left(y\cdot\ell^{-1}(m)\right)\right)\right)\\ &= \ell\left(x\cdot\left(y\cdot\ell^{-1}(m)\right)\right)\\ &= \ell\left(xy\cdot\ell^{-1}(m)\right)\\ &= f(xy)(m).\end{aligned}$$

- 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. $\diamond$

You should read through Example 5.41 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 5.41 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 operation table for $G$. By this fact we know that $f$ is one-to-one and onto (see also Theorem 2.41 on page 29). The proof that $f$ is a homomorphism is identical to the proof for Example 5.41: 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 $G \cong f(G) < S_n$. $\square$

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 5.42. In Example 5.41 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 2.2 on page 38 and 5.2.

EXERCISE 5.43. 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 5.44. The subgroup of $S_4$ that you identified in Exercise 5.43 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 5.45. Since $S_3$ has six elements, we know it is isomorphic to a subgroup of $S_6$. Can you identify this subgroup *without* using the isomorphism used in the proof of Cayley's Theorem?

## 5.5. ALTERNATING GROUPS

A special kind of symmetry group 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 5.46. 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 5.47. The permutation $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \in S_3$ is a 3-cycle. The permutation $\begin{pmatrix} 2 & 3 \end{pmatrix} \in S_3$ is a transposition. The permutation $\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} \in S_4$ 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 $\begin{pmatrix} 1 & 3 & ? \end{pmatrix}$. 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. $\diamondsuit$

Thanks to 1-cycles, any permutation can be written with many different numbers of cycles: for example,

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}(1) = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}(1)(3) = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}(1)(3)(1) = \cdots .$$

In addition, a neat trick allows us to write every permutation as a composition of transitions.

EXAMPLE 5.48. $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$. Also

$$\begin{pmatrix} 1 & 4 & 8 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 8 \end{pmatrix}\begin{pmatrix} 1 & 4 \end{pmatrix}.$$

Also $(1) = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$. $\diamondsuit$

LEMMA 5.49. *Any permutation can be written as a composition of transitions.*

PROOF. You do it! See Exercise (5.58). $\square$

At this point it is worth looking at Example 5.48 and the discussion before it. Can we write $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ with many different numbers of *transpositions*? Yes:

$$\begin{aligned}
\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} &= \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix} \\
&= \cdots .
\end{aligned}$$

Notice something special about the representation of $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$. No matter how you write it, it always has an *even* number of transpositions. By contrast, consider

$$\begin{aligned}\begin{pmatrix} 2 & 3 \end{pmatrix} &= \begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\\ &= \begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix} = \cdots .\end{aligned}$$

No matter how you write it, you always represent $\begin{pmatrix} 2 & 3 \end{pmatrix}$ with an *odd* number of transpositions.

Is this always the case?

THEOREM 5.50. *Let $\alpha$ be a cycle.*

- *If $\alpha$ 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 $\alpha$ 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

$$g = \prod_{1 \le i < j \le n} \left(x_i - x_j\right) \qquad \text{and} \qquad g_\alpha := \prod_{1 \le i < j \le n} \left(x_{\alpha(i)} - x_{\alpha(j)}\right).$$

Sometimes $g = g_\alpha$; for example, if $\alpha = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ then

$$g = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

and

$$g_\alpha = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = [(-1)(x_1 - x_3)][(-1)(x_2 - x_3)](x_1 - x_2) = g. \tag{5.5.1}$$

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 $g_\alpha = x_2 - x_1 \neq g$.

Failing this, can we write $g_\alpha$ *in terms of* $g$? Try the following. If $\alpha(i) < \alpha(j)$, then the binomial $x_{\alpha(i)} - x_{\alpha(j)}$ appears in $g$, so we'll leave it alone. (An example would be $(x_1 - x_2)$ in equation (5.5.1).) Otherwise $\alpha(i) > \alpha(j)$ and the binomial $x_{\alpha(i)} - x_{\alpha(j)}$ does not appear in $g$. (An example would be $(x_3 - x_1)$ in equation (5.5.1).) However, the binomial $x_{\alpha(j)} - x_{\alpha(i)}$ does appear in $g$, so rewrite $g_\alpha$ by replacing $x_{\alpha(i)} - x_{\alpha(j)}$ as $\left[-\left(x_{\alpha(j)} - x_{\alpha(i)}\right)\right]$.

Recall that $\alpha$ is a one-to-one function: for each $i$, $x_i$ is mapped to one unique $x_{\alpha(i)}$. In addition, each binomial $x_i - x_j$ in $g$ is unique, so for each $i, j$, the binomial $x_i - x_j$ is mapped to a binomial $x_{\alpha(i)} - x_{\alpha(j)}$ where the subscripts are unique; that is, in $g_\alpha$ there is are no $k, \ell$ such that the binomial $x_{\alpha(k)} - x_{\alpha(\ell)}$ has the same pair of subscripts as $x_{\alpha(i)} - x_{\alpha(j)}$. Thus, factoring the constant -1 multiples from the product gives us

$$g_\alpha = (-1)^{\operatorname{swp}\alpha} g, \tag{5.5.2}$$

where $\operatorname{swp}\alpha \in \mathbb{N}$ is an integer representing the number of swapped indices that $\alpha$ provoked in the binomials of $g$.

It is important to note we made no assumptions about how $\alpha$ was written when deriving equation (5.5.2). We worked only with what $\alpha$ actually does. Thus, equation (5.5.2) remains true *no matter what $\alpha$ "looks like" in a representation by transpositions*.

With that in mind, consider two different representations of $\alpha$ by transpositions. If the first representation has an even number of transpositions, then an even number of binomials in $g$

swapped indices to get $g_\alpha$, so swp $\alpha$ is even. Hence $g_\alpha = g$. If the second representation had an odd number of transpositions, there would be an odd number of swaps from $g$ to $g_\alpha$, , and swp $\alpha$ would be odd and $g_\alpha = -g$. However, we pointed out in the previous paragraph that the value of $g_\alpha$ depends on the *permutation* $\alpha$, not on its *representation by transpositions*. Since $g$ is non-zero, it is impossible that $g_\alpha = g$ and $g_\alpha = -g$. It follows that both representations must have the same number of transpositions.

The statement of the theorem follows: if we can write $\alpha$ as a product of an even (resp. odd) number of transpositions, then it cannot be written as the product of an odd (resp. even) number of transpositions. □

So Lemma (5.49) tells us that any permutation can be written as a composition of transpositions, and Theorem 5.50 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 5.51. 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 5.52. The permutation $\rho = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \in S_3$ is even, since as we saw earlier $\rho = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$. So is the permutation $\iota = (1) = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$.

The permutation $\varphi = \begin{pmatrix} 2 & 3 \end{pmatrix}$ is odd. ◇

At this point we are ready to define a new group.

DEFINITION 5.53. 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. Although $A_3$ is not the same as "$A_3$" in Example 3.49 on page 53, the two are isomorphic because $D_3 \cong S_3$.

THEOREM 5.54. *For all $n \geq 2$, $A_n$ is a group under the operation of composition of functions.*

PROOF. Let $n \geq 2$. We show that $A_n$ satisfies properties (G1)–(G4) of a group.

(G1): For closure, let $\alpha, \beta \in A_n$. Both $\alpha$ and $\beta$ can be written as the composition of an even number of transpositions. The sum of two even numbers is also even, so $\alpha \circ \beta$ is also the composition of an even number of transpositions.

(G2): The associative property is inherited from $S_n$, or more generally from the associative property of the composition of functions.

(G3): The identity element is $\iota = (1)$, which Example 5.48 shows is even.

(G4): Let $\alpha \in A_n$. Write $\alpha$ as a composition of transpositions, denoted by

$$\alpha = \tau_1 \tau_2 \cdots \tau_m$$

for some $m \in \mathbb{N}^+$. Since $\alpha \in A_n$, $m$ is even. Let

$$\beta = \tau_m \tau_{m-1} \cdots \tau_1.$$

You will show in Exercise 5.59 that any transposition is its own inverse, so

$$\begin{aligned}
\alpha\beta &= (\tau_1\tau_2\cdots\tau_m)(\tau_m\tau_{m-1}\cdots\tau_1)\\
&= (\tau_1\tau_2\cdots\tau_{m-1})(\tau_m\tau_m)(\tau_{m-1}\tau_{m-1}\cdots\tau_1)\\
&= (\tau_1\tau_2\cdots\tau_{m-1})\,\iota\,(\tau_{m-1}\tau_{m-2}\cdots\tau_1)\\
&= (\tau_1\tau_2\cdots\tau_{m-2})(\tau_{m-1}\tau_{m-1})(\tau_{m-2}\tau_{m-3}\cdots\tau_1)\\
&= (\tau_1\tau_2\cdots\tau_{m-2})\,\iota\,(\tau_{m-2}\tau_{m-3}\cdots\tau_1)\\
&\vdots\\
&= \tau_1\tau_1\\
&= \iota.
\end{aligned}$$

Hence $\alpha\beta = (\ 1\ )$. A similar argument shows that $\beta\alpha = (\ 1\ )$, so $\beta = \alpha^{-1}$. We have written $\beta$ with $m$ transpositions. Recall that $m$ is even, so $\alpha^{-1} = \beta \in A_n$.

□

How large is $A_n$, relative to $S_n$?

THEOREM 5.55. *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 51, 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 $\alpha$ is an even permutation, then $X = A_n$. Otherwise, $\alpha$ is odd. Let $\beta$ be any other odd permutation. Write out the odd number of transpositions of $\alpha^{-1}$, followed by the odd number of transpositions of $\beta$, to see that $\alpha^{-1}\beta$ is an even permutation. Hence $\alpha^{-1}\beta \in A_n$, and by Lemma 3.27 on page 48 $\alpha A_n = \beta A_n$.

We have shown that any coset of $A_n$ is either $A_n$ itself or $\alpha A_n$ for some odd permutation $\alpha$. 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 5.56. *For any $n \geq 2$, $A_n \triangleleft S_n$.*

PROOF. You do it! See Exercise 5.61. □

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 5.57. List the elements of $A_2, A_3$, and $A_4$ in cycle notation.

EXERCISE 5.58. Show that any permutation can be written as a product of transpositions. *Hint:* Lemma 5.49 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 $\alpha = (\ \alpha_1 \quad \alpha_2 \quad \cdots \quad \alpha_n\ )$ and write it as a product of transpositions, as suggested by Example 5.48. Be sure to explain why this product does in fact equal $\alpha$.

EXERCISE 5.59. Show that the inverse of any transposition is a transposition. *Hint:* You can do this by showing that any transposition is its own inverse. Take an arbitrary transposition $\alpha = (\ \alpha_1 \quad \alpha_2\ )$ and show that $\alpha^2 = \iota$.

EXERCISE 5.60. Show that the function $\operatorname{swp}\alpha$ defined in Theorem 5.50 satisfies the property that for any two cycles $\alpha, \beta$ we have $(-1)^{\operatorname{swp}(\alpha\beta)} = (-1)^{\operatorname{swp}\alpha}(-1)^{\operatorname{swp}\beta}$. *Hint:* Let $\alpha$ and $\beta$ be arbitrary cycles. Consider the four possible cases where $\alpha$ and $\beta$ are even or odd.

EXERCISE 5.61. Show that for any $n \geq 2$, $A_n \triangleleft S_n$. *Hint:* See a previous exercise about subgroups or cosets.

## 5.6. THE 15-PUZZLE

The 15-puzzle is similar to a toy you probably played with as a child. It looks like a $4 \times 4$ 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 $\tau$ 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 5.62. 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 5.63. *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 $\tau$ 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 $\sigma$ consisting of an even number of transpositions. By Theorem 5.50 on page 96 and Definitions 5.51 and 5.53, $\sigma \in A_{16}$. □

We can now show that there is no solution to the 15-puzzle.

THEOREM 5.64. *The 15-puzzle has no solution.*

PROOF. By way of contradiction, assume that it has a solution $\sigma$. 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 $\sigma^{-1}$ 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 $\sigma^{-1}$, 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.[2]

The textbook [**Lau03**] contains a more general discussions of solving puzzles of this sort using algebra.

EXERCISES.

EXERCISE 5.65. 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 | |

.

*Hint:* Use the same strategy as that of the proof of Theorem 5.64: find the permutation $\sigma^{-1}$ 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.

---

[2]According to the website `http://www.measuringworth.com/ppowerus/result.php`.

CHAPTER 6

# Applications of groups to elementary number theory

The theory of groups was originally developed by mathematicians who were trying to answer questions about permutations of the roots of polynomials. From such beginnings it has grown to many applications that would seem to have little in common with the roots of polynomials. Some of the most widely-used applications in recent decades are in number theory, the study of properties of the integers, especially the properties of so-called "prime" numbers.

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 of these tools will 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 describe in Chapter 1.1.

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 Greatest Common Divisor and the Euclidean Algorithm

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. Many of the concepts underlying greatest common divisors turn out to be deeply interesting topics on their own. Because of this, we review them as well, starting with a definition which you probably don't expect.

Definition 6.1. Let $n \in \mathbb{N}^+$ and assume $n > 1$. We say that $n$ is **irreducible** if the only integers that divide $n$ are $\pm 1$ and $\pm n$.

You may read this and think, "Oh, he's talking about prime numbers." Yes and no. More on that in the next section.

Example 6.2. The integer 36 is not irreducible, because $36 = 6 \times 6$. The integer 7 is irreducible, because the only integers that divide 7 are $\pm 1$ and $\pm 7$. $\diamondsuit$

**Algorithm 1**

```
            algorithm Euclidean algorithm
inputs
   m, n ∈ ℤ
outputs
   gcd(m, n)
do
   s := max(m, n)
   t := min(m, n)
   while t ≠ 0
      Let q, r ∈ ℤ be the result of dividing s by t
      s := t
      t := r
   return s
```

DEFINITION 6.3. 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** $d \mid n$. The **greatest common divisor of** $m$ **and** $n$, written $\gcd(m,n)$, is the largest of the common divisors of $m$ and $n$.

EXAMPLE 6.4. Common divisors of 36 and 210 are 1, 2, 3, and 6. ◇

One way to compute the list of common divisors is to list all possible divisors of both integers, and identify the largest possible positive divisor. In practice, this takes a Very Long Time™, so it would be nice to have a different method. One such method was described by the Greek mathematician Euclid many centuries ago.

THEOREM 6.5 (The Euclidean Algorithm). *Let $m,n \in \mathbb{Z}$. One 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 6.6. We compute $\gcd(36,210)$ using the Euclidean algorithm. Start by setting $s = 210$ and $t = 36$. Subsequently:

1. Dividing 210 by 36 gives $q = 5$ and $r = 30$. Set $s = 36$ and $t = 30$.
2. Dividing 36 by 30 gives $q = 1$ and $r = 6$. Set $s = 30$ and $t = 6$.
3. Dividing 30 by 6 gives $q = 5$ and $r = 0$. Set $s = 6$ and $t = 0$.

Now that $t = 0$, we stop, and conclude that $\gcd(36,210) = s = 6$. ◇

When we prove that the Euclidean algorithm generates a correct answer, we will argue that it computes $\gcd(m,n)$ by claiming

$$\gcd(m,n) = \gcd(m,r_1) = \gcd(r_1,r_2) = \cdots = \gcd\left(r_{k-1},0\right)$$

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 6.7 proves this claim.

LEMMA 6.7. *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 15. Then* $\gcd(s,t) = \gcd(t,r)$.

PROOF. Let $d = \gcd(s,t)$. First we show that $d$ is a divisor of $r$. From Definition 1.16 on page 16, 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 1.16 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 $s = q\left(d'x\right) + d'y$; 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) **Termination.** To prove that any algorithm provides a correct answer, you must prove that it gives *some* answer. How can this be a problem? If you look at the Euclidean algorithm, you see that one of its instructions asks us to "repeat" some steps "until $t = 0$." 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.
(2) **Correctness.** Even if the algorithm terminates, we have to guarantee that it terminates with the correct answer.

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 1.3; 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 step 2. The first time we compute step 2(a), we compute the quotient $q$ and remainder $r$ of division of $s$ by $t$. By the Division Theorem,

$$0 \leq r < t. \tag{6.1.1}$$

Denote this value of $r$ by $r_1$. In step 2(b) we set $s$ to $t$, and in step 2(c) we set the value of $t$ to $r_1 = r$. Thanks to equation (6.1.1), the value of $t_{\text{new}} = r$ is smaller than $s_{\text{new}} = t_{\text{old}}$. If $t \neq 0$, then we return to 2(a) 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

$$0 \leq r_2 < r_1.$$

As long as we repeat step 2, we generate a set of integers $R = \{r_1, r_2, \ldots\} \subset \mathbb{N}$. 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, step 2 of the algorithm must stop repeating; otherwise, we would generate $r_{i+1} < r_i$, contradicting the fact that $r_i$ is the smallest element of $R$. Since step 2 of the algorithm terminates, the algorithm itself terminates.

Now we show that the algorithm terminates *with the correct answer*. If step 2 of the algorithm repeated $k$ times, then applying Lemma 6.7 repeatedly to the remainders of the divisions gives us the chain of equalities

$$\begin{aligned}
\gcd\left(r_{k-1}, r_{k-2}\right) &= \gcd\left(r_{k-2}, r_{k-3}\right) \\
&= \gcd\left(r_{k-3}, r_{k-4}\right) \\
&\;\vdots \\
&= \gcd\left(r_2, r_1\right) \\
&= \gcd\left(r_1, s\right) \\
&= \gcd\left(t, s\right) \\
&= \gcd\left(m, n\right).
\end{aligned}$$

What is $\gcd\left(r_{k-1}, r_{k-2}\right)$? The final division of $s$ by $t$ is the division of $r_{k-1}$ by $r_{k-2}$; since the algorithm terminates after the $k$th repetition, $r_k = 0$. By Definition 1.16, $r_{k-1} \mid r_{k-2}$, 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 $r_{k-2}$ is $r_{k-1}$. Following the chain of equalities, we conclude that $\gcd\left(m, n\right) = r_{k-1}$: 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 6.7 we showed that $\gcd\left(m, n\right) = \gcd\left(m, r\right)$ where $r$ is the remainder after division of $m$ by $n$. Prove the following more general statement: for all $m, n, q \in \mathbb{Z}$ $\gcd\left(m, n\right) = \gcd\left(m - qn\right)$.

## 6.2. THE CHINESE REMAINDER THEOREM; THE CARD TRICK EXPLAINED

In this section we explain how the card trick from Section 1.1 works. The result is based on an old, old Chinese observation.

THEOREM 6.11 (The Chinese Remainder Theorem, simple version). *Let $m, n \in \mathbb{Z}$ such that $\gcd\left(m, n\right) = 1$. 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* $N = mn$*.*

Before giving the 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. This gave the remainders $\alpha$ from division by three and $\beta$ from division by four, leading to the 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 us that there is a solution for $x$, and that this solution 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. $\diamondsuit$

The reader may be thinking, "Well, and good, 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. How does the Chinese Remainder Theorem help with that?" This emerges from the proof. 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 6.6 the computation of $\gcd(210, 36)$. The divisions gave us a series of equations:

$$210 = 5 \cdot 36 + 30 \tag{6.2.1}$$
$$36 = 1 \cdot 30 + 6 \tag{6.2.2}$$
$$30 = 5 \cdot 6 + 0.$$

We concluded from the Euclidean Algorithm that $\gcd(210, 36) = 6$. We start by rewriting the equation 6.2.2:

$$36 - 1 \cdot 30 = 6. \tag{6.2.3}$$

This looks a little like what we want, but we need 210 instead of 30. Equation 6.2.1 allows us to rewrite 30 in terms of 210 and 36:

$$30 = 210 - 5 \cdot 36. \tag{6.2.4}$$

Substituting this result into equation 6.2.3, we have

$$36 - \cdot 1 (210 - 5 \cdot 36) = 6 \quad \Longrightarrow \quad 6 \cdot 36 + (-1) \cdot 210 = 6.$$

We have found integers $m = 6$ and $n = -1$ such that for $a = 36$ and $b = 210$, $\gcd(a, b) = 6$. $\diamondsuit$

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

$$\begin{aligned}
m &= q_1 n + r_1 \\
n &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \qquad (6.2.5)\\
r_{k-2} &= q_k r_{k-1} + r_k \qquad (6.2.6)\\
r_{k-1} &= q_{k+1} r_k + 0 \\
\text{and } r_k &= \gcd(m,n).
\end{aligned}$$

Using the last equation, we can rewrite equation 6.2.6 as

$$r_{k-2} = q_k r_{k-1} + \gcd(m,n).$$

Solving for $\gcd(m,n)$, we have

$$r_{k-2} - q_k r_{k-1} = \gcd(m,n). \qquad (6.2.7)$$

Now solve equation 6.2.5 for $r_{k-1}$ to obtain

$$r_{k-3} - q_{k-1} r_{k-2} = r_{k-1}.$$

Substitute this into equation 6.2.7 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 will exhaust the list of equations, concluding by rewriting the first equation in the form $am + bn = \gcd(m,n)$ for some integers $a, b$. □

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 $am + bn = \gcd(m,n) = 1$. 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 also need a lemma about arithmetic with clockwork groups. Lemma 3.66 on page 57 already tells you how you can add in clockwork groups; Lemma  allows you to multiply in a similar way.

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.

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 $bn \in 1 + \langle m \rangle$ and $am \in 1 + \langle n \rangle$. Or, in the bracket notation, $[bn] = [1]$ in $\mathbb{Z}_m$ and $[am] = [1]$ in $\mathbb{Z}_n$. By Lemmas 3.64 and 3.66 on page 57, $[\alpha bn] = [\alpha]$ in $\mathbb{Z}_m$ and $[\beta am] = [\beta]$ in $\mathbb{Z}_n$. Likewise, $[\alpha bn] = [0]$ in $\mathbb{Z}_n$ and $[\beta am] = [0]$ in $\mathbb{Z}_m$. Hence

$$\begin{cases} [\alpha bn + \beta am] & = [\alpha] \text{ in } \mathbb{Z}_m; \text{ and} \\ [\alpha bn + \beta am] & = [\beta] \text{ in } \mathbb{Z}_n. \end{cases}$$

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 $[x] = [y]$ in $\mathbb{Z}_n$, $[x - y] = [0]$, so $n \mid (x - y)$. 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 by Lemma 3.69 $[x] = [y]$ in $\mathbb{Z}_N$, as desired. □

The existence part of the proof gives us an algorithm to solve problems involving the Chinese Remainder Theorem:

COROLLARY 6.16 (Chinese Remainder Theorem Algorithm, simple version). *Let $m, n \in \mathbb{Z}$ such that* $\gcd(m,n) = 1$. *Let $\alpha, \beta \in \mathbb{Z}$. Write $N = mn$. We can solve the system of linear congruences*

$$\begin{cases} [x] & = [\alpha] \textit{ in } \mathbb{Z}_m; \\ [x] & = [\beta] \textit{ in } \mathbb{Z}_n; \end{cases}$$

*for $[x] \in \mathbb{Z}_N$ by the following steps:*

(1) *Use the Extended Euclidean Algorithm to find $a, b \in \mathbb{Z}$ such that $am + bn = 1$.*
(2) *The solution is $[\alpha bn + \beta am]$ in $\mathbb{Z}_N$.*

PROOF. The proof follows immediately from the existence proof of Theorem 6.11. □

EXAMPLE 6.17. The algorithm of Corollary 6.16 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. $\diamond$

The Chinese Remainder Theorem can be generalized to larger systems with more than two equations under certain circumstances.

THEOREM 6.18 (Chinese Remainder Theorem on $\mathbb{Z}$). *Let $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ and assume that* $\gcd\left(m_i, m_j\right) = 1$ *for all $1 \leq i < j \leq n$. 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 6.19. *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 $\pm 1$; 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

$$\begin{aligned} 1 &= \left(a' m_1 + b' m_2 m_3\right)(em_1 + fm_4) \\ &= \left(a' em_1 + a' fm_4 + b' em_2 m_e\right) m_1 + \left(b' f\right)(m_2 m_3 m_4). \end{aligned}$$

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 $\gcd(m_1, N_1) = 1$. $\square$

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 6.19, $\gcd(m_i, N_i) = 1$. Use the Extended Euclidean Algorithm to compute $a_1, b_1, a_2, b_2, \ldots, a_n, b_n$ such that

$$\begin{gathered} a_1 m_1 + b_1 N_1 = 1 \\ a_2 m_2 + b_2 N_2 = 1 \\ \vdots \\ a_n m_n + b_n N_n = 1. \end{gathered}$$

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 $[\alpha_i b_i N_i] = [0]$. 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 6.19, $\gcd(m_1 m_2, m_3) = 1$, 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 6.20. 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 6.21. 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 6.22. Solve the system of linear congruences

$$\begin{cases} [x] & = [33] \text{ in } \mathbb{Z}_{16}; \\ [x] & = [-4] \text{ in } \mathbb{Z}_{33}; \\ [x] & = [17] \text{ in } \mathbb{Z}_{504}. \end{cases}$$

*Hint:* This problem is a little tougher, since $\gcd(16, 504) \neq 1$ and $\gcd(33, 504)$. 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 6.23. 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 6.24. 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 6.25. Is it possible to modify the card trick to work with only eight cards instead of 12? If so, how; if not, why not?

## 6.3. MULTIPLICATIVE CLOCKWORK GROUPS

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. *Warning:* the following definition is guaranteed to offend your sensibilities.

DEFINITION 6.26. Let $p \in \mathbb{Z}$ 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 6.27. 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 $b$, because it is prime. In fact, $17 \times 4 = 68 = a$. ◇

The definition of a prime number may surprise you, since ordinarily people think of a *prime* number as being *irreducible*. In fact, you will prove for homework:

THEOREM 6.28. *A positive integer is irreducible if and only if it 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 encounter one such set later in the notes.

Primes are useful because every integer has a unique factorization into primes:

THEOREM 6.29. *Let $n \in \mathbb{Z}$ and assume $n > 1$. 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 (hence, prime) and $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}_{\geq 0}$. In addition, this representation is unique if we order $p_1 < p_2 < \ldots < p_n$.*

PROOF. The proof has two parts: a proof of existence and a proof of uniqueness.

*Existence:* We proceed by induction on the integers larger than or equal to two.

*Inductive base:* If $n = 2$, $n$ 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, so there exists an 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 $p_1^{\alpha_1} \mid n$. Use the definition of divisibility (Definition 1.16 on page 16) to find $q \in \mathbb{Z}$ such that $n = q p_1$. By the definition of irreducible, we know that $p_1 \neq 1$, so $q < n$. Since $p_1$ is not negative, $q > 1$. 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:* 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 6.30. *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 3.27 on page 48 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 3.27 again tells us that $[ab] = [cb]$ as desired, so the proposed multiplication of elements in $\mathbb{Z}_n$ is well-defined. □

EXAMPLE 6.31. 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 $\mathbb{Z}_5\backslash\{[0]\}$? 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. $\diamondsuit$

You might think that this trick of dropping zero and building a multiplication table always works, *but it doesn't*.

EXAMPLE 6.32. 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:

| × | 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. $\diamondsuit$

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 $\mathbb{Z}_6\backslash\{[0],[2],[3],[4]\} = \{[1],[6]\}$.

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. Can we find a criterion to detect this?

LEMMA 6.33. *Let $x \in \mathbb{Z}_n$, with $x \neq [0]$. The following are equivalent:*
*(A) There exists $y \in \mathbb{Z}_n$, $y \neq [0]$, such that $xy = [0]$.*
*(B) For any representation $[a]$ of $x$, there exists a common divisor $d$ of $a$ and $n$ such that $d \neq \pm 1$.*

PROOF. *That (B) implies (A):* If $a$ and $n$ share a common divisor $d$, use the definition of divisibility to choose $q$ such that $n = qd$. Likewise choose $t$ such that $a = td$. Then

$$qx = q[a] = q[td].$$

Lemma 3.66 implies that

$$q[td] = [qtd] = t[qd] = t[n] = [0].$$

Likewise, we conclude that if $y = [q]$ then $xy = [0]$.

*That (A) implies (B):* 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 3.69 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 $\pm 1$, 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

$$b = p_1 b_1 = p_1 (p_2 b_2) = \cdots = p_1 (p_2 (\cdots (p_r b_r))) \tag{6.3.1}$$

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 $\pm 1$.

*Case* 2. If $n_r = 1$, then $n = p_1 p_2 \cdots p_r$. By substitution into equation 6.3.1, $b = nb_r$. 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 $\pm 1$. □

Let's try then to make a *multiplicative* group out of the set of elements of $\mathbb{Z}_n$ that do not violate the zero product rule.

DEFINITION 6.34. Let $n \in \mathbb{Z}$. 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) We say that $a, b \in \mathbb{Z}_n$ are **zero divisors** if the canonical representation of $[ab]$ is $[0]$. That is, zero divisors are the elements of $\mathbb{Z}_n$ that violate the zero-product property of multiplication.
(3) 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,
$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \setminus \{0\} : \forall y \in \mathbb{Z}_n \; ab \neq 0\}.$$

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 6.35. *$\mathbb{Z}_n^*$ is an abelian group under its multiplication.*

PROOF. We showed in Lemma 6.30 that the operation is well-defined. We check each of the requirements of a group:

(G1): Let $x, y \in \mathbb{Z}_n^*$; represent $x = [a]$ and $y = [b]$. By definition of $\mathbb{Z}_n^*$, $a$ and $b$ have no common divisors with $n$ aside from $\pm 1$; thus $ab$ also has no common divisors with $n$ aside from $\pm 1$. As a result, $xy = [ab] \in \mathbb{Z}_n^*$.

(G2): Let $x, y, z \in \mathbb{Z}_n^*$; represent $x = [a]$, $y = [b]$, and $z = [c]$. Then

$$x(yz) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = (xy)z.$$

(G3): 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 $[1] \cdot x = x$.

(G4): 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 $x \neq 0$, $m \notin \mathbb{Z}_n$, so $n \nmid m$. From Lemma 6.33, $m$ and $n$ have no common divisors except $\pm 1$; 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 3.27 on page 48, 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

$$yx = [1].$$

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 $\pm 1$ divide 1, so $\gcd(a, n) = 1$. So $y \in \mathbb{Z}_n^*$, and $x$ has an inverse in $\mathbb{Z}_n^*$.

(G5) 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, $\mathbb{Z}_n^*$.

EXERCISES.

EXERCISE 6.36. 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 6.37. 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 6.38. Let $p \in \mathbb{Z}$, and $p > 1$. Show that $p$ is irreducible iff $p$ is prime. *Hint:* Use the prime factorization of $ab$ (Theorem 6.29), and use the properties of prime numbers.

## 6.4. EULER'S NUMBER, EULER'S THEOREM, AND FAST EXPONENTIATION

In Section 6.3 we defined the group $\mathbb{Z}_n^*$ for all $n \in \mathbb{N}_{>1}$. This group satisfies an important property called *Euler's Theorem.* Much of what follows is related to some work of Euler, pronounced in a way that rhymes with "oiler". Euler was a very influential mathematician: You already know of Euler's number $e = \lim_{x\to\infty}\left(1+\frac{1}{x}\right)^x \approx 2.718$; Euler is well-known for contributions to Calculus, Differential Equations, and to Number Theory. He was extremely prolific, and is said to have calculated the way "ordinary" men breathe. After losing his sight in one eye, he expressed his happiness at being only half as distracted from his work as he was before. He sired a large number of children, and used to work with one child sitting on each knee. He is, in short, the kind of historical figure that greatly lowers my self-esteem as a mathematician.

DEFINITION 6.39. **Euler's $\varphi$-function** is $\varphi(n) = \left|\mathbb{Z}_n^*\right|$.

THEOREM 6.40 (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 3.40 to Lagrange's Theorem, $\operatorname{ord}(x) \mid \left|\mathbb{Z}_n^*\right|$. Hence $\operatorname{ord}(x) \mid \varphi(n)$; 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 6.41. *For all $x \in \mathbb{Z}_n^*$, $x^{-1} = x^{\varphi(n)-1}$.*

PROOF. You do it! See Exercise 6.50. □

It thus becomes an important computational question to ask, how large is this group? For irreducible integers this is easy: if $p$ is irreducible, $\varphi(p) = p - 1$. For reducible integers, it is not so easy: using Definitions 6.39 and 6.34, $\varphi(n)$ is the number of positive integers smaller than $n$ and sharing no common divisors with $n$. 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 is unsatisfactory: it requires us to try two divisions on all the positive integers between 2 and 28. That takes too long, and becomes even more burdensome when dealing with large numbers. There has to be a better way! Unfortunately, no one knows it.

One thing we can do is break $n$ into its factors. Presumably, it would be easier to compute $\varphi(m)$ for these smaller integers $m$, but how to recombine them?

LEMMA 6.42. *Let* $n \in \mathbb{N}^+$. *If* $n = pq$ *and* $\gcd(p,q) = 1$, *then* $\varphi(n) = \varphi(p)\varphi(q)$.

EXAMPLE 6.43. In the table above, we have $\varphi(15) = 8$. Notice that this satisfies

$$\varphi(15) = \varphi(5 \times 3) = \varphi(5)\varphi(3) = 4 \times 2 = 8. \diamondsuit$$

PROOF. Recall from Exercise 2.46 on page 30 that $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ is a group; a counting argument shows that 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 $f([a]_n) = ([a]_p, [a]_q)$ where $[a]_i$ denotes the congruence class of $a$ in $\mathbb{Z}_i$. First we show that $f$ is a homomorphism: Let $a, b \in \mathbb{Z}_n^*$; then

$$\begin{aligned} f([a]_n [b]_n) = f([ab]_n) &= ([ab]_p, [ab]_q) \\ &= ([a]_p [b]_p, [a]_q [b]_q) \\ &= ([a]_p, [a]_q)([b]_p, [b]_q) \\ &= f([a]_n) f([b]_n) \end{aligned}$$

(where Lemma 6.30 on page 112 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. We claim that this follows from the simple version of the Chinese Remainder Theorem, since the mapping $f$ corresponds precisely to the system of linear congruences

$$\begin{aligned} [x] &= [a] \text{ in } \mathbb{Z}_p^*; \\ [x] &= [b] \text{ in } \mathbb{Z}_q^*. \end{aligned}$$

That $f$ is onto follows from the fact that any such $x$ exists in $\mathbb{Z}_n$; that $f$ is one-to-one follows from the fact 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 we must show that more specifically $x \in \mathbb{Z}_n^*$. To see that indeed $x \in \mathbb{Z}_n^*$, let $d$ be any common divisor of $x$ and $n$. Let $c \in \mathbb{Z}$ such that $n = cd$. Let $r$ be an irreducible divisor of $d$; then $r \mid n$. Now $n = pq$, so $r \mid pq$, so $r \mid p$ or $r \mid q$. Then $d$ shares a common divisor with $p$ or with $q$. However, $x \in \mathbb{Z}_p^*$ implies that $\gcd(x,p) = 1$; likewise, $\gcd(x,q) = 1$. Since $d$ is a common divisor of $x$ and $p$ or $q$, it must be that $d = 1$. Since it was an arbitrary common divisor of $x$ and $n$, $\gcd(x,n) = 1$; hence $x \in \mathbb{Z}_n^*$ and $f$ is one-to-one. $\square$

Corollary 6.41 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 6.44. *For any* $n \in \mathbb{N}^+$, $[x^a] = [x]^a$ *in* $\mathbb{Z}_n^*$.

PROOF. You do it! See Exercise 6.52 on the following page. □

EXAMPLE 6.45. 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 6.46. *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 $q_b, q_{b-1}, \ldots, q_1, q_0$.*
(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 6.46 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 6.44 gives an added bonus.

EXAMPLE 6.47. Since $10 = 2^3 + 2^1$, we can compute

$$4^{10} = 4^{2^3 + 2^1}$$

by following the algorithm of Theorem 6.46:

(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 6.48. Compute $3^{28}$ in $\mathbb{Z}$ using fast exponentiation. Show each step.

EXERCISE 6.49. Compute $24^{28}$ in $\mathbb{Z}_7^*$ using fast exponentiation. Show each step.

EXERCISE 6.50. Prove that for all $x \in \mathbb{Z}_n^*$, $x^{\varphi(n)-1} = x^{-1}$.

EXERCISE 6.51. 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 6.52. Prove that for any $n \in \mathbb{N}^+$, $[x^a] = [x]^a$ in $\mathbb{Z}_n^*$. *Hint:* Consider the factorization of $a$ into irreducibles, and Lemma 6.30 on page 112.

## 6.5. THE RSA ENCRYPTION ALGORITHM

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 in Section 1.1: when you buy something online, you usually submit some private information, in the form either of a credit card number or a bank account number. There is no guarantee that, as this information passes through the internet, it passes through trustworthy computers. In fact, it is quite likely that the information sometimes passes through a computer run by at least one ill-intentioned hacker, and possibly even organized crime. Identity theft has emerged in the last few decades as an extremely profitable pursuit.

Given the inherent insecurity of the internet, the solution is to disguise your private information so that disreputable snoopers cannot understand it. A common method in use today is the RSA encryption algorithm.[1] First we describe the algorithms for encryption and decryption; afterwards we explain the ideas behind each stage, illustrating with an example; finally we prove that it succesfully encrypts and decrypts messages.

THEOREM 6.53 (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 that satisfy the following two criteria:*

- $\gcd(p,q) = 1$*; and*
- $(p-1)(q-1) > \max\{m : m \in M\}$.

[1]RSA stands for Rivest (of MIT), Shamir (of the Weizmann Institute in Israel), and Adleman (of USC).

*Let $N = pq$, and let $e \in \mathbb{Z}^*_{\varphi(N)}$, where $\varphi$ is the Euler phi-function. If we apply the following algorithm to $M$:*

(1) *Let $C$ be a list of positive integers found by computing the canonical representation of $[m^e] \in \mathbb{Z}_N$ 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 $\left[c^d\right] \in \mathbb{Z}_N$ for each $c \in C$.*

*then $D = M$.*

EXAMPLE 6.54. Consider the text message

ALGEBRA RULZ.

We will convert the letters to integers in the fashion that you might expect: A=1, B=2, ..., Z=26. We will also assign 0 to the space. Thus

$$M = (1, 12, 7, 5, 2, 18, 1, 0, 18, 21, 12, 26).$$

Let $p = 5$ and $q = 11$; then $N = 55$. Let $e = 3$; note that

$$\gcd(3, \varphi(N)) = \gcd(3, \varphi(5) \cdot \varphi(11)) = \gcd(3, 4 \times 10) = \gcd(3, 40) = 1.$$

We 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 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 $d = 27$ (since $3 \times 27 = 81$ and $[81] = [1]$ in $\mathbb{Z}^*_{40}$). We 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.

It does, doesn't it?. ◇

A few observations are in order.

(1) Usually encryption is not done letter-by-letter; instead, letters are grouped together and converted to integers that way. 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

$$\text{ALGE} \quad \rightarrow \quad 1 \times 26^3 + 12 \times 26^2 + 7 \times 26 + 5 = 25,785.$$

In order to encrypt this, we would need larger values for $p$ and $q$. We give an example of this 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 $e = \ldots$." Even the snooper knows $N$ and $e$!

(3) If even the snooper knows $N$ 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 $\varphi(N)$, but there is *no known method* of computing $\varphi(N)$ "quickly". If $p$ and $q$ are small, this isn't hard: one simply tries to factor $N$ and uses Lemma 6.42, which tells us that $\varphi(N) = (p-1)(q-1)$. In practice, however, $p$ and $q$ are *very* large numbers (many digits long). There is a careful science to choosing $p$ and $q$ in such a way that it is 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 $\gcd(e, \varphi(N)) = 1$, the Extended Euclidean Algorithm tells us that there exist $a, b \in \mathbb{Z}$ such that

$$1 = ae + b\varphi(N).$$

Rearranging the equation, we see that

$$1 - ae = b\varphi(N);$$

in other words, $[1 - ae] = [0] \in \mathbb{Z}_{\varphi(N)}$, so that $[1] = [a][e] \in \mathbb{Z}_{\varphi(N)}$. By definition of an inverse, $[a] = [e]^{-1} = [d] \in \mathbb{Z}^*_{\varphi(N)}$. (Notice that we omitted the star previously, but now we include it.)

Without loss of generality, $d, e > 0$, which implies that $b < 0$. Let $c = -b$. Substitution gives us

$$(m^e)^d = m^{ed} = m^{ae} = m^{1-b\varphi(N)} = m^{1+c\varphi(N)}.$$

We claim that $[m]^{1+c\varphi(N)} = [m] \in \mathbb{Z}_N$. This requires us to show two subclaims.

CLAIM (1). $[m]^{1+c\varphi(N)} = [m] \in \mathbb{Z}_p$.

If $p \mid m$, then $[m] = [0] \in \mathbb{Z}_p$, and

$$[m]^{1+c\varphi(N)} = [0]^{1+c\varphi(N)} = [0] = [m] \in \mathbb{Z}_p.$$

Otherwise, recall that $p$ is irreducible; then $\gcd(m, p) = 1$ and by Euler's Theorem on page 116

$$[m]^{\varphi(p)} = [1] \in \mathbb{Z}_p^*.$$

Thus

$$[m]^{1+c\varphi(N)} = [m] \cdot [m]^{c\varphi(N)} = [m] \left( [m]^{\varphi(N)} \right)^c = [m] \cdot [1]^c = [m] \in \mathbb{Z}_p^*.$$

What is true for $\mathbb{Z}_p^*$ is also true in $\mathbb{Z}_p$, since the former is a subset of the latter. Hence

$$[m]^{1+c\varphi(N)} = [m] \in \mathbb{Z}_p.$$

CLAIM (2). $[m]^{1+c\varphi(N)} = [m] \in \mathbb{Z}_q$.

The argument is similar to that of the first claim.

Since $[m]^{1+c\varphi(N)} = [m]$ in both $\mathbb{Z}_p$ and $\mathbb{Z}_q$, properties of the quotient groups $\mathbb{Z}_p$ and $\mathbb{Z}_q$ tell us that $\left[ m^{1+c\varphi(N)} - m \right] = [0]$ in both $\mathbb{Z}_p$ and $\mathbb{Z}_q$ as well. In other words, both $p$ and $q$ divide $m^{1+c\varphi(N)} - m$. You will show in Exercise 123 that this implies that $N$ divides $m^{1+c\varphi(N)} - m$.

From the fact that $N$ divides $m^{1+c\varphi(N)} - m$, we have $[m]_N^{1+c\varphi(N)} = [m]_N$. From the fact that we use canonical representations of the cosets, computing $(m^e)^d$ in $\mathbb{Z}_{\varphi(N)}$ gives us $m$. □

EXERCISES.

EXERCISE 6.55. 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. *Hint:* Using the Extended Euclidean Algorithm might make this go faster. The proof of the RSA algorithm outlines how to use it.
(d) Decrypt the message.

EXERCISE 6.56. 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. *Hint:* That largest number should come from encrypting ZZZZ.

(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. *Hint:* Using the Extended Euclidean Algorithm might make this go faster. The proof of the RSA algorithm outlines how to use it.
(e) Decrypt the message to verify that you did this correctly.

EXERCISE 6.57. Let $m, p, q \in \mathbb{Z}$ and suppose that $\gcd(p, q) = 1$. Show that if $p \mid m$ and $q \mid m$, then $pq \mid m$. *Hint:* 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 $ab \mid m$.

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 2

# An introduction to ring theory

CHAPTER 7

# Rings and ideals

## 7.1. RINGS

Groups are simple in the following respect: a group is defined by a set and *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.

Besides adding matrices or integers, one can also multiply matrices or integers. We can deal with multiplication independently of addition by restricting the set in certain ways—using the subset $\mathrm{GL}_m(\mathbb{R})$, for example. 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.

DEFINITION 7.1. Let $R$ be a set *with at least two elements*, and $+$ and $\times$ two 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. 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, $\mathtt{0}$. We sometimes write $\mathtt{0}_R$ to emphasize that it is the additive identity of a ring. Likewise, if there is a multiplicative identity, we write $1$ or $1_R$, *not* $e$.

Notice the following:

- While the addition is guaranteed to be commutative by (R1), we have *not* stated that multiplication is commutative. Indeed, our first example ring has non-commutative for multiplication.
- There is not 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
  - $\mathtt{0}_R\cdot a=\mathtt{0}_R$ for any $a\in R$.

EXAMPLE 7.2. 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. We pass over the details, but they can be found in any reputable linear algebra book.

We do want to emphasize the following. 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
$$\forall a, b \in R \qquad ab = 0 \quad \Longrightarrow \quad a = 0 \text{ or } b = 0.$$

◇

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 7.3. *For all $r \in R$, $r \cdot 0_R = 0_R \cdot r = 0_R$.*

PROOF. Since $(R, +)$ is an abelian group, we know that $0_R + 0_R = 0_R$. Let $r \in R$. 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 $s$. Substitution followed by the associative, inverse, and identity properties implies that

$$\begin{aligned} s + (r \cdot 0_R + r \cdot 0_R) &= s + r \cdot 0_R \\ (s + r \cdot 0_R) + r \cdot 0_R &= s + r \cdot 0_R \\ 0_R + r \cdot 0_R &= 0_R \\ r \cdot 0_R &= 0_R. \end{aligned}$$

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 7.4. 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 7.5. The set of matrices $\mathbb{R}^{m\times m}$ is a ring with unity, with the identity matrix $I_m$ as the multiplicative identity. However, it is not a commutative ring.

You will show in Exercise 7.7 that $2\mathbb{Z}$ is a ring. It is also a commutative ring, but it is not a ring with unity.

For a commutative ring with unity, we have $\mathbb{Z}$. ◇

We conclude this section by characterizing all rings with only two elements.

EXAMPLE 7.6. Let $R$ be a ring with only two elements. There are two possible structures for $R$.

*Why?* Since $(R,+)$ is an abelian group, by Section 2.1 the addition table of $R$ has the form

| $+$ | $0_R$ | $a$ |
|---|---|---|
| $0_R$ | $0_R$ | $a$ |
| $a$ | $a$ | $0_R$ |

.

By Proposition 7.3, 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 7.8 to see that this is a ring) then $a=[1]$ and $a\cdot a=a$; but
- if
$$R=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}, a=\begin{pmatrix}0&1\\0&0\end{pmatrix}\right\}\subset\left(\mathbb{Z}_2^*\right)^{2\times 2}$$
(two-by-two matrices whose entries are elements of $\mathbb{Z}_2^*$), then $a\cdot a=0\neq a$. ◇

EXERCISES.

EXERCISE 7.7. (a) Show that $2\mathbb{Z}$ is a ring under the usual addition and multiplication of integers.

(b) Show that $n\mathbb{Z}$ is a ring for all $n\in\mathbb{Z}$ under the usual addition and multiplication of integers. *Hint:* 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 7.8. (a) Show that $\mathbb{Z}_2$ is a ring under the addition and multiplication of cosets defined in Sections 3.5 and 6.3.

(b) Show that $\mathbb{Z}_n$ is a ring for all $n\in\mathbb{Z}$ where $n>1$, under the addition and multiplication of cosets defined in Sections 3.5 and 6.3.

EXERCISE 7.9. Let $R$ be a ring.

(a) Show that for all $r,s\in R$, $(-r)s=r(-s)=-(rs)$. *Hint:* This is short, but not trivial. You need to show that $(-r)s+rs=0_R$. Try using the distributive property.

(b) Suppose that $R$ has unity. Show that $-r=-1_R\cdot r$ for all $r\in R$. *Hint:* 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 7.10. Let $R$ be a ring with unity. Show that $1_R\neq 0_R$. *Hint:* 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 7.11. Consider the two possible ring structures from Example 7.6. Show that if a ring $R$ has only two elements, one of which is unity, then it can have only one of the structures. *Hint:* Use the result of Exercise 7.10.

EXERCISE 7.12. 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 2.13 and 2.14 on page 21). Is $(R, \oplus, \wedge)$ a ring? If it is a ring, what is the zero element? *Hint:* 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.

## 7.2. INTEGRAL DOMAINS AND FIELDS

Example 7.2 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 demosntrates 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 7.13. If the elements of $R$ satisfy the zero product property, then we call $R$ an **integral domain**. If on the other hand $R$ does not satisfy the zero product property, then we call any two non-zero elements $a, b \in R$ such that $ab = 0$ **zero divisors**.

EXAMPLE 7.14. Consider the ring $\mathbb{R}^{2\times 2}$; this is not an integral domain since

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{R}^{2\times 2} \quad \text{but} \quad AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Hence $A$ and $B$ are zero divisors in $\mathbb{R}^{2\times 2}$.

Although $\mathbb{R}^{m\times m}$ is not an integral domain, $\mathrm{GL}_m(\mathbb{R})$ is: Let $A, B \in \mathrm{GL}_m(\mathbb{R})$. Assume $AB = 0$ but $A \neq 0$. Thus $A^{-1}$ exists and

$$\begin{aligned} AB &= 0 \\ A^{-1}(AB) &= A^{-1} \cdot 0 \\ B &= 0. \end{aligned}$$

Since $A, B$ were arbitrary in $\mathrm{GL}_m(\mathbb{R})$, $\forall A, B \in \mathrm{GL}_m(\mathbb{R})$ if $AB = 0$ then one of $A, B$ is also the zero matrix. That is, $\mathrm{GL}_m(\mathbb{R})$ is an integral domain.

Likewise, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are integral domains, as is the polynomial ring $R[x_1, x_2, \ldots, x_n]$ whenever $R$ is itself an integral domain. ◇

DEFINITION 7.15. If every non-zero element of $R$ has a multiplicative inverse, then we call $R$ a **field**.

EXAMPLE 7.16. The rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

On the other hand, define **the set of fractions over** $R$ (a commutative ring)

$$\operatorname{Frac}(R) := \left\{ \frac{p}{q} : \ p, q \in R \text{ and } q \neq 0 \right\},$$

with addition and multiplication defined in the usual way for "fractions", and equality defined by

$$\frac{a}{b} = \frac{p}{q} \quad \Longleftrightarrow \quad aq = bp.$$

It turns out that $\operatorname{Frac}(R)$ is not a field *unless $R$ is an integral domain.*

Why do we say this? Assume that $R$ is an integral domain. First we show that $\operatorname{Frac}(R)$ is an additive group. Let $f, g, h \in R$; choose $a, b, p, q, r, s \in \operatorname{Frac}(R)$ such that $f = a/b$, $g = p/q$, and $h = r/s$.

*closure:* This is fairly routine, using common denominators and the fact that $R$ is a domain:

$$\begin{aligned} f + g &= \frac{a}{b} + \frac{p}{q} \\ &= \frac{aq}{bq} + \frac{bp}{bq} \\ &= \frac{aq + bp}{bq} \\ &\in \operatorname{Frac}(R). \end{aligned}$$

Why did we need $R$ do be an integral domain? If not, then it is possible that $bq = 0$, and if so, $f + g \notin \operatorname{Frac}(R)$!

*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:* A ring identity of $\text{Frac}(R)$ 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.

Next we have to show that $\text{Frac}(R)$ satisfies the requriments of a ring.

*closure:* Using closure in $R$ and the fact that $R$ is an integral domain, this is straightdorward: $fg=(ap)/(bq)\in\text{Frac}(R)$.

*associative:* Using the associative property of $R$, this is straightforward:

$$\begin{aligned}
(fg)h &= \left(\frac{ap}{bq}\right)\frac{r}{s}\\
&= \frac{(ap)r}{(bq)s}\\
&= \frac{a(pr)}{b(qs)}\\
&= \frac{a}{b}\frac{(pr)}{qs}\\
&= f(gh).
\end{aligned}$$

*distributive:* We rely on the distributive property of $R$:

$$\begin{aligned}
f(g+h) &= \frac{a}{b}\left(\frac{p}{q}+\frac{r}{s}\right)\\
&= \frac{a}{b}\left(\frac{ps+qr}{qs}\right)\\
&= \frac{a(ps+qr)}{b(qs)}\\
&= \frac{a(ps)+a(qr)}{b(qs)}\\
&= \frac{a(ps)}{b(qs)}+\frac{a(qr)}{b(qs)}\\
&= \frac{ap}{bq}+\frac{ar}{bs}\\
&= fg+fh.
\end{aligned}$$

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 7.22 that any element $0_R/a\in\mathrm{Frac}(R)$ is equal 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 7.22, you will show that

$$\frac{ab}{ab} = 1_{\mathrm{Frac}(R)}.\ \Diamond$$

DEFINITION 7.17. For any integral domain $R$, we call $\mathrm{Frac}(R)$ the **ring of fractions of** $R$.

NOTATION. We generally denote fields with the "blackboard bold" font: for example, we denote an arbitrary field by $\mathbb{F}$. However, not every set denoted by blackboard bold is a field: $\mathbb{N}$ and

$\mathbb{Z}$ are not fields, for example. Likewise, not every field is denoted with blackboard bold: $F$ of Example 7.16, for example.

Already in Example 7.16 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 than you might have anticipated.

THEOREM 7.18. *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 7.3 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 7.19. Explain why $n\mathbb{Z}$ is always an integral domain. Is it also a field?

EXERCISE 7.20. 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 7.21. You might think from Exercise 7.20 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 why this doesn't work.

EXERCISE 7.22. Show that if $R$ is an integral domain, then the set of fractions has the following properties for any nonzero $a \in R$:

$$\frac{0_R}{a} = \frac{0_R}{1} = 0_{\text{Frac}(R)} \qquad \text{and} \qquad \frac{a}{a} = \frac{1_R}{1_R} = 1_{\text{Frac}(R)}.$$

*Hint:* Use the definition of equality in this set given in Example 7.16.

EXERCISE 7.23. To see concretely why $\text{Frac}(R)$ is not a field if $R$ is not a domain, consider $R = \mathbb{Z}_4$. Find nonzero $b, q \in \text{Frac}(R)$ such that $bq = 0$, and use them to find $f, g \in \text{Frac}(R)$ such that $fg \notin \text{Frac}(R)$. *Hint:* For the latter part, try to find $fg$ such that $fg$ is not even defined, let alone an element of $\text{Frac}(R)$.

EXERCISE 7.24. Show that if $R$ is an integral domain, then $\text{Frac}(R)$ is the intersection of all fields containing $R$ as a subring.

## 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 7.25. Let $S$ be a set.

- An **indeterminate variable of** $S$ is a symbol that represents an arbitrary value of $S$. A **scalar of** $S$ is a symbol that represents a fixed value of $S$. Usually we refer to an indeterminate variable as simply "a variable".
- A **monomial over** $S$ is a finite product of variables of $S$.
  - The **total degree** of a monomial is the number of factors in the product.
- A **termover** $S$ is the product of a monomial over $S$ and a scalar of $S$. The scalar in a term is called the **coefficient** of the term.
- A **polynomial over** $S$ is a finite sum of terms over $S$.
  - We say that the polynomial $f$ is a **zero polynomial** if, whenever we substitute arbitrary values of $S$ for the variables, $f$ simplifies to zero.
  - We say that two polynomials $f$ and $g$ are equal if $f - g$ is a zero polynomial.
  - As with integers, we say that the polynomial $f$ **divides** the polynomial $g$, both over $S$, if there exists a polynomial $q$ over $S$ such that $g = qf$ or $g = fq$.
- $S[x]$ is the set of **univariate** polynomials in in the variable $x$ over $S$. That is, $f \in S[x]$ if and only if there exist $n \in \mathbb{N}$ and $a_m, a_{m-1}, \ldots, a_1 \in S$ such that
$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0.$$
- The set $S[x,y]$ is the set of **bivariate** polynomials in the variables $x$ and $y$ whose coefficients are in $S$.
- For $n \geq 2$, the set $S[x_1, x_2, \ldots, x_n]$ is the set of **multivariate** polynomials in the variables $x_1, x_2, \ldots, x_n$ whose coefficients are in $S$. We usually use the term bivarate when $n = 2$, but bivariate polynomials are in fact multivariate.
- The **degree** of a univariate polynomial $f$, written , is the largest exponent of a variable in $f$. Unless we say otherwise, the degree of a multivariate polynomial is undefined.

We call $R$ the **ground ring** of each set, and for any polynomial in the set, $R$ is the ground ring of the polynomial.

EXAMPLE 7.26. Definition 7.25 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 $4 \in \mathbb{Z}_6[x,y]$. $\diamondsuit$

Technically, we should write the coefficients of $f$ and $g$ with brackets, since the coefficients are cosets and not integers. However, this grows tedious quickly, so drop the practice of writing brackets altogether.

REMARK. Watch out for the following pitfalls!

(1) Polynomial rings are not always commutative. If the ground ring is non-commutative, we *cannot* assume that $x_i x_j = x_j x_i$. Think of matrices. That said, we will state explicitly

when we work with non-commutative rings. In general, we will work with integral domains.

(2) If $f$ is a zero polynomial, that does *not* imply that $f(x) = 0$; that is, that all the coefficients of $f$ are zero. Consider the following 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.*

From here on let $R$ be an integral domain. Our goal is to show that we can treat the univariate, bivariate, and multivariate polynomials over $R$ into rings. Before we can do that, we must answer an important question: when is the zero polynomial, zero?

PROPOSITION 7.27. *If $R$ is a non-zero integral domain, then the following are equivalent.*
*(A) $0$ is the only zero polynomial.*
*(B) $R$ has infinitely many elements.*

Before proving Proposition 7.27, we need the following lemma.

THEOREM 7.28 (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 7.34 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 7.27.

PROOF OF LEMMA 7.27. 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

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_m).$$

Let $a \in R$; we can set $a = r_i$ for some $i \in \{1, 2, \ldots, m\}$, and

$$f(a) = (a - r_1) \cdots (a - r_{i-1})(a - r_i)(a - r_{i+1}) \cdots (a - r_m).$$

Now $a - r_i = 0$ by the properties of a ring, and by the properties of zero $f(a) = 0$.

*(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 7.28, $x - a$ 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 factor (otherwise the degree would be too large). 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 $f = 0$.

*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 we have found elements of $R$ that, when substituted for the variables, do not simplify $f$ to zero. 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, $g = 0$. 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. $\square$

DEFINITION 7.29. To define **addition** and **multipication** for the set of univariate polynomials, let $f, g \in R[x]$ and write

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0.$$

Without loss of generality, we may assume that $m \geq n$. Define addition in $R[x]$ by

$$(f+g)(x) = a_m x^m + \cdots + a_{n+1} x^{n+1} + (a_n + b_n) x^n + \cdots + (a_0 + b_0) x^0.$$

Let $cx^\ell$ be a polynomial with only one term, and define the term multiple of a polynomial by

$$\left(cx^\ell\right) \cdot f(x) = (c \cdot a_m) x^{\ell+m} + \cdots + (c \cdot a_0) x^\ell.$$

Now define polynomial multipiclation by

$$(fg)(x) = \sum_{i=1}^{m} \left(a_i x^i\right) \cdot g(x);$$

that is, polynomial multiplication is simply the sum of the term multiples of the second polynomial with the terms of the first.

We come to the main purpose of this section.

THEOREM 7.30. *The univariate and multivariate polynomial rings over a ring $R$ are themselves rings.*

PROOF. We prove the theorem for an arbitrary univariate ring $R[x]$, noting that the results generalize easily to a multivariate ring. However, although the generalization is "easy", it is also "tedious", so we stick with the univariate case.

Let $n \in \mathbb{N}^+$ and $R$ a ring. We claim that $R[x_1, \ldots, x_n]$ is a ring, and that if $R$ is an integral domain then $R[x_1, \ldots, x_n]$ is also an integral domain. Consider the requirements of a ring in turn; we will use the following representations of polynomials to check the properties:

$$
\begin{aligned}
f(x) &= a_\ell x^\ell + \cdots + a_0 = \sum_{i=1}^{\ell} a_i x^i \\
g(x) &= b_m x^m + \cdots + b_0 = \sum_{i=1}^{m} b_i x^i \\
h(x) &= c_n x^n + \cdots + c_0 = \sum_{i=1}^{n} c_i x^i .
\end{aligned}
$$

We may assume, without loss of generality, that $a_i = b_j = c_k = 0$ for $i > \ell, j > m, k > n$.

(R1) First we show that $R[x_1, \ldots, x_n]$ is an abelian group.

(G1) By the definition of polynomial addition, $(f+g)(x) = \sum_{i=1}^{\max(\ell,m)} (a_i + b_i) x^i$. Since $R$ is closed under addition, $f + g \in R[x_1, \ldots, x_n]$.

(G2) We rely on the associative property of $R$:

$$
\begin{aligned}
(f+(g+h))(x) &= \sum_{i=1}^{\ell} a_i x^i + \sum_{j=1}^{\max(m,n)} \left(b_j + c_j\right) x^j \\
&= \sum_{i=1}^{\max(\ell,m,n)} \left[a_i + (b_i + c_i)\right] x^i \\
&= \sum_{i=1}^{\max(\ell,m,n)} \left[(a_i + b_i) + c_i\right] x^i \\
&= \sum_{i=1}^{\max(\ell,m)} (a_i + b_i) x^i + \sum_{j=1}^{n} c_j x^j \\
&= ((f+g)+h)(x) .
\end{aligned}
$$

(G3) We claim that $0$ is the identity. We can write $0 = 0x^\ell + \cdots + 0x + 0$, and then

$$
\begin{aligned}
(f+0)(x) &= \sum_{i=1}^{\ell} a_i x^i + \sum_{i=1}^{\ell} 0 \cdot x^i \\
&= \sum_{i=1}^{\ell} (a_i + 0) x^i \\
&= \sum_{i=1}^{\ell} a_i x^i \\
&= f(x) .
\end{aligned}
$$

(G4) Let $p = \sum_{i=1}^{\ell} (-a_i) x^i$. We claim that $p$ is the additive inverse of $f$. In fact,

$$\begin{aligned}(p+f)(x) &= \sum_{i=1}^{\ell} (-a_i) x^i + \sum_{i=1}^{\ell} a_i x^i \\ &= \sum_{i=1}^{\ell} (-a_i + a_i) x^i \\ &= \sum_{i=1}^{\ell} 0 \cdot x^i \\ &= 0.\end{aligned}$$

(G5) By the definition of polynomial addition, $(g+f)(x) = \sum_{i=1}^{\max(\ell,m)} (b_i + a_i) x^i$. Since $R$ is commutative under addition, $g + f = f + g$. Notice that we are using implicitly the fact that $(g+f) - (f+g) = 0$.

(R2) Applying the definitions of polynomial and term multiplication, we have

$$\begin{aligned}(fg)(x) &= \sum_{i=1}^{\ell} \left[ \left(a_i x^i\right) \cdot g(x) \right] \\ &= \sum_{i=1}^{\ell} \left[ \left(a_i x^i\right) \cdot \left( \sum_{j=1}^{m} b_j x^j \right) \right] \\ &= \sum_{i=1}^{\ell} \sum_{j=1}^{m} \left[ \left(a_i x^i\right) \cdot \left(b_j x^j\right) \right] \\ &= \sum_{i=1}^{\ell} \sum_{j=1}^{m} \left(a_i b_j\right) x^{i+j}.\end{aligned}$$

Since $R$ is closed under multiplication, each $\left(a_i b_j\right) x^{i+j}$ 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):

$$\begin{aligned}((fg)h)(x) &= \left( \left( \sum_{i=1}^{\ell} a_i x^i \right) \cdot \left( \sum_{j=1}^{m} b_j x^j \right) \right) \cdot \left( \sum_{k=1}^{n} c_k x^k \right) \\ &= \left( \sum_{i=1}^{\ell} \sum_{j=1}^{m} \left(a_i b_j\right) x^{i+j} \right) \cdot \left( \sum_{k=1}^{n} c_k x^k \right) \\ &= \sum_{i=1}^{\ell} \sum_{j=1}^{m} \sum_{k=1}^{n} \left( \left(a_i b_j\right) c_k \right) x^{(i+j)+k}.\end{aligned}$$

Now apply the associative property of multiplication in $R$ and the associative property of addition in $\mathbb{Z}$:

$$((fg)h)(x) = \sum_{i=1}^{\ell}\sum_{j=1}^{m}\sum_{k=1}^{n}\left(a_i\left(b_jc_k\right)\right)x^{i+(j+k)}.$$

Now unapply the form of a product that we derived in (R2):

$$\begin{aligned}((fg)h)(x) &= \left(\sum_{i=1}^{\ell}a_ix^i\right)\cdot\left(\sum_{j=1}^{m}\sum_{k=1}^{n}\left(b_jc_k\right)x^{j+k}\right)\\ &= \left(\sum_{i=1}^{\ell}a_ix^i\right)\cdot\left(\left(\sum_{j=1}^{m}b_jx^j\right)\cdot\left(\sum_{k=1}^{n}c_kx^k\right)\right)\\ &= (f(gh))(x).\end{aligned}$$

(R4) To analyze, $f(g+h)$, we first apply addition, then multiplication:

$$\begin{aligned}(f(g+h))(x) &= \left(\sum_{i=1}^{\ell}a_ix^i\right)\cdot\left(\sum_{j=1}^{m}b_jx^j+\sum_{k=1}^{n}c_kx^k\right)\\ &= \left(\sum_{i=1}^{\ell}a_ix^i\right)\cdot\left(\sum_{j=1}^{\max(m,n)}\left(b_j+c_j\right)x^j\right)\\ &= \sum_{i=1}^{\ell}\sum_{j=1}^{\max(m,n)}\left[a_i\left(b_j+c_j\right)\right]x^{i+j}.\end{aligned}$$

Now apply the distributive property in the ring, and unapply the addition and multiplication:

$$\begin{aligned}(f(g+h))(x) &= \sum_{i=1}^{\ell}\sum_{j=1}^{\max(m,n)}\left(a_ib_j+a_ic_j\right)x^{i+j}\\ &= \sum_{i=1}^{\ell}\sum_{j=1}^{\max(m,n)}\left(a_ib_j\right)x^{i+j}+\sum_{i=1}^{\ell}\sum_{j=1}^{\max(m,n)}\left(a_ic_j\right)x^{i+j}\\ &= \left(\sum_{i=1}^{\ell}a_ix^i\right)\cdot\left(\sum_{j=1}^{\max(m,n)}b_jx^j\right)+\left(\sum_{i=1}^{\ell}a_ix^i\right)\cdot\left(\sum_{j=1}^{\max(m,n)}c_jx^j\right).\end{aligned}$$

Remembering that $b_j = c_k = 0$ for $j > m, k > n$, we conclude that

$$(f(g+h))(x) = (fg)(x) + (fh)(x),$$

as desired.

□

We will separate into another theorem the consequence for integral domains.

THEOREM 7.31. *If $R$ is an integral domain, then any univariate or multivariate polynomial ring over $R$ is also an integral domain.*

PROOF. As with rings, we restrict ourselves to the univariate case. Assume that $R$ is an integral domain. Let $f, g \in R[x]$; we must show that if $fg = 0$, then $f = 0$ or $g = 0$. Assume that $fg = 0$; that is, $fg$ is the zero polynomial. In other words, every coefficients of $fg$ is zero.

Write

$$f = \sum_{i=1}^{m} a_i x^i \quad \text{and} \quad g = \sum_{j=1}^{n} b_j x^j.$$

Assume $f \neq 0$. At least one of its terms is non-zero. Recall from the proof of Theorem 7.30 that

$$(fg)(x) = \sum_{i=1}^{m}\sum_{j=1}^{n} \left(a_i b_j\right) x^{i+j},$$

so

$$0 = \sum_{\substack{i=1\dots m\\ a_i\neq 0}} \sum_{\substack{j=1\dots n\\ b_j\neq 0}} \left(a_i b_j\right) x^{i+j}. \tag{7.3.1}$$

Consider the lowest-degree term $t$ with nonzero coefficient of $f$. Let $u$ be any term of $g$; we claim that the coefficient of $u$ is zero. Proceed by induction on the degree $k$ of $u$. Denote the degree of $t$ by $d$, so the coefficent of $t$ is $a_d$. By assumption, $a_d = 0$ and $a_i = 0$ whenever $0 \leq i < d$.

*Inductive base:* Let $k = 0$. We have $\deg tu = \deg t$. For any other nonzero term $w$ in $f$, and for any other term $v$ in $g$,

$$\deg wu = \deg w + \deg u > \deg t + \deg u = \det tu$$

and

$$\deg wv = \deg w + \deg v > \deg t + \deg v \geq \deg t + \deg u = \deg tu.$$

Thus $tu$ is only product in the right hand side of (7.3.1) of degree $\deg t$. Applying the definition of an integral domain, and the fact that $a_d \neq 0$,

$$a_d b = 0 \quad \Longrightarrow \quad b = 0.$$

*Inductive hypothesis:* Assume that for all $\ell < k$, $b_\ell = 0$.

*Inductive step:* Consider the term $\sum_{\alpha+\beta=k+d} \left(a_\alpha b_\beta\right) x^{k+d}$ in the right hand side of (7.3.1). Since $d$ is the smallest nonzer index of $\alpha$ in this term, all other values of $\alpha$ of interest are larger than $d$, implying that all values of $\beta$ are smaller than $k$. The inductive hypothesis implies that $b_\beta = 0$ for all of these, so the term simplifies to $a_d b_k$. Recall that this term is zero, because $fg$ is the zero polynomial. Since $a_d \neq 0$ and $R$ is an integral domain, $b_k = 0$.

We have shown by inducation that all the coefficients of $g$ are zero. Thus $g$ is the zero polynomial. Since $f$ and $g$ were arbitrary polynomials in $R[x]$, and the assumption $fg = 0$ forced one of the two to be zero, $R[x]$ is an integral domain. □

EXERCISES.

EXERCISE 7.32. Let $f(x) = x^2 + x$ and $g(x) = x + 1$ in $\mathbb{Z}_2[x]$.

(a) Compute the polynomial $p = fg$.
(b) Show that $p(x) = 0$ for every $x \in \mathbb{Z}_2$.
(c) Explain why this does *not* contradict Proposition 7.27.

EXERCISE 7.33. 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 7.34. 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 $f(x) = q(x) \cdot (x - a) + r$. *Hint:* Proceed by induction on $\deg f$.

EXERCISE 7.35. Let $R$ be a ring and define

$$R(x) = \operatorname{Frac}(R[x]);$$

for example,

$$\mathbb{Z}(x) = \operatorname{Frac}(\mathbb{Z}[x]) = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}[x] \right\}.$$

Is $R(x)$ a ring? is it a field?

## 7.4. EUCLIDEAN DOMAINS AND A GENERALIZED EUCLIDEAN ALGORITHM

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 domain, and therefore 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*.

THEOREM 7.36. *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)* $\deg r < \deg f$.

*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* $n = 0$, let $q = \frac{\text{lc}\,g}{\text{lc}\,f}$; and $r = g - qf$. The degree of $r$ is the degree of $g - qf$. Since $\deg g = \deg f = m$, there exist $a_m, \ldots, a_1, b_m, \ldots, b_1 \in R$ such that

$$\begin{aligned} g &= a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \\ f &= b_m x_m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0. \end{aligned}$$

Apply substitution, ring distribution, and the definition of 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 $\deg r < \deg f$.

For the *inductive hypothesis*, assume that for all $i < n$ there exist $q, r \in R[x]$ such that $g = qf + r$ and $\deg r < \deg f$.

For the *inductive step*, let $q_o = \frac{\text{lc}\,g}{\text{lc}\,f} \cdot x^n$ and $r_0 = g - q_0 f$. Let $\ell = \deg f$ and $m = \deg f$; by definition of degree, there exist $a_\ell, \ldots, a_0, b_m, \ldots, b_0 \in R$ such that

$$\begin{aligned} f &= a_\ell x^\ell + \cdots + a_0 \\ g &= b_m x^m + \cdots + b_0. \end{aligned}$$

Apply substitution and ring distribution to obtain

$$\begin{aligned} r_0 &= g - q_0 f \\ &= \left(a_\ell x^\ell + \cdots + a_0\right) - \frac{a_\ell}{b_m} \cdot x^n \left(b_m x^m + \cdots + b_0\right) \\ &= \left(a_\ell x^\ell + \cdots + a_0\right) - \left(a_\ell x^{m+n} + \frac{a_\ell b_{m-1}}{b_m} \cdot x^{m-1+n} + \cdots + \frac{a_\ell b_0}{b_m} \cdot x^n\right). \end{aligned}$$

Recall that $n = \deg g - \deg f = m - \ell$. Apply substitution and the definition of polynomial addition to obtain

$$\begin{aligned} r_0 - q_0 f &= \left(a_\ell x^\ell + \cdots + a_0\right) - \left(a_\ell x^\ell + \frac{a_\ell b_{m-1}}{b_m} \cdot x^{\ell-1} + \cdots + \frac{a_\ell b_0}{b_m} \cdot x^n\right) \\ &= 0x^\ell + \left(a_{\ell-1} - \frac{a_\ell b_{m-1}}{b_m}\right) x^{\ell-1} + \cdots + \left(a_n - \frac{a_\ell b_0}{b_m}\right) x^n + a_{n-1} x^{n-1} \cdots + a_0. \end{aligned}$$

Observe that $\deg r_0 < n$. By the inductive hypothesis, there exist $q_1, r_1 \in R[x]$ such that $r_0 = q_1 f + r_1$ and $\deg r_1 < \deg f$. By substitution,

$$\begin{aligned} g &= q_0 f + r_0 \\ &= q_0 f + (q_1 f + r_1) \\ &= (q_0 f + q_1 f) + r_1 \\ &= (q_0 + q_1) f + r_1. \end{aligned}$$

Put $q = q_0 + q_1$ and $r = r_1$ and we have satisfied everything in the theorem except uniqueness.

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

$$\begin{aligned} q_1 f + r_1 &= q_2 f + r_2 \\ 0 &= (q_2 - q_1) f + (r_2 - r_1). \end{aligned}$$

We know from linear algebra (or earlier) that if two polynomials are equal, then the coefficients of like terms are equal. Here the two polynomials that are equation are $0$ and $(q_2 - q_1) f + (r_2 - r_1)$. Every term of $(q_2 - q_1) f$ has degree no smaller than $\deg f$, and every term of $(r_2 - r_1)$ has degree smaller than $\deg f$, so we deduce that

$$(q_2 - q_1) f = 0 \quad \text{and} \quad r_2 - r_1 = 0.$$

Immediately we have $r_1 = r_2$. The facts that (1) $R[x]$ is a domain *in this case* and (2) $f \neq 0$ imply that $q_2 - q_1 = 0$, and thus $q_1 = q_2$. That is, $q$ and $r$ are unique. □

We did *not* list $\mathbb{Z}$ as one of the rings of the theorem. Exercise 7.33 explains why. So that's a shame: for some integral domains, we can perform a division, 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 7.37. Let $R$ be a commutative ring with unity 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 $v(r) \leq v(f)$.

If $f, g \in R$ are such that $g \neq 0$ and $f = qg$ for some $q \in R$, then we say that $g$ **divides** $f$.

EXAMPLE 7.38. Both $\mathbb{Z}$ and $R[x]$ of Theorem 7.36 are Euclidean domains.
- In $\mathbb{Z}$, the valuation function is $v(r) = |r|$.
- In $R[x]$ above, the valuation function is $v(r) = \deg r$. ◇

If you think about it, you will see for *any* field $\mathbb{F}$, the ring $\mathbb{F}[x]$ is a Euclidean domain.

THEOREM 7.39. *Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a Euclidean domain.*

PROOF. You do it! See Exercise 7.47. □

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 loosen our notion of uniqueness for the greatest common divisor.

DEFINITION 7.40. 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 7.41. In $\mathbb{Q}[x]$, $x+1$ is a greatest common divisor of $2x^2-2$ and $2x^2+4x+2$. However, $2x+2$ is also a greatest common divisor of $2x^2-2$ and $2x^2+4x+2$, and so is $\frac{x+1}{3}$. ◇

However, they do have something in common.

PROPOSITION 7.42. *Let $R$ be a Euclidean domain with respect to $v$, and $a, b \in R$. Suppose that $d$ and $d'$ are both greatest common divisors 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 the properties of the valuation function,

$$v(d') \le v(qd') = v(d).$$

On the other hand, $d'$ is also a greatest common divisor of $a$ and $b$ , and $d$ is a common divisor. An argument similar to the one above shows that

$$v(d) \le v(d') \le v(d).$$

Hence $v(d) = v(d')$. □

The reader may be wondering why we stopped at proving that $v(d) = v(d')$, and not that $d = d'$. The reason is that we *cannot* show that.

EXAMPLE 7.43. Consider $x^2-1, x^2+2x+1 \in \mathbb{Q}[x]$. Recall from Theorem 7.36 and Definition 7.37 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 $\deg(2x+2) = \deg(x+1)$. ◇

Finally we come to the point of a Euclidean domain: we can use the Euclidean algorithm to compute the gcd of any two elements! Essentialyl we transcribe the Euclidean Algorithm for integers (Theorem 6.5 on page 103 of Section 6.1).

THEOREM 7.44 (The Euclidean Algorithm for Euclidean domains). *Let $R$ be a Euclidean domain and $m, n \in R$. One 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* $\gcd(m,n)$.

PROOF. You do it! See Exercise . □

We conclude by pointing out that, 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.

EXERCISES.

EXERCISE 7.45. 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? *Hint:* $\mathbb{Z}[x]$ 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 7.46. Show that every field is a Euclidean domain. *Hint:* Since it's a field, you should never encounter a remainder, so finding a valuation function should be easy.

EXERCISE 7.47. Prove Theorem 7.39. *Hint:* 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 7.36 carefully.

EXERCISE 7.48. Prove Theorem 7.44, the Euclidean Algorithm for Euclidean domains. *Hint:* For correctness, you will need to show something similar to Lemma 6.7 on page 104. Remember, however, that there is not necessarily a unique gcd if the Euclidean domain is not $\mathbb{Z}$.

EXERCISE 7.49. A famous Euclidean domain is the ring of *Gaussian integers*

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

where $i^2 = -1$. We can turn this ring into a Euclidean domain using the valuation function

$$v(a + bi) = a^2 + b^2.$$

To find a quotient, you must use the fact that the smallest distance between $a + bi$ and other complex number is at most $\frac{1}{2}\sqrt{2\left(a^2 + b^2\right)}$. ...I need to finish this problem.

## 7.5. IDEALS

Just as groups have subgroups, rings have subrings:

DEFINITION 7.50. Let $R$ be a ring, and $S \subset R$. If $S$ is also a ring under the same operations as $R$, then $S$ is a subring of $R$.

EXAMPLE 7.51. Recall from Exercise 7.7 that $2\mathbb{Z}$ is a ring. It is also a subset of $\mathbb{Z}$, another ring. Hence $2\mathbb{Z}$ 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, but to two properties:

THEOREM 7.52 (The Subring Theorem). *Let $R$ be a ring and $S \subset R$. 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 (Theorem 3.5 on page 42) 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 that 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 cosets. No, actually: although we are moving to something called a "quotient ring", and we will build an analogue of cosets, we won't do it with subrings! Instead, we will use a special class of subrings called *ideals*.

DEFINITION 7.53. Let $A$ be a subring of $R$ that satisfies the **absorption property**:

$$\forall r \in R\ \forall a \in A \quad ra, ar \in A.$$

(If $R$ is commutative, it suffices to show that $ra \in A$.) We say that $A$ is an **ideal subring** of $R$, or simply, an **ideal**. We write $A \triangleleft R$.

An ideal $A$ is **proper** if $A \neq R$.

EXAMPLE 7.54. 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 7.61 and 7.62. ◇

Ideals in the ring of integers have a nice property that we will use quite a bit in future examples.

LEMMA 7.55. *Let $a, b \in \mathbb{Z}$. The following are equivalent:*

*(A) $a \mid b$;*
*(b) $b\mathbb{Z} \subset a\mathbb{Z}$.*

PROOF. You do it! See Exercise 7.63. □

EXAMPLE 7.56. 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 verifies that $6\mathbb{Z} \subset 3\mathbb{Z}$.

That said, we can prove this: 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 $6\mathbb{Z} \subset 3\mathbb{Z}$. ◇

The absorption property of ideals distinguishes them from other subrings, and makes them useful for applications.

EXAMPLE 7.57. Let $\mathbb{C}[x, y]$ be the set of all polynomials in $x$ and $y$ with complex coefficients. You showed in Exercise 7.3 that this is a ring.

Now 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 by definition of $A$ 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
  - $a - b = (h_a f + k_a g) - (h_b f + k_b g) = (h_a - h_b)\, f + (k_a - k_b)\, g \in A$; and
  - $ab = (h_a f + k_a g)(h_b f + k_b g) = h_a h_b f^2 + h_a k_b f g + h_b k_a f g + k_a k_b g^2 = h' f + k' g$ where

    $$h' = h_a h_b f + h_a k_b g + h_b k_a g \quad \text{and} \quad k' = k_a k_b g,$$

    which shows that $ab$ has the form of an element of $A$. Thus $ab \in A$ 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

  $$ra = r\,(h_a f + k_a g) = (r h_a)\, f + (r k_a)\, g = h' f + k' g$$

  where $h' = r h_a$ and $k' = r k_a$. This shows that $ra$ has the form of an element of $A$, so $ra \in A$.

We have shown that $A$ satisfies the subring and absorption properties; thus, $A \triangleleft \mathbb{C}[x, y]$.

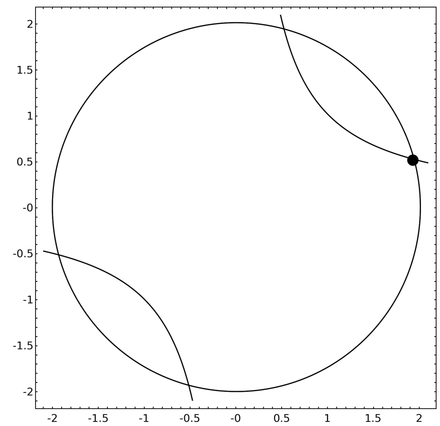
What's most interesting about $A$ is the following algebraic fact: *the common roots of $f$ and $g$ are roots of any element of $A$.* To see this, let $(\alpha, \beta)$ be a common root of $f$ and $g$; that is, $f(\alpha, \beta) = g(\alpha, \beta) = 0$. Let $p \in A$; by definition of $A$ we can write $p = hf + kg$ for some $h, k \in \mathbb{C}[x, y]$. Substitution shows us that

$$\begin{aligned} p(\alpha, \beta) &= (hf + kg)(\alpha, \beta) \\ &= h(\alpha, \beta) \cdot f(\alpha, \beta) + k(\alpha, \beta) \cdot g(\alpha, \beta) \\ &= h(\alpha, \beta) \cdot 0 + k(\alpha, \beta) \cdot 0 \\ &= 0; \end{aligned}$$

that is, $(\alpha, \beta)$ is a root of $p$.

To elaborate, a common root of $f$ and $g$ is $(\alpha, \beta) = \left(\sqrt{2 + \sqrt{3}}, 2\sqrt{2 + \sqrt{3}} - \sqrt{6 + 3\sqrt{3}}\right)$. (See Figure 7.1.) It is also a common root of every element of $A$. ◇

FIGURE 7.1. A common root of $x^2+y^2-4$ and $xy-1$




You will show in Exercise 7.69 that the ideal of Example 7.57 can be generalized to other rings and larger numbers of variables.

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 7.57 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 conclude with a theorem that allows us to decide easily if a subset of a ring is an ideal.

THEOREM 7.58 (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 7.64. □

We conclude by defining a special kind of ideal, with a notation similar to that of cyclic subgroups, but with a different meaning.

DEFINITION 7.59. Let $R$ be a commutative ring with unity and $r_1, r_2, \dots, r_m \in R$. Define the ideal $\langle r_1, r_2, \dots, r_m \rangle$ as the intersection of all the ideals of $R$ that contain all of $r_1, r_2, \dots, r_m$. We call $\langle r_1, r_2, \dots, r_m \rangle$ the **ideal generated by** $r_1, r_2, \dots, r_m$.

PROPOSITION 7.60. *The ideal $\langle r_1, r_2, \dots, r_m \rangle$ is precisely the set*

$$I = \{h_1 r_1 + h_2 r_2 + \cdots + h_m r_m : h_i \in R\}.$$

PROOF. It is evident from the definition of an ideal and the closure of a subring that

$$I \subseteq \langle r_1, \dots, r_m \rangle,$$

so it remains to show the reverse inclusion. This follows from the fact 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

$$x = h_1 r_1 + \cdots + h_m r_m \text{ and}$$
$$y = p_1 r_1 + \cdots + p_m r_m.$$

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

$$\begin{aligned} x - y &= (f_1 r_1 + \cdots + f_m r_m) - (p_1 r_1 + \cdots + p_m r_m) \\ &= (f_1 r_1 - p_1 r_1) + \cdots + (f_m r_m - p_m r_m) \\ &= (f_1 - p_1)\, r_1 + \cdots + (f_m - p_m)\, r_m \\ &\in I. \end{aligned}$$

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

$$r_i = 1 \cdot r_i + \sum_{j \neq i} 0 \cdot r_j \in I.$$

Since it is a subset of $\langle r_1, \ldots, r_m \rangle$, the *smallest* ideal containing the $r_i$, the two must be equal. □

EXERCISES.

EXERCISE 7.61. Show that for any $n \in \mathbb{N}^+$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

EXERCISE 7.62. Show that every ideal $A$ of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

EXERCISE 7.63. Prove Lemma 7.55.

EXERCISE 7.64. Prove Theorem 7.58 (the Ideal Theorem).

EXERCISE 7.65. Suppose that $R$ is a ring with unity, and $A$ is an ideal. Show that if $1_R \in A$, then $A = R$.

EXERCISE 7.66. Explain why, in the ring of square matrices, the smallest ideal containing the invertible matrices is the ring itself.

EXERCISE 7.67. Show that in any field $\mathbb{F}$, the only two distinct ideals are the zero ideal and $\mathbb{F}$ itself.

EXERCISE 7.68. 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) $AI = \{xy : x \in A, y \in I\}$

EXERCISE 7.69. Let $R$ be a commutative ring with unity. Recall from Section 7.3 the polynomial ring $R[x_1, x_2, \ldots, x_n]$, whose ground ring is $R$. 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 7.57 showed that the set $A = \left\langle x^2 + y^2 - 4, xy - 1 \right\rangle$ was an ideal; Proposition 7.60 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 $I$.

## 7.6. PRIME AND MAXIMAL IDEALS

Two important classes of ideals are *prime* and *maximal* ideals. Let $R$ be a ring.

DEFINITION 7.70. An ideal $A$ of $R$ is a **maximal ideal** if every proper ideal $I$ of $R$ satisfies $I \subset A$.

EXAMPLE 7.71. In Exercise 7.62 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 $\{0\}$ is not a proper ideal.

We claim that $n$, is not divisible by any integers except $\pm 1, \pm n$. To see this, recall Lemma 7.55: if some $m \in \mathbb{Z}$ is a divisor of $n$, then $n\mathbb{Z} \subset m\mathbb{Z}$. Since $n\mathbb{Z}$ is maximal, we must have $m\mathbb{Z} = \mathbb{Z}$, so $m = \pm 1$, or $m = n\mathbb{Z}$, so $m = \pm n$. Hence $n$ is irreducible, and by Theorem 6.28 it is a prime integer. $\diamondsuit$

For prime ideals, you need to recall from Exercise 7.68 that for any two ideals $A, B$ of $R$, $AB$ is also an ideal.

DEFINITION 7.72. An ideal $P$ of $R$ is a **prime ideal** if for every two ideals $A, B$ of $R$ we know that

$$\text{if } AB \subset P \text{ then } A \subset P \text{ or } B \subset P.$$

Definition 7.72 should remind you of our definition of prime integers from page 6.26. In fact, we can illustrate the definition of prime integers using prime ideals.

EXAMPLE 7.73. 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 7.55 tells us that $(ab)\mathbb{Z} \subset p\mathbb{Z}$. 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 $AB \subset P$.

Recall that $p \mid a$; applying Lemma 7.55 again, we have $A = a\mathbb{Z} \subset p\mathbb{Z} = P$.

Conversely, if $n$ is not prime, it does not follow that $n\mathbb{Z}$ is a prime ideal: for example, $6\mathbb{Z}$ is not a prime ideal because $(2\mathbb{Z})(3\mathbb{Z}) \subset 6\mathbb{Z}$ but by Lemma 7.63 neither $2\mathbb{Z} \subset 6\mathbb{Z}$ nor $3\mathbb{Z} \subset 6\mathbb{Z}$. This can be generalized easily to all integers that are not prime: see Exercise 7.77. $\diamondsuit$

You might wonder if the relationship found in Example 7.71 works the other way. That is: we found in Example 7.71 that an ideal in $\mathbb{Z}$ is maximal iff it is generated by a prime integer, and in Example 7.73 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 7.74. *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 $AB \subset M$. We claim that $A \subset M$ or $B \subset M$ .

Assume that $A \not\subset M$; we show that $B \subset M$. Recall from Exercise 7.68 that $A + M$ is also an ideal. Since $M$ is maximal, $A + M = M$ or $A + M = R$. Since $A \not\subset M$, $A + M \neq M$; thus $A + M = R$. Since $R$ has unity, $1_R \in R = A + M$, so there exist $a \in A$, $m \in M$ such that

$$1_R = a + m. \tag{7.6.1}$$

Let $b \in B$ and multiply both sides of 7.6.1 on the right by $b$; we have

$$\begin{aligned} 1_R \cdot b &= (a + m)\, b \\ b &= ab + mb. \end{aligned}$$

Recall that $AB \subset M$; 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 $B$, $B \subset M$. □

THEOREM 7.75. *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 $R$:

*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, $rx = 4(xq) \in 4\mathbb{Z}$.

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 $4\mathbb{Z} \subsetneq 2\mathbb{Z}$. Let $x \in A \backslash 4\mathbb{Z}$; by division, $x = 4q + r$ such that $0 < r < 3$. Since $r \in 2\mathbb{Z}$, we know 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, $2 \in A$. Since $A$ is a subring, and thus closed under addition, $2n \in A$ 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 $A = 2\mathbb{Z}$. Thus $4\mathbb{Z}$ is maximal in $2\mathbb{Z}$.

Finally, we show that $4\mathbb{Z}$ is not prime. This is easy, however: $(2\mathbb{Z})(2\mathbb{Z}) \subseteq 4\mathbb{Z}$, but $2\mathbb{Z} \not\subseteq 4\mathbb{Z}$. □

THEOREM 7.76. *A prime ideal is not necessarily maximal, even in a ring with unity.*

PROOF. Recall that $R = \mathbb{C}[x, y]$ is a ring, and that $I = \langle x \rangle$ is an ideal of $R$.

We claim that $I$ is a prime ideals of $R$. Let $A, B$ be ideals of $R$ such that $AB \subset I$. Suppose that $A \not\subset I$; let $a \in I \backslash A$. Now for any $b \in B$, $ab \in \langle x \rangle$, which implies that $x \mid ab$; let $q \in R$ such that $xq = ab$. 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 $x$. Observe that $f \cdot x, g \cdot x \in \langle x \rangle$. Then

$$\begin{aligned} ab &= (f \cdot x + a')(g \cdot x + b') \\ qx &= (f \cdot x) \cdot (g \cdot x) + a' \cdot (g \cdot x) + b' \cdot (f \cdot x) + a' \cdot b' \\ (q - fg - a'g - b'f)\, x &= a'b'. \end{aligned}$$

Hence $a'b' \in \langle x \rangle$, but since no term of $a'$ or $b'$ is a multiple of $x$, no term of $a'b'$ is a multiple of $x$. Hence $a'b' = 0$, which by the zero product property of complex numbers implies that $b' = 0$. Hence $b = gx \in \langle x \rangle = I$. Since $b$ is arbitrary, this holds for all $b \in B$; that is, $B \subset I$. We took two arbitrary ideals such that $AB \subset I$ and showed that $A \subset I$ or $B \subset I$; hence $I = \langle x \rangle$ is prime.

However, $I$ is not maximal, since $\langle x \rangle \subsetneq \langle x, y \rangle \subsetneq \mathbb{C}[x, y]$: the latter inequality follows since $1 \notin \langle x, y \rangle$. □

CHAPTER EXERCISES.

EXERCISE 7.77. Let $n \in \mathbb{Z}$ be an integer that is not prime. Show that $n\mathbb{Z}$ is not a prime ideal. *Hint:* Follow the argument of Example 7.73.

EXERCISE 7.78. 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 7.79. Find all the maximal ideals of $\mathbb{Z}_{12}$. Are they prime? How do you know?

EXERCISE 7.80. Let $a_1, a_2 \ldots, a_n \in R$.

(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 $R[x_1, x_2, \ldots, x_n]$.

(b) Use Exercise 7.69 to describe what the common root(s) of this ideal.

## 7.7. 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 7.81. *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 defined 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 is a ring under these operations, called the* ***quotient ring****.*

NOTATION. When we consider $X \in R/A$, we will refer to the "usual representation" of $X$ to be $x + A$ for appropriate $x \in R$; that is, "big" $X$ is represented by "little" $x$.

Of course, usually 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 7.81 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 3.27 on page 48; before proving Theorem 7.81 we need a similar property for the classes $x + A$ of $R/A$.

LEMMA 7.82. *Let $X, Y \in R/A$ with representations $X = x + A$ and $Y = y + A$ for appropriate $x, y \in R$. Then $X = Y$ if and only if $x - y \in A$.*

PROOF. You do it! See Exercise 7.87. □

We now turn to the proof of Theorem 7.81.

REMARK. We only consider multiplication on the left in the the proof of Theorem 7.81. Strictly speaking, this is correct only for commutative rings, and the statement of the theorem is about non-commutative rings as well. Careful examination of the proofs will show that we do not actually *use* the commutative property in manipulating products, so that in non-commutative rings "a similar argument" will show the properties for multiplication on the right as well. It is tedious to write this, so we omit it, but the reader should think about this as he studies the proofs, and should write out the arguments for multiplication on the right.

PROOF OF THEOREM 7.81. First we show that the operations are well-defined. Let $X, Y \in R/A$ and suppose that $X$ has two representations $w + A, x + A$ while $Y = y + A$ for appropriate $w, x, y \in R$. Is addition well-defined? Let $z \in X + Y$; then

$$z \in (x + A) + (y + A) = (x + y) + A,$$

which implies that $z = (x + y) + a$ for some $a \in A$. Using the associative and commutative properties of addition in $R$, we can rewrite $z$ as $z = y + (x + a)$. Now, $x + a \in x + A = w + A$, so we can write $x + a = w + a'$ for some $a' \in A$. Thus

$$z = y + (w + a') = (y + w) + a' = (w + y) + a' \in (w + y) + A = (w + A) + (y + A).$$

Since $z$ was arbitrary, we have shown that $(x + A) + (y + A) \subseteq (w + A) + (y + A)$; a similar argument shows that $(x + A) + (y + A) \supseteq (w + A) + (y + A)$, so that

$$(x + A) + (y + A) = (w + A) + (y + A).$$

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.

Multiplication is a little trickier; we need to use the distributive property of the ring's multiplication. Let

$$z \in (x + A)(y + A) = (xy) + A,$$

so that $z = xy + a_0$ for some $a_0 \in A$. Adding the additive inverse of $xy$ to both sides, we see that $z - xy = a_0$. Now consider $z - wy$; distribution and substitution give us

$$\begin{aligned} z - wy &= z + 0 - wy \\ &= z - xy + xy - wy \\ &= a_0 + (x - w)y. \end{aligned}$$

Now $x + A = w + A$, so by Lemma 7.82 $x - w = a_1$ for some $a_1 \in A$. Hence

$$z - wy = a_0 + a_1 y.$$

Since $A$ is an ideal, $a_1 y \in A$, so $a_1 y = a_2$ for some $a_2 \in A$. By substitution and closure,

$$z - wy = a_0 + a_2 \in A.$$

This implies that $z - wy = a_3$ for some $a_3 \in A$, and rewriting this we have $z = wy + a_3$, or in other words

$$z \in (wy) + A = (w + A)(y + A).$$

Since $z$ was arbitrary in $(x + A)(y + A)$, it follows that $(x + A)(y + A) \subseteq (w + A)(y + A)$. A similar arguments shows that $(x + A)(y + A) \supseteq (w + A)(y + A)$, so that

$$(x + A)(y + A) = (w + A)(y + A).$$

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 now turn to showing that it 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, $X + Y = (x + y) + A$, so that $X + Y \in R/A$.

*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 $R/A$. Let $X \in R/A$ with the usual representation. Indeed, substitution and the additive identity of $R$ demonstrate this:

$$\begin{aligned}X+A &= (x+0)+A\\ &= x+A\\ &= X.\end{aligned}$$

*inverse:* Let $X \in R/A$ with the usual representation. We claim that $-x + A$ is the additive inverse of $X$. Indeed,

$$\begin{aligned}X+(-x+A) &= (x+(-x))+A\\ &= 0+A\\ &= A.\end{aligned}$$

We showed above that $A$ is the additive identity of $R/A$, so $-x + A$ 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 associative 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 $R$,

$$\begin{aligned} X(Y+Z) &= (x+A)((y+z)+A) \\ &= (x(y+z))+A \\ &= (xy+xz)+A \\ &= ((xy)+A)+((yz)+A) \\ &= XY+XZ. \end{aligned}$$

Hence $R/A$ is a ring. □

PROPOSITION 7.83. *If $R$ is a commutative ring with unity, then $R/A$ is also a commutative ring with unity. The multiplicative identity of $R/A$ is $1_R + A$.*

PROOF. You do it! See Exercise 7.88. □

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 by Exercise 7.61 $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, it follows that $\mathbb{Z}_n$ is also a ring. Of course, you had already argued this in Exercise 7.8.

We can go a little bit further. You should have found in Exercise 7.21 that $\mathbb{Z}_n^*$ is a field, but in Exercise 7.20 that $\mathbb{Z}_n$ is not, in general, an integral domain, let alone field. The relationship between maximal ideals and prime ideals that we studied in Section 7.6 helps explain this.

THEOREM 7.84. *If $R$ is a commutative 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 commutative 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 7.68, Definition 7.59, and Proposition 7.60). By Exercise 7.65, $1 \notin M$. Thus $\langle 1 \rangle + M$ also satisfies $\langle 1 \rangle + M = R$. In other words, $\langle x \rangle + M = \langle 1 \rangle + M$. Since $1 = 1 \cdot 1 + 0 \in \langle 1 \rangle + M$, 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 7.82

$$1 + M = hx + M = (h+M)(x+M).$$

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 7.82 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 7.65 $N = R$. Since $N$ was an arbitrary ideal that contained $M$ properly, $M$ is maximal. □

A similar property holds true for prime ideals.

THEOREM 7.85. *If $R$ is a commutative 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 commutative ring 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 7.82 $xy \in P$. We claim that this implies that $x \in P$ or $y \in P$.

Assume to the contrary that $x, y \notin P$. However, $\langle x \rangle \langle y \rangle \subset P$, since for any $z \in \langle x \rangle \langle y \rangle$ we have $z = (hx)(qy)$ for appropriate $h, q \in R$, and since $R$ is commutative and $P$ absorbs multiplication, $z = (hq)(xy) \in P$. Now $P$ is a prime ideal, so $\langle x \rangle \subset P$ or $\langle y \rangle \subset P$; without loss of generality, $\langle x \rangle \subset P$, and $x = 1_R x \in \langle x \rangle \subset P$, so $x \in P$.

Since $x \in P$, $x + P = P$. 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 $A \not\subseteq P$ 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 7.82 $b \in P$ 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. $\square$

A corollary gives us an alternate proof of Theorem .7.74.

COROLLARY 7.86. *In a commutative ring with unity, every maximal ideal is prime, but the converse is not necessarily true.*

PROOF. Let $R$ be a commutative ring with unity, and $M$ a maximal ideal. By Theorem 7.84, $R/M$ is a field. By Theorem 7.18, $R/M$ is an integral domain. By Theorem 7.85, $M$ is prime.

The converse is not necessarily true because not every integral domain is a field. $\square$

EXERCISES.

EXERCISE 7.87. Prove Lemma 7.82.

EXERCISE 7.88. Prove Proposition 7.83.

EXERCISE 7.89. Consider the ideal $I = \langle x^2 + 1 \rangle$ in $R = \mathbb{C}[x]$. The purpose of this exercise is to show that $I$ is maximal.

(a) Explain why every $f \in R/I$ has the form $r + I$ for some $r \in R$ such that $\deg r < 2$.
(b) Part (a) implies that every element of $R/I$ can be written in the form $f = (ax + b) + I$ where $a, b \in \mathbb{C}$. If $f + I$ is a nonzero element of $R/I$, what must be true about $a$ and $b$?
(c) Let $f + I \in R/I$ and find an element $g + I \in R/I$ such that $g + I = (f + I)^{-1}$; that is, $(fg) + I = 1 + R/I$. *Hint:* 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 $c, d$.
(d) Explain why part (c) shows that $I$ is maximal.

EXERCISE 7.90. 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 $\mathbb{F}[x]/I$ is a field. *Hint:* Follow the strategy of Exercise 7.89.

EXERCISE 7.91. Recall the ideal $I = \langle x^2 + y^2 - 4, xy - 1 \rangle$ of Exercise 7.57. 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 the previous problem.

(a) Explain why someone might think naïvely that every $f \in R/I$ has the form $r + I$ where $r \in R$ and $r = p(y) + bx + cy + d$, for appropriate $p \in \mathbb{C}[y]$ and $b, c, d \in \mathbb{C}$; in the same way, someone might think naïvely that every distinct polynomial $r$ of that form represents a distinct element of $R/I$. *Hint:* Look at the previous problem.

(b) Show that, to the contrary, $1 + I = (y^3 - 4y + x + 1) + I$. *Hint:* Notice that

$$y\left(x^2 + y^2 - 4\right) + I = I$$

and $x(xy - 1) + I = I$. This is related to the idea of the *subtraction polynomials* in later chapters.

## 7.8. FINITE FIELDS

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 7.21 on page 134 you found that $\mathbb{Z}_n^*$ is always a field. You showed in Exercise 7.20 that if $n$ is irreducible, then $\mathbb{Z}_n$ is not only an integral domain, but a field. However, that does not characterize all cases where $\mathbb{Z}_n$ is a field. 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.[1]

Before we proceed, we will need the following definition.

DEFINITION 7.92. 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 $\varkappa$ such that $\varkappa r = 0_R$ for all $r \in R$. In this case, $R$ has **characteristic** $\varkappa$.

EXAMPLE 7.93. The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic zero, since $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. 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 7.21, $\mathbb{Z}_p = \mathbb{Z}_p^*$ is a field. Its characteristic is $p$. $\diamond$

Given these examples, you might expect the characteristic of a ring to be the number of elements in the ring. This is not always the case.

EXAMPLE 7.94. 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:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac, bd).$$

[1] 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.)

It is not hard to show that this is a ring; we leave it to Exercise 7.98. We see that $R$ 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 $4(a,b) = (4a,4b) = ([0]_2,[0]_4) = 0_R$. $\diamondsuit$

That said, we can make the following observation.

PROPOSITION 7.95. *In a commutative ring $R$ with multiplicative identity $1_R$, the characteristic of a ring is determined by the multiplicative identity. That is, if $x$ is the smallest positive integer such that $x \cdot 1_R = 0_R$, then $x$ is the characteristic of the ring.*

PROOF. You do it! See Exercise 7.99. □

In case you are wondering why we have dedicated this much time to Definition 7.92 and Proposition 7.95, 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 7.95.

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. 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 7.96. 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 $f$, 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 7.90, $I = \langle f \rangle$ is a maximal ideal in $R = \mathbb{Z}_2[x]$, and by Theorem 7.84, $R/I$ 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 $\deg g < 2$, since 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 $X$.

Since $\deg g < 2$, there are 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* 2. $\mathbb{F}_{16}$

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

$$\begin{aligned} a+c &= [0] \\ ac+b+d &= [0] \\ ad+bc &= [1] \\ bd &= [1]. \end{aligned} \tag{7.8.1}$$

From (??) we conclude that $a = -c$, but in $\mathbb{Z}_2$ this implies that $a = c$. The system now simplifies to

$$a^2 + b + d = [0] \tag{7.8.2}$$

$$a(b+d) = [1] \tag{7.8.3}$$

$$bd = [1]. \tag{7.8.4}$$

Again, in $\mathbb{Z}_2$ we know that $a^2 = a$ regardless of the value of $a$, so (??) implies $a = -(b+d) = b+d$. Substituting this into (??), 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 (??).

Thus $f$ does not factor. By Exercise 7.90, $I = \langle f \rangle$ is a maximal ideal in $R = \mathbb{Z}_2[x]$, and by Theorem 7.84, $R/I$ 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

$$\begin{array}{rrrr} I, & [1]+I, & x+I, & x+[1]+I, \\ x^2+I & x^2+[1]+I, & x^2+x+I, & x^2+x+[1]+I, \\ x^3+I, & x^3+[1]+I, & x^3+x+I, & x^3+x+[1]+I, \\ x^3+x^2+I, & x^3+x^2+[1]+I, & x^3+x^2+x+I, & x^3+x^2+x+[1]+I. \end{array}$$

◇

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 in principle 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 6.40 on page 116) 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 roots $p^n$ 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 7.97. *Suppose that $\mathbb{F}_n$ is a finite field with n elements. Then n is a power of an irreducible integer.*

PROOF. The proof has three steps.[2]

**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 7.95, $p$ is the smallest positive integer $x$ such that $x \cdot 1_{\mathbb{F}_n} = 0_{\mathbb{F}_n}$; thus $p \le a$. However, $a$ divides $p$, so $a \le p$. This implies that $a = p$ and $b = 1$; since $p = ab$ was an arbitrary factorization of $p$, $p$ is irreducible.

**Second,** let $q \in \mathbb{N}$ such that $q$ is irreducible. Consider the additive group of $\mathbb{F}_n$; suppose that $q$ divides $n = |\mathbb{F}_n|$. Let

$$\mathcal{L} = \left\{ \left(a_1, a_2, \dots, a_q\right) : \sum_{i=1}^{q} a_i = 0 \right\};$$

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 $\left(0_{\mathbb{F}_n}, 0_{\mathbb{F}_n}, \dots, 0_{\mathbb{F}_n}\right) \in \mathcal{L}$.

For any $\sigma \in S_q$, the commutative property of addition implies that $\sigma\left(a_1, a_2, \dots, a_q\right) \in \mathcal{L}$. In particular, if $\sigma \in \langle \begin{pmatrix} 1 & 2 & \cdots & q \end{pmatrix} \rangle$ then $\sigma\left(a_1, a_2, \dots, a_q\right) \in \mathcal{L}$. In fact, when we permute any element $A \in \mathcal{L}$ by some $\sigma \in \langle \begin{pmatrix} 1 & 2 & \cdots & q \end{pmatrix} \rangle$, then $\sigma(A) \ne A$ implies that $\sigma \ne \begin{pmatrix} 1 \end{pmatrix}$ and $A$ has at least two distinct elements. Assume that $\sigma \ne \iota$; if $\sigma(A) \ne A$, then all the permutations of $\langle \begin{pmatrix} 1 & 2 & \cdots & q \end{pmatrix} \rangle$ 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 $\sigma(A) \ne A$ implies that exactly one permutation of $A$ is in $\mathcal{M}_2$, though perhaps not $A$ itself.

[2]Adapted from the proofs of Theorems 31.5, 42.4, and 46.1 in [AF05].

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.

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 $S$ we can choose any elements from $\mathbb{F}_n$ that we want for the first $q-1$ elements; the final, $q$th 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,

$$n^{q-1}=r+qs.$$

Recall that $q\mid n$, say $n=qd$ for $d\in\mathbb{N}$, so

$$(qd)^{q-1}=r+qs$$
$$q\left[d\,(qd)^{q-2}-s\right]=r,$$

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,** recall that the characteristic of $\mathbb{F}_n$ is $p$. Thus $px=0$. Consider the additive cyclic group $\langle x\rangle$; by Exercise 2.58 on page 34, $\operatorname{ord}(x)\mid p$ , 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 $p$. □

EXERCISES.

EXERCISE 7.98. Recall $R=\mathbb{Z}_2\times\mathbb{Z}_4$ from Example 7.94.
(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. *Hint:* Proceed by induction on $n$.

EXERCISE 7.99. Prove Proposition 7.95. *Hint:* Rewrite an abitrary element of the ring using the multiplicative identity, then apply the commutative property of the ring.

EXERCISE 7.100. Build the addition and multiplication tables of the field of four elements that we constructed in Example 7.96 on page 159.

EXERCISE 7.101. Construct a field with 9 elements, and list them all.

EXERCISE 7.102. Construct a field with 27 elements, and list them all.

EXERCISE 7.103. Does every infinite field have characteristic 0? *Hint:* Think of a fraction field over an appropriate ring.

## 7.9. 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–addition and multiplication–rather than merely one, so we have to measure whether both ring operations behave similarly.

DEFINITION 7.104. 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 7.105. 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 7.106.

EXAMPLE 7.106. Let $f: \mathbb{Z} \to 2\mathbb{Z}$ by $f(x) = 4x$. In Example 4.2 on page 61 we showed that this was a homomorphism of groups. However, it is *not* a homomorphism of rings, because it does not preserve multiplication:

$$f(xy) = 4xy \quad \text{but} \quad f(x)f(y) = (4x)(4y) = 16xy \neq f(xy). \diamond$$

Example 7.106 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  shows that this is not possible, in a way that should not surprise you.

THEOREM 7.107. *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 $S$. Let $y \in S$; the fact that $R$ is onto implies that $f(x) = y$ for some $x \in R$. Applying the homomorphism property,

$$y \cdot f(1_R) = f(x) f(1_R) = f(x \cdot 1_R) = f(x) = f(1_R \cdot x) = f(1_R) f(x) = f(1_R) \cdot y$$

so $f(1_R)$ 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 unity (a multiplicative identity);
- by Theorem 7.107, $n\mathbb{Z}$ would also have to have unity;
- but $n\mathbb{Z}$ does not has unity when $n \neq 1$.

We should also identify some other properties of a ring homomorphism.

THEOREM 7.108. *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 multipicative 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 7.113 on page 167. □

We have not yet encountered an example of a ring isomorphism, so let's consider one.

EXAMPLE 7.109. Let $p = ax + b \in \mathbb{Q}[x]$, where $p \neq 0$. Recall from Exercise 7.90 that $\langle p \rangle$ is maximal in $\mathbb{Q}[x]$. Let $R = \mathbb{Q}[x]$ and $I = \langle p \rangle$; by Theorem 7.84, $R/I$ is a field.

Notice 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 $f(x) = x + I$ for every $x \in \mathbb{Q}$. Is $f$ a homomorphism?

*Homomorphism property?* Let $x, y \in \mathbb{Q}$; using the definition of $f$ and the properties of coset addition,

$$f(x+y) = (x+y) + I = (x+I) + (y+I) = f(x) + f(y).$$

Likewise,

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

*One-to-one?* Let $x, y \in \mathbb{Q}$ and suppose that $f(x) = f(y)$. Then $x + I = y + I$, which implies that $x - y \in I$. By the closure of $\mathbb{Q}$, $x - y$ is a rational number, while $I = \langle ax + b \rangle$ is the set of all multiples of $ax + b$. The only rational number in $I$ is therefore $0$, which implies that $x - y = 0$, so $x = y$.

*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

$$p + I = [q(ax+b) + r] + I = [q(ax+b) + I] + (r + I) = I + (r + I) = r + I.$$

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 7.110. 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 7.114 on page 167 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 7.111. *Let $R, S$ be commutative 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 a 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:

$$h(x + \ker f) = f(x) \quad \text{and} \quad h(y + \ker f) = f(y).$$

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 7.108 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 7.108, we see that

$$\begin{aligned} f(x) = f(y) &\Longrightarrow f(x) - f(y) = 0_S \\ &\Longrightarrow x - y \in \ker f \\ &\Longrightarrow (x - y) + \ker f = \ker f \\ &\Longrightarrow x + \ker f = y + \ker f, \end{aligned}$$

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 7.112. 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 $f(3x^3 - 1) = 23$.

*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 $f(3x^3 - 1) = 23$, and from our work prove that $f$ is onto, we can deduce that $f(x + 21) = 23$, so $f$ is not one-to-one.

Let's apply Theorem 7.111 to obtain an isomorphism. First, identify $\ker f$: it consists of all the polynomials $p \in \mathbb{Q}[x]$ such that $p(2) = 0$. Facts from high-school mathematics (the Factor Theorem, for example) imply 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 7.111 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 7.109, that $x - 2$ is a linear polynomial, which does not factor; that therefore $\langle x - 2 \rangle$ is a maximal ideal; and finally that $\mathbb{Q}[x] / \langle x - 2 \rangle$ is a field–as is $\mathbb{Q}$. ◇

EXERCISES.

EXERCISE 7.113. Prove Theorem 7.108. *Hint:* Use strategies similar to those used to prove Theorem 4.9 on page 64.

EXERCISE 7.114. 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,

$$\ker f = \{x \in R : f(x) = 0_S\}.$$

(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 7.115. Recall from Example 7.109 on page 164 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 7.111 on page 165 to show this a different way. *Hint:* Follow Example 7.112 on the preceding page.

EXERCISE 7.116. Use Theorem 7.111 on page 165 to show that $\mathbb{Q}[x] / \langle x^2 \rangle$ is isomorphic to

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \right\} \subset \mathbb{Q}^{2\times 2}.$$

*Hint:* 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 7.117. 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. *Hint:* Think about $i = \sqrt{-1}$.

CHAPTER 8

# Rings and polynomial factorization

CHAPTER 9

# 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:

$$
\begin{aligned}
axy - b_1 x - cy + d_1 &= 0\\
axy - b_2 x - cy + d_2 &= 0\\
axy - b_2 x - b_1 y + d_3 &= 0
\end{aligned}
\tag{9.0.1}
$$

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-known*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. From here on, all rings are polynomial rings over a field $\mathbb{F}$, *unless we say otherwise.*

## 9.1. GAUSSIAN ELIMINATION

Let's look again at the system (9.0.1) 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

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \vdots \qquad\qquad & \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

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 9.1. 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 9.2. 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 $\operatorname{lv}(g_i)$ for this variable, and order the variables as $x_1 > x_2 > \ldots > x_n$.

*The leading variable of the zero polynomial is undefined.*

**Algorithm 2** 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 $\operatorname{lv}(g_k) \geq \operatorname{lv}(g_\ell)$
    **if** $g_i \neq 0$
      Denote the coefficient of $\operatorname{lv}(g_i)$ by $a$
      **for** $j = i+1, i+2, \ldots m$
        **if** $\operatorname{lv}(g_j) = \operatorname{lv}(g_i)$
          Denote the coefficient of $\operatorname{lv}(g_j)$ by $b$
          Replace $g_j$ with $a g_j - b g_i$
  **return** $G$

EXAMPLE 9.3. Using the example from 9.1,

$$\operatorname{lv}(5x_1 + x_2 + 7x_2 + 8) = x_1 \quad \text{and} \quad \operatorname{lv}(x_3 + 11x_4 + 2x_5 + 12) = x_3. \diamond$$

REMARK. 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 9.4. A list of linear polynomials $F$ is in **triangular form** if for each $i < j$,

- $f_j = 0$, or
- $f_i \neq 0$ and $\operatorname{lv}(f_i) > \operatorname{lv}(f_j)$.

EXAMPLE 9.5. Using the example from 9.1,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 $\operatorname{lv}(f_2) = x_3$ and $\operatorname{lv}(f_3) = x_1$, so $\operatorname{lv}(f_2) < \operatorname{lv}(f_3)$, whereas we want $\operatorname{lv}(f_2) > \operatorname{lv}(f_3)$.

On the other hand, the list

$$G = (x_1 + 6, x_2 + 3x_4, 0)$$

is in triangular form, because $\operatorname{lv}(g_1) > \operatorname{lv}(g_2)$ and $g_3$ is zero. However, if we permute $G$ using the permutation $\pi = (\ 2 \quad 3\ )$, then

$$H = \pi(G) = (x_1 + 6, 0, x_2 + 3x_4)$$

is not in triangular form, because $h_3 \neq 0$ but $h_2 = 0$. $\diamond$

Algorithm 2 describes one way to apply the method.

THEOREM 9.6. *Algorithm (2) 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 $F$.

*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 $\operatorname{lv}\left(g_j\right)$ 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 $x = \operatorname{lv}(g_1)$. 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 $\operatorname{lv}(g_1)$ 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 the sublist $(g_1, g_2, \ldots, g_{i-1})$ is in triangular form *and* for each $j = 1, \ldots, i-1$ if $\operatorname{lv}\left(g_j\right)$ 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 $x = \operatorname{lv}(g_i)$. 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 $x < \operatorname{lv}\left(g_j\right)$ for $j = 1, \ldots, i-1$. Thus $(g_1, \ldots, g_i)$ is in triangular form, and the coefficient of $\operatorname{lv}(g_i)$ 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 $m$th 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 $a_{i,j} \in \mathbb{F}$ such that

$$g_j = a_{11} f_1 + a_{12} f_2 + \cdots + a_{1m} f_m.$$

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. 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 9.7. We use Algorithm 2 to illustrate Gaussian elimination for the system of equations described in Example 9.1.

- 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 $\operatorname{lv}(g_i)$; since $\operatorname{lv}(g_i) = x_1$, $a = 5$.
  - We now enter an *inner* loop:
    - ⋆ In the first iteration, $j = 2$.
    - ⋆ Since $\operatorname{lv}\left(g_j\right) = \operatorname{lv}(g_i)$, we proceed: denote $b$ as the coefficient of $\operatorname{lv}\left(g_j\right)$; since $\operatorname{lv}\left(g_j\right) = x_1$, $b = 3$.
    - ⋆ 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 $\operatorname{lv}\left(g_j\right) \neq \operatorname{lv}(g_i)$, 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 $\operatorname{lv}(g_i)$; since $\operatorname{lv}(g_i) = x_2$, $a = 6$.
  - We now enter an *inner* loop:
    - ⋆ In the first iteration, $j = 2$.
    - ⋆ Since $\operatorname{lv}\left(g_j\right) \neq \operatorname{lv}(g_i)$, 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 9.8. *Let $G = (g_1, g_2, \ldots, g_m)$ is a list of 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 9.8 can be found in any textbook on linear algebra, although probably not in one place.

EXAMPLE 9.9. 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 9.8 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 $g_2 = 0$,

$$6x_2 = 12x_3 + 8t + 8. \tag{9.1.1}$$

  The Euclidean algorithm helps us derive the multiplicative inverse of 6 in $\mathbb{Z}_2$; we get 11. Multiplying both sides of (9.1.1) 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:

$$\begin{aligned}
f_1 :& 5(7s + 9) + (4s + 6t + 12) + 7t + 8 \\
&= (9s + 6) + 4s + 20 \\
&= 0 \\
f_2 :& = (2s + 11t + 1) + 11s + 2t + 12 \\
&= 0 \\
f_3 :& 3(7s + 9) + 7(4s + 6t + 12) + 8(2s + 11t + 1) + 11 \\
&= (8s + 1) + (2s + 3t + 6) + (3s + 10t + 8) + 11 \\
&= 0. \diamondsuit
\end{aligned}$$

Before proceeding to the next section, study the proof of Theorem (9.6) carefully. Think about how we might relate these ideas to non-linear polynomials.

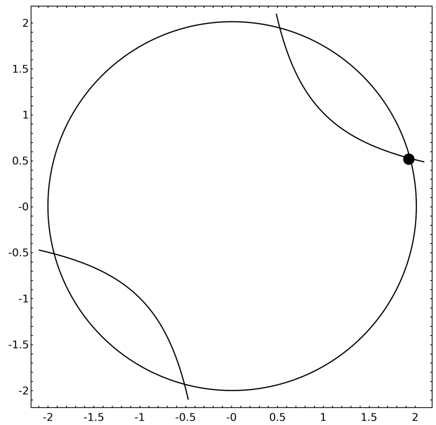



FIGURE 9.1. Plots of $x^2 + y^2 = 4$ and $xy = 1$

EXERCISES.

EXERCISE 9.10. 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 9.11. Find the triangular form of the following linear systems.
(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 9.12. 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 9.13. Does Algorithm 2 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?

## 9.2. 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 9.1. 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 polynomial that isn't obviously spanned by either of these two:

$$y\left(x^2+y^2-4\right)-x\left(xy-1\right)=x+y^3-4y. \tag{9.2.1}$$

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.

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 (9.2.1), 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.

DEFINITION 9.14. Let $t,u$ be monomials. The **lexicographic ordering of monomials over the variables** $x_1,x_2,\ldots,x_n$ 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. We denote the leading monomial of a polynomial $p$ as $\mathrm{lm}(p)$.

EXAMPLE 9.15. Using the lexicographic ordering over $x,y$,

$$\mathrm{lm}\left(x^2+y^2-4\right)=x^2$$
$$\mathrm{lm}\left(xy-1\right)=xy$$
$$\mathrm{lm}\left(x+y^3-4y\right)=x.\ \diamondsuit$$

Before proceeding, we should prove a few simple, but important, properties of the lexicographic ordering.

PROPOSITION 9.16. *For the lexicographic ordering over any list of variables* $\mathbf{x}=(x_1,x_2,\ldots,x_n)$, *each of the following holds for any two terms $t$ and $u$ in* $\mathbf{x}$.

*(A)* $1\le t$.

(B) *One of the following holds:* $t < u$, $t = u$, *or* $t > u$.
(C) *If* $t \mid u$, *then* $t \leq u$.
(D) *If* $t > u$, *then for any monomial* $v$ *over* $\mathbf{x}$, $tv > uv$.
(E) *The set of all monomials over* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ *is well-ordered by the lexicographic ordering. That is, every subset* $M$ *of* $\mathbb{M}$ *has a least element.*

PROOF. For (A), $\deg_{x_i} 1 = 0 \leq \deg_{x_i} t$ for all $i = 1, 2, \ldots, n$. Hence $1 \leq t$.

For (B), 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 (C), 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 (D), 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 $tv > uv$.

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 9.17. *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. □

Having identified these properties, let's turn to the notion of a "triangular form" of a non-linear system. The primary issue we would like to resolve is the one that we remarked immediately after computing the subtraction polynomial of equation (9.2.1): 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 7.58 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 generators of the ideal. Let's define a form of the basis of an ideal that will not give us this problem.

DEFINITION 9.18. Let $g_1, g_2, \ldots, g_m$ be generators 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 $I$ in the lexicographic ordering** 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 list of generators 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 $\mathbf{x}=(x_1,x_2,\dots,x_n)$. 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 $i=1,2,\dots,n$. 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 $i=1,2,\dots,n$. 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 9.19. *For any two polynomials $p,q\in\mathbb{F}[x_1,x_2,\dots,x_n]$, 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 $\tau,\mu$ and $a,b\in\mathbb{F}$, if $a\tau p-b\mu q$ cancels the leading terms of $\tau p$ and $\mu q$, 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 9.16,

$$\operatorname{lm}\left(\frac{\operatorname{lcm}(t,u)}{t}\cdot p\right)=\frac{\operatorname{lcm}(t,u)}{t}\cdot\operatorname{lm}(p)=\frac{\operatorname{lcm}(t,u)}{t}\cdot t=\operatorname{lcm}(t,u);$$

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 $\tau,\mu$ be monomials over $\mathbf{x}=(x_1,x_2,\dots,x_n)$ 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 $\alpha_i$ and $\beta_i$ 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 $\zeta_i$ and $\omega_i$ in $\mathbb{N}$. The leading monomials of $a\tau p-b\mu q$ cancel, so for each $i=1,2,\dots,n$

$$\alpha_i+\zeta_i=\beta_i+\omega_i.$$

We have

$$\alpha_i=\beta_i+(\omega_i-\zeta_i).$$

Thus

$\alpha_i - (\max(\zeta_i,\omega_i) - \zeta_i) = [(\beta_i + (\omega_i - \zeta_i)) - (\max(\zeta_i,\omega_i) - \zeta_i)] = \beta_i - (\max(\zeta_i,\omega_i) - \omega_i)$.

Let $\eta_i = \alpha_i - (\max(\zeta_i,\omega_i) - \zeta_i)$ and let

$$v = \prod_{i=1}^{n} x_i^{\eta_i}.$$

Then

$$a\tau p - b\mu q = v\left(a \cdot \frac{\mathrm{lcm}(t,u)}{t} \cdot p - b \cdot \frac{\mathrm{lcm}(t,u)}{u} \cdot q\right),$$

as claimed. □

The subtraction polynomial of Lemma 9.19 is important enough that we give it a special name.

DEFINITION 9.20. Let $p,q \in \mathbb{F}[x_1,x_2,\dots,x_n]$. We define the **$S$-polynomial of $p$ and $q$ with respect to the lexicographic ordering** to be

$$\mathrm{Spol}(p,q) = \mathrm{lc}(q) \cdot \frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(q))}{\mathrm{lm}(p)} \cdot p - \mathrm{lc}(p) \cdot \frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(q))}{\mathrm{lm}(q)} \cdot q.$$

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 2, 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 9.21. Let $p,q \in \mathbb{F}[x_1,x_2,\dots,x_n]$. If $\mathrm{lm}(p)$ divides $\mathrm{lm}(q)$, then we say that $p$ **top-reduces** $q$.

In addition, let $t = \mathrm{lm}(q)/\mathrm{lm}(p)$ and $c = \mathrm{lc}(q)/\mathrm{lm}(p)$. Let $r = q - ct \cdot p$; we say that $p$ **top-reduces $q$ to $r$**.

Finally, let $F = (f_1, f_2, \dots, f_m)$ be a list of polynomials in $\mathbb{F}[x_1,x_2,\dots,x_n]$, and $r_1, r_2, \dots, r_k \in \mathbb{F}[x_1,x_2,\dots,x_n]$ such that

- some polynomial of $F$ top-reduces $p$ to $r_1$,
- some polynomial of $F$ top-reduces $r_1$ to $r_2$,
- ...
- some polynomial of $F$ top-reduces $r_k$ to 0.

In this case, we say that $p$ **top-reduces to 0 modulo $F$**.

EXAMPLE 9.22. Let $p = x + 1$ and $q = x^2 + 1$. Clearly $p$ top-reduces $q$ to $r = -x + 1$. ◇

We will need the following properties of polynomial operations.

PROPOSITION 9.23. *Let $p,q,r \in \mathbb{F}[x_1,x_2,\dots,x_n]$. Each of the following holds:*

*(A)* $\mathrm{lm}(pq) = \mathrm{lm}(p) \cdot \mathrm{lm}(q)$

*(B)* $\mathrm{lm}(p \pm q) \leq \max(\mathrm{lm}(p),\mathrm{lm}(q))$

*(C)* $\mathrm{lm}(\mathrm{Spol}(p,q)) < \mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(q))$

*(D) If $p$ top-reduces $q$ to $r$, then* $\mathrm{lm}(r) < \mathrm{lm}(q)$.

PROOF. For convenience, write $t = \text{lm}(p)$ and $u = \text{lm}(q)$.

(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 $v \neq \text{lm}(p)$, then the definition of a leading monomial implies that $v < t$. Proposition 9.16 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 $\text{lm}(pq) = tu = \text{lm}(p)\,\text{lm}(q)$.

(B) Any monomial of $p \pm q$ is also a monomial of $p$ or a product of $q$. Hence $\text{lm}(p \pm q)$ is a monomial of $p$ or of $q$. The maximum of these is $\max(\text{lm}(p), \text{lm}(q))$. Hence $\text{lm}(p \pm q) \leq \max(\text{lm}(p), \text{lm}(q))$.

(C) Definition 9.20 and (B) imply that $\text{lm}(\text{Spol}(p,q)) < \text{lcm}(\text{lm}(p), \text{lm}(q))$.

(D) Assume that $p$ top-reduces $q$ to $r$. Top-reduction is a special case of of an $S$-polynomial; that is, $r = \text{Spol}(p,q)$. Here $\text{lcm}(\text{lm}(p), \text{lm}(q)) = \text{lm}(q)$, and (C) implies that $\text{lm}(r) < \text{lm}(q)$. □

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 9.24 (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 $1 \leq i < j \leq m$,* $\text{Spol}\left(g_i, g_j\right)$ top-reduces to zero with respect to $G$.

EXAMPLE 9.25. We conclude by reviewing two systems considered at the beginning of this chapter,

$$F = \left(x^2 + y^2 - 4, xy - 1\right)$$

and

$$G = \left(x^2 + y^2 - 4, xy - 1, x + y^3 - 4y\right).$$

Is either of these a Gröbner basis?

- Certainly $F$ is not; we already showed that the one $S$-polynomial is

  $$S = \text{Spol}(f_1, f_2) = y\left(x^2 + y^2 - 4\right) - x(xy - 1) = x + y^3 - 4y;$$

  this does not top-reduce to zero because $\text{lm}(S) = x$, and neither leading term of $F$ divides this.
- Neither is $G$ a Gröbner basis, for

  $$\begin{aligned} \text{Spol}(g_2, g_3) &= 1 \cdot (xy - 1) - y\left(x + y^3 - 4y\right) \\ &= -y^4 + 4y^2 - 1. \end{aligned}$$

  This polynomial is certainly in the ideal $\langle g_1, g_2, g_3 \rangle$, but no leading term of that ideal divides $y^4$.

- On the other hand, if we expand $G$ to include $-y^4+4y^3-1$, we finally have a Gröbner basis. You will verify this in Exercise 9.28.

◇

REMARK 9.26. Example 9.25 suggests a method to compute a Gröbner basis of an ideal: given a list of generators, use $S$-polynomials to find elements of the ideal that do not satisfy Definition 9.18; then keep adding these to the list of generators 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 9.24, but before we can do that we will need the following useful lemma. While small, it has important repercussions later.

LEMMA 9.27. *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 9.31. □

You will see in the following that Lemma 9.27allows us to replace polynomials that are "too large" with smaller polynomials. This allows us to obtain the desired form.

PROOF OF THEOREM 9.24. *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 $r_\ell$ top-reduces to $r_{\ell+1}$ for each $\ell \in \mathbb{N}$. From Proposition 9.23, 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 $R = \{r_1, r_2, \ldots, \}$! Thus the chain of top-reductions cannot continue indefinitely. It cannot conclude with a non-zero polynomial $r_{\text{last}}$, since:

- top-reduction keeps each $r_\ell$ 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 $r_{\text{last}}$ would be top-reducible by some element of $G$.

The chain of top-reductions must conclude with zero, so $\text{Spol}\left(g_i, g_j\right)$ top-reduces to zero.

*That (A) ⇐ (B):* Assume (B). We want to show (A); that is, any element of $\langle G\rangle$ is top-reducible by an element of $g$. So let $p \in \langle g_1, g_2, \ldots, g_m\rangle$; 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 $t_i = \text{lm}(g_i)$ and $u_i = \text{lm}(h_i)$. 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 $\text{lm}(p) = T$, then we are done, since

$$\text{lm}(p) = T = u_k t_k = \text{lm}(h_k)\,\text{lm}(g_k) \quad \exists k \in \{1, 2, \ldots, m\}.$$

Otherwise, there must be some cancellation among the leading monomials of each polynomial in the sum on the right hand side. That is,

$$T = \text{lm}\left(h_{\ell_1} g_{\ell_1}\right) = \text{lm}\left(h_{\ell_2} g_{\ell_2}\right) = \cdots = \text{lm}\left(h_{\ell_s} g_{\ell_s}\right)$$

for some $\ell_1, \ell_2, \ldots, \ell_s \in \{1, 2, \ldots, m\}$. From Lemma 9.19, 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,

$$\text{lm}\left(h_{\ell_1}\right) g_{\ell_1} + \text{lm}\left(h_{\ell_2}\right) g_{\ell_2} + \cdots + \text{lm}\left(h_{\ell_s}\right) g_{\ell_s} = \sum_{1 \le a < b \le s} c_{a,b} u_{a,b} \text{Spol}\left(g_{\ell_a}, g_{\ell_b}\right)$$

where for each $a, b$ we have $c_{a,b} \in \mathbb{F}$ and $u_{a,b} \in \mathbb{M}$. Let

$$S = \sum_{1 \le a < b \le s} c_{a,b} u_{a,b} \text{Spol}\left(g_{\ell_a}, g_{\ell_b}\right).$$

Observe that

$$\left[\text{lm}\left(h_{\ell_1}\right) g_{\ell_1} + \text{lm}\left(h_{\ell_2}\right) g_{\ell_2} + \cdots + \text{lm}\left(h_{\ell_s}\right) g_{\ell_s}\right] - S = 0. \tag{9.2.2}$$

By (B), we know that each $S$-polynomial of $S$ top-reduces to zero. This fact, Lemma 9.27 and Proposition 9.23, 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

$$\text{Spol}\left(g_{\ell_a}, g_{\ell_b}\right) = q_1^{(a,b)} g_1 + \cdots + g_m^{(a,b)} g_m$$

and for each $\lambda = 1, 2, \ldots, m$ we have $q_\lambda^{(a,b)} = 0$ or

$$\text{lm}\left(q_\lambda^{(a,b)}\right) \text{lm}(g_\lambda) \le \text{lm}\left(\text{Spol}\left(g_{\ell_a}, g_{\ell_b}\right)\right) < \text{lcm}\left(\text{lm}\left(g_{\ell_a}\right), \text{lm}\left(g_{\ell_b}\right)\right). \tag{9.2.3}$$

Let $Q_1, Q_2, \ldots, Q_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that

$$Q_k = \sum_{1 \le a < b \le s} q_k^{(a,b)}.$$

Then

$$S = Q_1 g_1 + Q_2 g_2 + \cdots + Q_m g_m.$$

In other words,

$$S - (Q_1 g_1 + Q_2 g_2 + \cdots + Q_m g_m) = 0.$$

By equation (9.2.3) and Proposition 9.23, for each $k=1,2,\ldots,m$ we have $Q_k=0$ or

$$
\begin{aligned}
\operatorname{lm}(Q_k)\operatorname{lm}(g_k) &\le \max_{1\le a<b\le s}\left\{\operatorname{lm}\left(q_k^{(a,b)}\right)\operatorname{lm}(g_k)\right\}\\
&\le \max_{1\le a<b\le s}\operatorname{lm}\left(\operatorname{Spol}\left(g_{\ell_a},g_{\ell_b}\right)\right)\\
&< \operatorname{lcm}\left(\operatorname{lm}\left(g_{\ell_a}\right),\operatorname{lm}\left(g_{\ell_b}\right)\right)\\
&= T. \qquad (9.2.4)
\end{aligned}
$$

By substitution,

$$
\begin{aligned}
p &= (h_1g_1+h_2g_2+\cdots+h_mg_m)-[S-(Q_1g_1+Q_2g_2+\cdots+Q_mg_m)]\\
&= ((h_1-\operatorname{lc}(h_1)\operatorname{lm}(h_1))\,g_1+\cdots+(h_m-\operatorname{lc}(h_m)\operatorname{lm}(h_m))\,g_m)\\
&\quad+[\operatorname{lc}(h_1)\operatorname{lm}(h_1)\,g_1+\cdots+\operatorname{lc}(h_m)\operatorname{lm}(h_m)\,g_m-S]\\
&\quad+(Q_1g_1+Q_2g_2+\cdots+Q_mg_m).
\end{aligned}
$$

By (9.2.2), this simplifies to

$$
\begin{aligned}
p &= ((h_1-\operatorname{lc}(h_1)\operatorname{lm}(h_1))\,g_1+\cdots+(h_m-\operatorname{lc}(h_m)\operatorname{lm}(h_m))\,g_m)\\
&\quad+(Q_1g_1+Q_2g_2+\cdots+Q_mg_m)\\
&= ((h_1-\operatorname{lc}(h_1)\operatorname{lm}(h_1)+Q_1)\,g_1+\cdots+(h_m-\operatorname{lc}(h_m)\operatorname{lm}(h_m)+Q_m)\,g_m).
\end{aligned}
$$

For each $k=1,2,\ldots,m$ and each nonzero $h_k,Q_k$ we see that $\operatorname{lm}(h_k-\operatorname{lc}(h_k)\operatorname{lm}(h_k))<\operatorname{lm}(h_k)$ and $\operatorname{lm}(Q_k)=\sum_{1\le a<b\le s}q_k^{(a,b)}$, so by Proposition 9.23 and equation (9.2.4) we have

$$h_k-\operatorname{lc}(h_k)\operatorname{lm}(h_k)+Q_k=0$$

or

$$
\begin{aligned}
\operatorname{lm}(h_k-\operatorname{lc}(h_k)\operatorname{lm}(h_k)+Q_k)\operatorname{lm}(g_k) &\le \max(\operatorname{lm}(h_k-\operatorname{lc}(h_k)\operatorname{lm}(h_k))\operatorname{lm}(g_k),\\
&\qquad\qquad \operatorname{lm}(Q_k)\operatorname{lm}(g_k))\\
&< T.
\end{aligned}
$$

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

$$p=H_1g_1+\cdots+H_mg_m$$

such that for each $k=1,2,\ldots,m$ $H_k=0$ or $\operatorname{lm}(H_k)\operatorname{lm}(g_k)\le\operatorname{lm}(p)$. Both sides of the equation must simplify to the same polynomial, with the same leading variable, so at least one $k$ has $\operatorname{lm}(H_k)\operatorname{lm}(g_k)=\operatorname{lm}(p)$; that is, $\operatorname{lm}(g_k)\mid\operatorname{lm}(p)$. Since $p$ was arbitrary, $G$ satisfies the definition of a Gröbner basis. □

EXERCISES.

EXERCISE 9.28. Show that $G = \left(x^2+y^2-4, xy-1, x+y^3-4y, -y^4+4y^3-1\right)$ is a Gröbner basis.

EXERCISE 9.29. Show that for any non-constant polynomial $f$, $F = (f, f+1)$ is not a Gröbner basis.

EXERCISE 9.30. Show that every list of monomials is a Gröbner basis.

EXERCISE 9.31. 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 modulo $F$.
(b) Show that there exist $q_1, q_2 \in \mathbb{F}[x,y]$ such that $p = q_1f_1 + q_2f_2$. *Hint:* use part (a).
(c) Generalize the argument of (b) to prove Lemma 9.27.

EXERCISE 9.32. For $G$ to be a Gröbner basis, Definition 9.18 requires that every polynomial in the ideal generated by $G$ be top-reducible by some element of $G$. We call these polynomials **redundant elements of the basis**.

(a) The Gröbner basis of Exercise 9.28 has redundant elements. Find a subset $G_{\text{minimal}}$ of $G$ that contains no redundant elements, but is still a Gröbner basis.
(b) Describe the method you used to find $G_{\text{minimal}}$.
(c) Explain why redundant polynomials are not required to satisfy Definition 9.18. That is, if we know that $G$ is a Gröbner basis, then we could remove redundant elements to obtain a smaller list, $G_{\text{minimal}}$, which is also a Gröbner basis *of the same ideal*. *Hint:* 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 9.27 is also useful.

## 9.3. GRÖBNER BASES FOR NON-LEXICOGRAPHIC TERM ORDERINGS

In the previous section, we defined and considered the Gröbner basis property using only the lexicographic ordering. This is not the only way to order monomials, and in this section we explore other ways to identify the leading term of a polynomial. How do we know this? If you look carefully at the proof of Theorem 9.24, you should notice that *it does not use any "lexicographic" properties of the lexicographic ordering!* It uses only the facts that (a) you *can* identify a "leading monomial", and (b) certain natural properties of polynomial multiplication and addition "preserve" the leading monomial. We now identify and generalize these properties of the lexicographic ordering in order to describe a generic ordering on monomials.

DEFINITION 9.33. An **admissible ordering** $<$ on the set $\mathbb{M}$ of monomials over $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is a relation where each of the following holds for every $t, u, v \in \mathbb{M}$.

(O1) One of the following holds: $t < u$, $t = u$, or $t > u$.
(O2) If $t \mid u$, then $t \leq u$.
(O3) If $t > u$, then for any monomial $v$ over $\mathbf{x}$, $tv > uv$.

PROPOSITION 9.34. *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.*

(C) *The properties of the lexicographic ordering described in Proposition 9.23 hold for any admissible ordering.*

PROOF. For (A), you do it! See Exercise . For (B), the argument is identical to Proposition 9.16—after all, we now have (O1)–(O3) and (A), which were used in Proposition 9.16. For (C), the argument is identical to Proposition 9.23. □

We can now introduce an ordering that you haven't seen before.

DEFINITION 9.35. 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 9.36. 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 9.37. 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 9.38. 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 $i$ 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 9.39. Under grevlex, $x^3y^2 > x^2y^3$ because the total degrees are the same and $y^2 < y^3$. ◇

Aside from lexicographic and graded reverse lexicographic orderings, there are limitless ways to design an admissible ordering.

DEFINITION 9.40. Let $t \in \mathbb{M}$. Define the **exponent vector** $\mathbf{t} \in \mathbb{N}^n$ where $t_i = \deg_{x_i} t$. Let $M \in \mathbb{R}^{n \times n}$. We define the **weighted vector** $w(t) = M\mathbf{t}$.

EXAMPLE 9.41. 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 9.42. *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 9.43. *If a matrix $M$ satisfies (B) of Theorem 9.42, 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 9.44. In Example 9.41, 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 9.42. 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 $\alpha$ in row $i$, column $j$. The topmost nonzero entry $\beta$ 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 $i$th 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 $k$th row of $M$. For any $\mathbf{t} \in \mathbb{M}$, the $i$th 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 9.42.

PROOF OF THEOREM 9.42. *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 $i$th position. The product $M\mathbf{t} > M\mathbf{u}$ if the $i$th element of the top row of $M$ is negative, but this contradicts Proposition 9.34(A). For (MO1), observe that property (O1) of Definition 9.33 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 9.33 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 9.43 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 9.45. Find a matrix that represents the lexicographic term ordering.

EXERCISE 9.46. Show that $G$ of Exercise 9.28 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 9.47. 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 9.48. Can every admissible ordering can be represented by a matrix? Why or why not?

## 9.4. BUCHBERGER'S ALGORITHM TO COMPUTE A GRÖBNER BASIS

Algorithm 2 on page 171 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 9.49. 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 $yz + z^2 \in \langle G \rangle$. $\diamondsuit$

Thus we will adapt Algorithm 2 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

**Algorithm 3** Buchberger's algorithm to compute a Gröbner basis

**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 $P = \{(f, g) : \forall f, g \in G \text{ such that } f \neq g\}$
  **while** $P \neq \emptyset$
    Choose $(f, g) \in P$
    Remove $(f, g)$ from $P$
    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 $P \cup \{(h, r) : h \in G\}$
      Append $r$ to $G$
  **return** $G$

leading variables are the same. With non-linear polynomials, Buchberger's characterization (Theorem 9.24) 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 3.

THEOREM 9.50. *For any list of polynomials $F$ over a field, Buchberger's algorithm terminates with a Gröbner basis of $\langle F \rangle$.*

We cannot yet prove Theorem 9.50. 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. To show termination, we need to introduce an important property of some rings, called the Ascending Chain Condition.

DEFINITION 9.51. Let $R$ be a ring. If for every **ascending chain of ideals** $I_1 \subset I_2 \subset \cdots$ we can find an integer $k$ such that $I_k = I_{k+1} = \cdots$, then we say that the ring satisfies the **Ascending Chain Condition**.

REMARK. Another name for ring that satisfies the Ascending Chain Condition is **Noetherian**, after Emmy Noether.

PROPOSITION 9.52. *Each of the following holds.*

*(A) Any field $\mathbb{F}$ satisfies the Ascending Chain Condition.*
*(B) If a ring $R$ satisfies the Ascending Chain Condition, so does $R[x]$.*
*(C) If a ring $R$ satisfies the Ascending Chain Condition, so does $R[x_1, x_2, \ldots, x_n]$.*
*(D) For any field $\mathbb{F}$, $\mathbb{F}[x_1, x_2, \ldots, x_n]$ satisfies the Ascending Chain Condition.*

PROOF. (A) Recall from Exercise 7.67 on page 150 that a field has only two distinct ideals: the zero ideal, and the field itself. (Why? If an ideal $I$ of $\mathbb{F}$ is nonzero, then choose nonzero $a \in I$. Since $a^{-1} \in \mathbb{F}$, absorption implies that $1_{\mathbb{F}} = a \cdot a^{-1} \in I$. Then for any $b \in \mathbb{F}$, absorption again implies that $1_{\mathbb{F}} \cdot b \in I$.) Hence any ascending chain of ideals stabilizes either at the zero ideal or at $\mathbb{F}$.

(B) 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 $I_1 \subset I_2 \subset \cdots$ the set $I = \cup_{i=1}^{\infty} I_i$ is also an ideal (see Exercise 9.54), and is finitely generated, say $I = \langle f_1, \ldots, f_m \rangle$, which implies that the chain stabilizes at $I_M$ where $f_m \in I_m$. So let $I$ be an ideal that is not finitely generated, and choose $f_1, f_2, \ldots \in I$ in the following way: $f_1$ is of minimal degree in $I$; $f_2$ is of minimal degree in $I \backslash \langle f_1 \rangle$, $f_3$ is of minimal degree in $I \backslash \langle f_1, f_2 \rangle$, and so forth. Then $\langle f_1 \rangle \subset \langle f_1, f_2 \rangle \subset \cdots$ is an ascending chain of ideals. Denote the leading coefficient of $f_i$ by $a_i$ and let $J_i = \left\langle a_1, a_2, \ldots, a_j \right\rangle$. Since $R$ satisfies the Ascending Chain Condition, the ascending chain of ideals $J_1 \subset J_2 \subset \cdots$ stabilizes for some $m \in \mathbb{N}$. Thus $a_{n+1} = b_1 a_1 + \cdots + b_m a_m$ for some $b_1, \ldots, b_m \in \mathbb{F}$. Write $d_i = \deg_x f_i$ , and consider

$$p = b_1 f_1 x^{d_{m+1} - d_1} + \cdots + b_m f_m x^{d_{m+1} - d_m}.$$

Note that choosing the $f_i$'s to be of minimal degree implies that $d_{m+1} - d_i$ is nonnegative for each $i$. Moreover the leading term of $p$ is $a_{m+1} x^{d_{m+1}}$, so $f_{m+1} - p$ is a polynomial in the ideal $I$ that has degree smaller than $f_{m+1}$. However, $p \in \langle f_1, f_2, \ldots, f_m \rangle$ and $f_{m+1} \notin \langle f_1, f_2, \ldots, f_m \rangle$ implies that $f_{m+1} - p \notin \langle f_1, f_2, \ldots, f_m \rangle$, so $f_{m+1} - p \in I \backslash \langle f_1, f_2, \ldots, f_m \rangle$, contradicting the choice of minimality of $f_{m+1}$.

(C) Follows from (B) and 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.

(D) Follows from (A) and (C). □

We can now prove that Buchberger's Algorithm terminates correctly.

PROOF OF THEOREM 9.50. For *termination*, let $\mathbb{F}$ be a field, and $F$ a list of polynomials over $\mathbb{F}$. Designate

$$\begin{aligned}
I_0 &= \langle \operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_m) \rangle \\
I_1 &= \left\langle \operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_m), \operatorname{lm}(g_{m+1}) \right\rangle \\
I_2 &= \left\langle \operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_m), \operatorname{lm}(g_{m+1}), \operatorname{lm}(g_{m+2}) \right\rangle \\
&\vdots \\
I_i &= \left\langle \operatorname{lm}(g_1), \operatorname{lm}(g_2), \ldots, \operatorname{lm}(g_m), \operatorname{lm}(g_{m+1}), \operatorname{lm}(g_{m+2}), \ldots, \operatorname{lm}(g_{m+i}) \right\rangle
\end{aligned}$$

where $g_{m+i}$ is the $i$th polynomial added to $G$ by line 15 of Algorithm 3.

We claim that $I_0 \subset I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals. After all, a polynomial $r$ is added to the basis only when it is non-zero (line 13); 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 9.30 on page 185, any list of monomials is a Gröbner basis; hence

$$T = (\mathrm{lm}(g_1), \mathrm{lm}(g_2), \ldots, \mathrm{lm}(g_{m+i-1}))$$

is a Gröbner basis, and by Definition 9.18 every polynomial in $I_{i-1}$ is top-reducible by $T$. Since $p$ is not top-reducible by $T$, $\mathrm{lm}(p) \notin I_{i-1}$.

Thus $I_{i-1} \subsetneq I_i$, and $I_0 \subset I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals in $\mathbb{F}[x_1 x_2, \ldots, x_n]$. By Proposition 9.52 and Definition 9.51, 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 10 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

$$p = h_1 g_1 + \cdots + h_m g_m. \tag{9.4.1}$$

We consider three cases.

*Case* 1. There exists $i$ such that $\mathrm{lm}(h_i)\,\mathrm{lm}(g_i) = \mathrm{lm}(p)$.
In this case $\mathrm{lm}(g_i)$ divides $\mathrm{lm}(p)$, and we are done.

*Case* 2. For all $i = 1, 2, \ldots, m$, $\mathrm{lm}(h_i)\,\mathrm{lm}(g_i) = \mathrm{lm}(p)$.
This and Proposition 9.34 contradict equation (9.4.1), so this case cannot occur.

*Case* 3. There exists $i$ such that $\mathrm{lm}(h_i)\,\mathrm{lm}(g_i) > \mathrm{lm}(p)$.

Choose $i$ such that $\mathrm{lm}(h_i)\,\mathrm{lm}(g_i)$ is maximal among the monomials *and* $i$ is maximal among the indices. Write $t = \mathrm{lm}(h_i)\,\mathrm{lm}(g_i)$. To satisfy equation (9.4.1), $t$ must cancel with another term on the right hand side. Thus, there exists $j \neq i$ such that $t = \mathrm{lm}(h_j)\,\mathrm{lm}(g_j)$; choose such a $j$. We now show how to use the $S$-polynomial of $g_i$ and $g_j$ to rewrite equation (9.4.1) with a "smaller" representation.

Let $a \in \mathbb{F}$ such that

$$a \cdot \mathrm{lc}(h_j)\,\mathrm{lc}(g_j) = -\mathrm{lc}(h_i)\,\mathrm{lc}(g_i).$$

Thus

$$\mathrm{lc}(h_i)\,\mathrm{lm}(h_i)\,\mathrm{lc}(g_i)\,\mathrm{lm}(g_i) + a \cdot \mathrm{lc}(h_j)\,\mathrm{lm}(h_j)\,\mathrm{lc}(g_j)\,\mathrm{lm}(g_j) = \left[\mathrm{lc}(h_i)\,\mathrm{lc}(g_i) + a \cdot \mathrm{lc}(h_j)\,\mathrm{lc}(g_j)\right] \cdot t = 0.$$

By Lemma 9.19, $\mathrm{lc}(h_i)\,\mathrm{lm}(h_i)\,g_i + a \cdot \mathrm{lc}(h_j)\,\mathrm{lm}(h_j)\,g_j$ is a multiple of $\mathrm{Spol}(g_i, g_j)$; choose a constant $b \in \mathbb{F}$ and a monomial $t \in \mathbb{M}$ such that

$$\mathrm{lc}(h_i)\,\mathrm{lm}(h_i)\,g_i + a \cdot \mathrm{lc}(h_j)\,\mathrm{lm}(h_j g_j) = bt \cdot \mathrm{Spol}(g_i, g_j).$$

The algorithm has terminated, so it considered this $S$-polynomial and top-reduced it to zero with respect to $G$. By Lemma 9.27 there exist $q_1, \ldots, q_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that

$$\mathrm{Spol}(g_i, g_j) = q_1 g_1 + \cdots + q_m g_m$$

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 $k = 1, 2, \ldots, m$. Rewrite equation (9.4.1) in the following way:

$$\begin{aligned}
p &= h_1 g_1 + \cdots + h_m g_m \\
&= (h_1 g_1 + \cdots + h_m g_m) - bt \cdot \operatorname{Spol}\left(g_i, g_j\right) + bt \cdot (q_1 g_1 + \cdots + q_m g_m) \\
&= (h_1 g_1 + \cdots + h_m g_m) \\
&\quad - bt \cdot \left[\operatorname{lc}\left(g_j\right) \frac{\operatorname{lcm}\left(\operatorname{lm}(g_i), \operatorname{lm}\left(g_j\right)\right)}{\operatorname{lm}(g_i)} \cdot g_i - \operatorname{lc}(g_i) \frac{\operatorname{lcm}\left(\operatorname{lm}(g_i), \operatorname{lm}\left(g_j\right)\right)}{\operatorname{lm}\left(g_j\right)} \cdot g_j\right] \\
&\quad\quad + bt \cdot (q_1 g_1 + \cdots + q_m g_m).
\end{aligned}$$

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 $H_i$; likewise $\operatorname{lm}\left(H_j\right)\operatorname{lm}\left(g_j\right) < \operatorname{lm}\left(h_j\right)\operatorname{lm}\left(g_j\right)$. 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

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 (9.4.1) so that $\operatorname{lm}(h_k)\operatorname{lm}(g_k) < t$ for all $k = 1, 2, \ldots, m$.

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 9.34(B) on page 185, 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 9.53. Using $G$ of Exercise 9.28, compute a Gröbner basis with respect to the grevlex ordering.

EXERCISE 9.54. Show that for any ascending chain of ideals $I_1 \subset I_2 \subset \cdots$, their union $I = \cup_{i=1}^{\infty} I_i$ is also an ideal. *Hint:* Use the Ideal Theorem.

EXERCISE 9.55. Show that the ring of integers satisfies the Ascending Chain Condition. *Hint:* Use Exercise 7.62 on page 150, Exercise 7.63, and an important property of the integers.

EXERCISE 9.56. Following up on Exercises 9.46 and 9.53, 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 all the monomials in $x$ and $y$ on the $x$-$y$ plane by plotting $x^\alpha y^\beta$ at the point $(\alpha, \beta)$.

(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 9.57. 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 9.58. 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

$$\begin{array}{cl}
\begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2h & xyh & y^2h & xh^2 & yh^2 & h^3 \end{array} & \\
\begin{pmatrix}
1 & & 1 & & & & & -4 & & \\
 & 1 & & 1 & & & & & -4 & \\
 & & & & 1 & & 1 & & & -4 \\
 & 1 & & & & & & -1 & & \\
 & & 1 & & & & & & -1 & \\
 & & & & & 1 & & & & -1
\end{pmatrix} & \begin{array}{l} xf_1 \\ yf_1 \\ hf_1 \\ xf_2 \\ yf_2 \\ hf_2 \end{array}
\end{array}.$$

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 = macaulay_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 macaulay_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
```

## 9.5. ELEMENTARY APPLICATIONS OF GRÖBNER BASES

We now turn our attention to posing, and answering, questions that make Gröbner bases interesting. 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;
- $F \subset \mathcal{R}$;
- $V_F \subset \mathbb{F}$ 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 9.59 (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 $\mathrm{lm}(p)$ is top-reducible by some element of $G$. Let $g \in G$ such that $\mathrm{lm}(g) \mid \mathrm{lm}(p)$, and choose $c \in \mathbb{F}$ and $u \in \mathbb{M}$ such that $\mathrm{lc}(p)\,\mathrm{lm}(p) = cu \cdot \mathrm{lc}(g)\,\mathrm{lm}(g)$. Let $r_1$ be the result of the top-reduction; that is,

$$r_1 = p - cu \cdot g.$$

Then $\mathrm{lm}(r_1) < \mathrm{lm}(p)$ 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 $\mathrm{lm}(p)$ 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

$$\mathrm{lm}(p) > \mathrm{lm}(r_1) > \mathrm{lm}(r_2) > \cdots.$$

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 modulo $G$. 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 9.27 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 7.69 on page 150 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. (As with most of the remaining theorems of this section, we do not prove Theorem 9.60, but encourage the interested reader to look in [**CLO97**].)

THEOREM 9.60. *$F$ has common roots if and only if $G$ has no constant polynomials.*

Once we know common solutions exist, we want to know how many there are.

THEOREM 9.61. *There are finitely many complex solutions if and only if for each $i = 1, 2, \ldots, n$ we can find $g \in G$ and $\alpha \in \mathbb{N}$ such that* $\mathrm{lm}(g) = x_i^\alpha$.

EXAMPLE 9.62. Recall the system from Example 9.25,

$$F = \left(x^2 + y^2 - 4, xy - 1\right).$$

In Exercise 9.28 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 $x = \mathrm{lm}(g_1)$ and $y^4 = \mathrm{lm}(g_2)$, 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 9.63. *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 $\widehat{I} = I \cup \mathbb{F}$.)*

*(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 $\mathrm{lm}(g)$ divides $\mathrm{lm}(p)$. 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 9.64. 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 9.63 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 9.65. We can find the common solutions of the circle and the hyperbola in Figure 9.1 on page 175 using the Gröbner basis computed in Example 9.62. 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 9.66. 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 9.67. Determine the common roots of $x^2 + 1$ and $xy + 1$ in $\mathbb{C}$.

EXERCISE 9.68. Repeat the problem in $\mathbb{Z}_2$.

## 9.6. THE GEBAUER-MÖLLER ALGORITHM TO COMPUTE A GRÖBNER BASIS

Buchberger's algorithm (Algorithm 3 on page 190) 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 14 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 9.69. Let $p = x^2 + 2xy + 3x$ and $q = y^2 + 2x + 1$. Consider any ordering such that $\operatorname{lm}(p) = x^2$ and $\operatorname{lm}(q) = y^2$. 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):

$$\begin{aligned} S &= y^2 p - x^2 q \\ &= 2\mathbf{xy^3} - 2x^3 + 3xy^2 - x^2. \end{aligned}$$

This $S$-polynomial top-reduces to zero:

$$\begin{aligned} S - 2xyq &= \left(3xy^2 - 2x^3 - x^2\right) - \left(4x^2y + 2xy\right) \\ &= -2\mathbf{x^3} - 4x^2y + 3xy^2 - x^2 - 2xy; \end{aligned}$$

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

$$\begin{aligned} (S - 2xyq + 2xp - 3xq) + p &= (-2xy - 3x) + (2xy + 3x) \\ &= 0. \diamondsuit \end{aligned}$$

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:

$$S = -\left(q - \operatorname{lc}(q)\operatorname{lm}(q)\right) \cdot p + \left(p - \operatorname{lc}(p)\operatorname{lm}(p)\right) \cdot q.$$

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

$$S = -\operatorname{tts}(q) \cdot p + \operatorname{tts}(q) \cdot p.$$

If this were true in general, it might—*might*—be helpful.

LEMMA 9.70 (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*

$$S = -\operatorname{tts}(q) \cdot p + \operatorname{tts}(p) \cdot q.$$

PROOF. Since $u$ and $v$ have no common variables, $\operatorname{lcm}(u, v) = uv$. Thus the $S$-polynomial of $p$ and $q$ is

$$\begin{aligned}
S &= \operatorname{lc}(q) \cdot \frac{uv}{u} \cdot (\operatorname{lc}(p) \cdot u + \operatorname{tts}(p)) - \operatorname{lc}(p) \cdot \frac{uv}{v} \cdot (\operatorname{lc}(q) \cdot v + \operatorname{tts}(q)) \\
&= \operatorname{lc}(q) \cdot v \cdot \operatorname{tts}(p) - \operatorname{lc}(p) \cdot u \cdot \operatorname{tts}(q) \\
&= \operatorname{lc}(q) \cdot v \cdot \operatorname{tts}(p) - \operatorname{lc}(p) \cdot u \cdot \operatorname{tts}(q) + [\operatorname{tts}(p) \cdot \operatorname{tts}(q) - \operatorname{tts}(p) \cdot \operatorname{tts}(q)] \\
&= \operatorname{tts}(p) \cdot [\operatorname{lc}(q) \cdot v + \operatorname{tts}(q)] - \operatorname{tts}(q) \cdot [\operatorname{lc}(p) \cdot u + \operatorname{tts}(p)] \\
&= \operatorname{tts}(p) \cdot q - \operatorname{tts}(q) \cdot p.
\end{aligned}$$

□

Lemma 9.70 is not quite enough. Recall Theorem 9.24 on page 181, the characterization theorem of a Gröbner basis:

THEOREM (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* $1 \le i < j \le m$, $\operatorname{Spol}(g_i, g_j)$ top-reduces to zero with respect to $G$.

To satisfy Theorem 9.24, we have to show that the $S$-polynomials top-reduce to zero. However, the proof of Theorem 9.24 used Lemma 9.27:

LEMMA. *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* $\operatorname{lm}(q_k) \operatorname{lm}(g_k) \le \operatorname{lm}(p)$.

We can describe this in the following way, due to Daniel Lazard:

THEOREM 9.71 (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* $1 \le i < j \le m$, $\operatorname{Spol}(g_i, g_j)$ top-reduces to zero with respect to $G$.

*(C)* *For any pair* $i, j$ *with* $1 \le i < j \le m$, $\operatorname{Spol}(g_i, g_j)$ *has the form*

$$\operatorname{Spol}(g_i, g_j) = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m$$

*and for each* $k = 1, 2, \ldots, m$, $q_k = 0$ *or* $\operatorname{lm}(q_k) \operatorname{lm}(g_k) < \operatorname{lcm}(\operatorname{lm}(p), \operatorname{lm}(q))$.

PROOF. That (A) is equivalent to (B) was the substance of Buchberger's characterization. That (B) implies (C) is a consequence of Lemma 9.27. That (C) implies (A) is implicit in the proof of Buchberger's characterization: you will extract it in Exercise 9.79. □

The form of an $S$-polynomial described in (C) of Theorem 9.71 is important enough to identify with a special term.

DEFINITION 9.72. 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 with respect to** $G$ if there exist $q_1,q_2,\ldots,q_m$ such that (C) of Theorem 9.71 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 9.73. *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 $1\le i<j\le m$, one of the following holds:*
- (B1) The leading monomials of $g_i$ and $g_j$ have no common variables.
- (B2) $\mathrm{Spol}\left(g_i,g_j\right)$ 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 9.70) implies that

$$\mathrm{Spol}\left(g_i,g_j\right)=q_1g_1+\cdots+q_mg_m \tag{9.6.1}$$

where $q_i=-\mathrm{tts}\left(g_j\right)$, $q_j=\mathrm{tts}\left(g_i\right)$, and $q_k=0$ for $k\neq i,j$. Notice that

$$\mathrm{lm}\left(q_i\right)\mathrm{lm}\left(g_i\right)=\mathrm{lm}\left(\mathrm{tts}\left(g_j\right)\right)\cdot\mathrm{lm}\left(g_i\right)<\mathrm{lm}\left(g_j\right)\mathrm{lm}\left(g_i\right)=\mathrm{lcm}\left(\mathrm{lm}\left(g_i\right),\mathrm{lm}\left(g_j\right)\right).$$

Thus 9.6.1 is an $S$-representation of $\mathrm{Spol}\left(g_i,g_j\right)$, so $(i,j)\in\widehat{P}$. If $(i,j)$ satisfes (B2), then Lemma 9.27 implies that $(i,j)\in\widehat{P}$ 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 9.28 and 9.53.

We need, therefore, a stronger criterion. The next one is a little harder to discover, so we present it directly.

LEMMA 9.74 (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 $\mathrm{lcm}\,(u,v)$, then the $S$-polynomial of $p$ and $q$ has the form*

$$S=\frac{\mathrm{lc}\,(q)\cdot\mathrm{lcm}\,(u,v)}{\mathrm{lc}\,(f)\cdot\mathrm{lcm}\,(t,u)}\cdot\mathrm{Spol}\,(p,f)+\frac{\mathrm{lc}\,(p)\cdot\mathrm{lcm}\,(u,v)}{\mathrm{lc}\,(f)\cdot\mathrm{lcm}\,(t,v)}\cdot\mathrm{Spol}\,(f,q). \tag{9.6.2}$$

PROOF. First we show that the fractions in equation (9.6.2) reduce to monomials. Let $x$ be any variable. Since $t$ divides $\mathrm{lcm}\,(u,v)$, we know that

$$\deg_x t\le\deg_x\mathrm{lcm}\,(u,v)=\max\left(\deg_x u,\deg_x v\right).$$

(See Exercise 9.78.) Thus

$$\deg_x\mathrm{lcm}\,(t,u)=\max\left(\deg_x t,\deg_x u\right)\le\max\left(\deg_x u,\deg_x v\right)=\deg_x\mathrm{lcm}\,(u,v).$$

A similar argument shows that

$$\deg_x \operatorname{lcm}(t,v) \le \deg_x \operatorname{lcm}(u,v).$$

Thus the fractions in (9.6.2) reduce to monomials.

It remains to show that (9.6.2) 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

$$\begin{aligned}\frac{\operatorname{lc}(q)\cdot L_{u,v}}{\operatorname{lc}(f)\cdot L_{t,u}}\cdot S_{p,f}+\frac{\operatorname{lc}(p)\cdot L_{u,v}}{\operatorname{lc}(f)\cdot L_{t,v}}\cdot S_{f,q} &= \operatorname{lc}(q)\cdot\frac{L_{u,v}}{u}\cdot p\\ &\qquad -\cancel{\frac{\operatorname{lc}(p)\cdot\operatorname{lc}(q)}{\operatorname{lc}(f)}\cdot\frac{L_{u,v}}{t}}\cdot f\\ &\qquad +\cancel{\frac{\operatorname{lc}(p)\cdot\operatorname{lc}(q)}{\operatorname{lc}(f)}\cdot\frac{L_{u,v}}{t}}\cdot f\\ &\qquad -\operatorname{lc}(p)\cdot\frac{L_{u,v}}{v}\cdot q\\ &= S_{p,q}.\end{aligned}$$

□

How does this help us?

COROLLARY 9.75. *Let $g_1,g_2,\dots,g_m\in\mathbb{F}[x_1,x_2,\dots,x_n]$. The following are equivalent.*

*(A) $G=(g_1,g_2,\dots,g_m)$ is a Gröbner basis of the ideal $I=\langle g_1,g_2,\dots,g_m\rangle$.*

*(B) For any pair $i,j$ with $1\le i<j\le m$, 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*

- $\operatorname{lm}(g_k)$ *divides* $\operatorname{lcm}\left(\operatorname{lm}(g_i),\operatorname{lm}\left(g_j\right)\right)$*;*
- $\operatorname{Spol}(g_i,g_k)$ *has an $S$-representation with respect to $G$; and*
- $\operatorname{Spol}\left(g_k,g_j\right)$ *has an $S$-representation with respect to $G$.*

(B3) $\operatorname{Spol}\left(g_i,g_j\right)$ top-reduces to zero with respect to $G$.

PROOF. We need merely show that (B2) implies the existence of an $S$-representation of $\operatorname{Spol}\left(g_i,g_j\right)$ with respect to $G$; Lazard's characterization and the proof of Corollary 9.73 supply the rest. So assume (B2). Choose $h_1,h_2,\dots,h_m$ such that

$$\operatorname{Spol}(g_i,g_k)=h_1g_1+\cdots+h_mg_m$$

and for each $\ell=1,2,\dots,m$ we have $h_\ell=0$ or

$$\operatorname{lm}(h_\ell)\operatorname{lm}(g_\ell)<\operatorname{lcm}(\operatorname{lm}(g_i),\operatorname{lm}(g_k)).$$

Also choose $q_1,q_2,\dots,q_m$ such that

$$\operatorname{Spol}\left(g_k,g_j\right)=q_1g_1+\cdots+q_mg_m$$

and for each $\ell=1,2,\dots,m$ we have $q_\ell=0$ or

$$\operatorname{lm}(q_\ell)\operatorname{lm}(g_\ell)<\operatorname{lcm}\left(\operatorname{lm}(g_k),\operatorname{lm}\left(g_j\right)\right).$$

Write $L_{a,b} = \operatorname{lcm}(\operatorname{lm}(g_a), \operatorname{lm}(g_b))$. Buchberger's lcm criterion tells us that

$$\operatorname{Spol}(g_i, g_j) = \frac{\operatorname{lc}(g_j) \cdot L_{i,j}}{\operatorname{lc}(g_k) \cdot L_{i,k}} \cdot \operatorname{Spol}(g_i, g_k) + \frac{\operatorname{lc}(g_i) \cdot L_{i,j}}{\operatorname{lc}(g_k) \cdot L_{j,k}} \cdot \operatorname{Spol}(g_k, g_j).$$

For $i = 1, 2, \ldots, m$ let

$$H_i = \frac{\operatorname{lc}(g_j) \cdot L_{i,j}}{\operatorname{lc}(g_k) \cdot L_{i,k}} \cdot h_i + \frac{\operatorname{lc}(g_i) \cdot L_{i,j}}{\operatorname{lc}(g_k) \cdot L_{j,k}} \cdot q_i.$$

Substitution implies that

$$\operatorname{Spol}(g_i, g_j) = H_1 g_1 + \cdots + H_m g_m. \tag{9.6.3}$$

In addition, for each $i = 1, 2, \ldots, m$ we have $H_i = 0$ or

$$\begin{aligned}
\operatorname{lm}(H_i)\operatorname{lm}(g_i) &\le \max\left(\frac{L_{i,j}}{L_{i,k}} \cdot \operatorname{lm}(h_i), \frac{L_{i,j}}{L_{j,k}} \cdot \operatorname{lm}(q_i)\right) \cdot \operatorname{lm}(g_i) \\
&= \max\left(\frac{L_{i,j}}{L_{i,k}} \cdot \operatorname{lm}(h_i)\operatorname{lm}(g_i), \frac{L_{i,j}}{L_{j,k}} \cdot \operatorname{lm}(q_i)\operatorname{lm}(g_i)\right) \\
&< \max\left(\frac{L_{i,j}}{\cancel{L_{i,k}}} \cdot \cancel{L_{i,k}}, \frac{L_{i,j}}{\cancel{L_{j,k}}} \cdot \cancel{L_{j,k}}\right) \\
&= L_{i,j} \\
&= \operatorname{lcm}(\operatorname{lm}(g_i), \operatorname{lm}(g_j)).
\end{aligned}$$

Thus equation (9.6.3) is an $S$-representation of $\operatorname{Spol}(g_i, g_j)$.

The remainder of the corollary follows as described. □

It is not hard to exploit Corollary 9.75 and modify Buchberger's algorithm in such a way as to take advantage of these criteria. The result is Algorithm 4. 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 5 and 6). This implementation attempts to apply Buchberger's criteria as quickly as possible. Thus the first `while` loop of Algorithm 6 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 9.32).

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

**Algorithm 4** 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 $Done = \{\}$
  **while** $P \neq \emptyset$
    Choose $(f, g) \in P$
    Remove $(f, g)$ from $P$
    **if** $\operatorname{lm}(f)$ and $\operatorname{lm}(g)$ share at least one variable — check gcd criterion
      **if not** ($\exists p \neq f, g$ such that $\operatorname{lm}(p)$ divides $\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$ **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** $G$

criteria. Nevertheless, the Gebauer-Möller algorithm continues to reduce a large number of $S$-polynomials to zero.

EXERCISES.

EXERCISE 9.76. In Exercise 9.28 on page 185 you computed the Gröbner basis for the system

$$F = \left(x^2 + y^2 - 4, xy - 1\right)$$

in the lexicographic ordering using Algorithm 3 on page 190. Review your work on that problem, and identify which pairs $(i, j)$ would not generate an $S$-polynomial if you had used Algorithm 4 instead.

EXERCISE 9.77. 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 $C$, $D$, $E$, $G_{\text{new}}$, and $P_{\text{new}}$ after each `while` loop in Algorithm 6 on page 208.

EXERCISE 9.78. 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 9.79. Study the proof of Buchberger's characterization, and extract from it a proof that (C) implies (A) in Theorem 9.71.

**Algorithm 5** 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 $P := \{\}$
  **while** $F \neq \emptyset$
    Let $f \in F$
    Remove $f$ from $F$
    — See Algorithm 6 for a description of Update
    $G, P := \text{Update}(G, P, f)$
  **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** $h \neq 0$
      $G, P := \text{Update}(G, P, h)$
  **return** $G$

## 9.7. $d$-GRÖBNER BASES AND FAUGÈRE'S ALGORITHM F4 TO COMPUTE A GRÖBNER BASIS

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 9.58 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. 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

$$F = \left(x^2 + y^2 - 4h^2, xy - h^2\right),$$

**Algorithm 6** Update the Gebauer-Möller pairs

**inputs**
  $G_{\text{old}}$, a list of polynomials in $n$ variables, whose coefficients are from a field $\mathbb{F}$.
  $P_{\text{old}}$, a set of critical pairs of elements of $G_{\text{old}}$
  a non-zero polynomial $p$ in $\langle G_{\text{old}} \rangle$
**outputs**
  $G_{\text{new}}$, a (possibly different) list of generators of $\langle G_{\text{old}} \rangle$.
  $P_{\text{old}}$, a set of critical pairs of $G_{\text{new}}$
**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
  **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
  **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
      $E := E \cup (p,g)$
  — $P_{\text{int}}$ is the result of pruning pairs of $P_{\text{old}}$ using Buchberger's lcm criterion
  Let $P_{\text{int}} := \{\}$
  **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 $P_{\text{int}}$
  — 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 $G_{\text{new}} := \{\}$
  **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 $G_{\text{new}}$
  Add $p$ to $G_{\text{new}}$
  **return** $G_{\text{new}}, P_{\text{new}}$

the usual degree-3 ordered Macaulay matrix would be

$$\begin{array}{cl} \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2h & xyh & y^2h & xh^2 & yh^2 & h^3 \end{array} & \\ \left(\begin{array}{cccccccccc} 1 & & 1 & & & & & -4 & & \\ & 1 & & 1 & & & & & -4 & \\ & & & & 1 & & 1 & & & -4 \\ & 1 & & & & & & -1 & & \\ & & 1 & & & & & & -1 & \\ & & & & & 1 & & & & -1 \end{array}\right) & \begin{array}{l} xf_1 \\ yf_1 \\ hf_1 \\ xf_2 \\ yf_2 \\ hf_2 \end{array} \end{array}.$$

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

$$\begin{array}{cl} \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2h & xyh & y^2h & xh^2 & yh^2 & h^3 \end{array} & \\ \left(\begin{array}{cccccccccc} & 1 & & 1 & & & & & -4 & \\ & 1 & & & & & & -1 & & \end{array}\right) & \begin{array}{l} yf_1 \\ xf_2 \end{array} \end{array}.$$

Triangularizing it results in

$$\begin{array}{cl} \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2h & xyh & y^2h & xh^2 & yh^2 & h^3 \end{array} & \\ \left(\begin{array}{cccccccccc} & 1 & & 1 & & & & & -4 & \\ & & & 1 & & & & 1 & 4 & \end{array}\right) & \begin{array}{l} yf_1 \\ yf_1 - xf_2 \end{array} \end{array},$$

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 $y^2 f_2$ and $xf_3$. The non-leading monomial of $y^2 f_2$ is $y^2 h^2$, 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 $h^2 f_1$ and $h^2 f_2$. The non-leading monomials of $h^2 f_1$ 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 $h^2 f_2$ is $h^4$.

We have now identified all the polynomials that *might* be necessary in the top-reduction of the $S$-polynomial for $(f_2, f_3)$:

$$y^2 f_2, xf_3, h^2 f_1, \text{ and } h^2 f_2.$$

We build the matrix using rows that correspond to these polynomials, resulting in

$$\begin{array}{cl} \begin{array}{ccccc} xy^3 & x^2h^2 & xyh^2 & y^2h^2 & h^2 \end{array} & \\ \left(\begin{array}{ccccc} 1 & & & -1 & \\ 1 & 1 & 4 & & \\ & 1 & & 1 & -4 \\ & & 1 & & -1 \end{array}\right) & \begin{array}{l} y^2 f_2 \\ xf_3 \\ h^2 f_1 \\ h^2 f_2 \end{array} \end{array}.$$

Triangularizing this matrix results in (step-by-step)

$$\begin{array}{cc} \begin{array}{ccccc} xy^3 & x^2h^2 & xyh^2 & y^2h^2 & h^2 \end{array} & \\ \left(\begin{array}{ccccc} 1 & & & -1 & \\ & -1 & -4 & -1 & \\ & 1 & & 1 & -4 \\ & & 1 & & -1 \end{array}\right) & \begin{array}{l} y^2f_2 \\ y^2f_2-xf_3 \\ h^2f_1 \\ h^2f_2 \end{array} \end{array};$$

$$\begin{array}{cc} \begin{array}{ccccc} xy^3 & x^2h^2 & xyh^2 & y^2h^2 & h^2 \end{array} & \\ \left(\begin{array}{ccccc} 1 & & & -1 & \\ & & -4 & 0 & -4 \\ & 1 & & 1 & -4 \\ & & 1 & & -1 \end{array}\right) & \begin{array}{l} y^2f_2 \\ y^2f_2-xf_3+h^2f_1 \\ h^2f_1 \\ h^2f_2 \end{array} \end{array};$$

and finally

$$\begin{array}{cc} \begin{array}{ccccc} xy^3 & x^2h^2 & xyh^2 & y^2h^2 & h^2 \end{array} & \\ \left(\begin{array}{ccccc} 1 & & & -1 & \\ & & & & 0 \\ & 1 & & 1 & -4 \\ & & 1 & & -1 \end{array}\right) & \begin{array}{l} y^2f_2 \\ y^2f_2-xf_3+h^2f_1+4h^2f_2 \\ h^2f_1 \\ h^2f_2 \end{array} \end{array}.$$

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 4 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 7 describes a simplified F4 algorithm. The approach outlined has an important advantage that we have not yet explained.

DEFINITION 9.80. 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 9.81. 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. $\diamond$

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 9.82. 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

$$S_{12} = yh^2 - xh^2,$$

**Algorithm 7** 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 $d := 1$
  **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 $R := \{tp, uq : (p,q) \in Q \text{ and } t = L_{p,q}/\operatorname{lm}(p), u = L_{p,q}/\operatorname{lm}(q)\}$
    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 $G_{\text{new}}$ 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** $G$

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 9.59.

THEOREM 9.83. *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 9.27 implies that $p \in I$. $\square$

EXERCISES.

EXERCISE 9.84. Use the simplified F4 algorithm given here to compute a $d$-Gröbner bases for $\left\langle x^2y - z^2h, xz^2 - y^2h, yz^3 - x^2h^2 \right\rangle$ for $d \leq 6$. Use the grevlex term ordering with $x > y > z > h$.

EXERCISE 9.85. Given a non-homogeneous polynomial system $F$, describe how you could use the simplified F4 to compute a non-homogeneous Gröbner basis of $\langle F \rangle$.

# Part 3

# Appendices

CHAPTER 10

# Where can I go from here?

## 10.1. Advanced group theory

Galois theory [**Rot98**], representation theory, other topics [**AF05**, **Rot06**]

## 10.2. Advanced ring theory

Commutative algebra [**GPS05**], algebraic geometry [**CLO97**, **CLO98**], non-commutative algebra

## 10.3. Applications

General [**LP98**], coding theory, cryptography, computational algebra [**vzGG99**]

# Bibliography


[AF05] Marlow Anderson and Todd Feil. *A First Course in Abstract Algebra*. Chapman and Hall/CRC, second edition, 2005.

[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.

[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.

[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.

[Lyx09] Lyx Team. *Lyx*, 2008–2009. 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.html`.

[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.

# Index