JOURNAL OF INQUIRY-BASED LEARNING IN MATHEMATICS
No. **3**, (Apr. 2007)

Theory of Groups

David M. Clark

SUNY New Paltz

Contents

Acknowledgments

This guide was written under the auspices of SUNY New Paltz. The author gratefully acknowledges Harry Lucas and the Educational Advancement Foundation for their support, Allison Vandenbrul for her help in the preparation of the included graphics, and the referee for many useful suggestions. He also wishes to acknowledge the hard work of the many SUNY New Paltz students whose efforts and feedback have led to the refined guide that is now before you.

DMC

To the Instructor

This guide was written for a two semester senior level introductory course in group theory at SUNY New Paltz. The first semester is required of all mathematics and mathematics secondary education majors, with the second semester available as an elective. For most students in these classes this is a first serious course requiring them to prove theorems on their own. Students with prior experience would be likely to move through it more quickly. This guide was also used at a considerably more competitive university by another instructor who completed it in one semester.

You will find here 105 problems and theorems which students do outside of class and present in class. I discuss each solution after it is presented, and ask all of the students to write up a correct version of each in a neatly bound portfolio that must be complete by the end of the semester. Scattered problems and theorems are not presented in class, or not presented in full, but are instead left for all students to do on their own. During the semester students give me their portfolios to check as often as they like, and some require multiple tries before they are able to do certain assignments correctly. I require the portfolios to be completed and handed in at the end of each chapter. I check that it is complete and read carefully only those few that were not done in class.

The first chapter offers students an opportunity to familiarize themselves with an assortment of particular groups, finite and infinite, commutative and non-commutative. The tables created in Problem 1 are valuable references throughout the course. Problems 2 and 3 provide a good reminder that a counterexample, and not a failed proof, is necessary to show that a universal property does not hold. Problem 5 can be done laboriously from scratch, or efficiently for students who remember some basic linear algebra.

Building on the first chapter, the second gives a sequence of elementary theorems of abstract group theory. As much as I possibly can, I try to draw on experimental evidence from our examples to get students to state conjectures and then prove them formally. Corollary 11 is the first good example of this. For finite groups, Theorems 12, 14 and 15 are three ways of saying that the rows and columns of a group table are permutations. Theorem 16 begins a central theme of characterizing groups of different finite orders, and foreshadows the notions of equivalence relation and isomorphism.

In Chapter 3 we study cyclic groups. Lemma 22 is used in Problem 23 to give a bare hands proof that every subgroup of $\mathbf{Z}_n$ is cyclic when $n = 12$. Imagining doing this rather laborious computation for other values of n helps my students appreciate the value of abstract mathematics when later they prove Theorem 32. Problem 25 is another good example of an empirical conjecture, and the correct answer to the last question appears to be 'No' until they reach the last theorem of the chapter.

In Chapter 4 we pull LaGrange's Theorem out of some more concrete arguments. Theorem 16 initiates the broad question as to which values of n have the property that every n–element group is cyclic, that is, for which finite cardinalities are the group axioms categorical. Theorems 36 and 37 say that this is the case for 5 and 7 and lead to a conjecture in Problem 40 that is later proven as Theorem 47. Meanwhile, the arguments of Theorems 36 and 37 suggest the idea of coset decomposition and LaGrange's Theorem. Problem 39 foreshadows Theorem 48. The chapter ends by asking the students to try to answer the opening question for numbers up to 60.

Chapter 5, Equivalence Relations, could be skipped if students come with a good knowledge of this topic. I find that they rarely do, as it is often presented in elementary courses before they have enough examples to draw from to make the concept meaningful. I only pursue the final question in the chapter if students choose to work on it.

The level of abstraction steps up in Chapter 6, where the emphasis is on isomorphism rather than homomorphism. Theorem 65 now makes it possible to make precise the problem of classification of finite groups initiated in Theorem 16. This theme culminates in Problem 81, which adds to the results of Problem 49. I count on Chapter 7 to give an entertaining introduction to quotient groups.

Rather than devising a superficial overview of groups, rings, fields and linear spaces, I prefer to give my students an in depth experience with group theory alone. My belief is that this will give them a much better sense of what algebra is about. To compensate for these omissions, the final Chapter 8 introduces other algebraic systems with an indication as to how the basic notions of subalgebra, isomorphism and homomorphism can be applied.

David Clark
clarkd@newpaltz.edu
April, 2005

Chapter 1

Concrete Groups

A **binary operation on a set G** is a rule $*$ which associates with every pair of elements a and b of **G** a unique element $a*b$ of **G**. More formally, a binary operation $*$ on **G** is a function $*: \mathbf{G}\times\mathbf{G}\to\mathbf{G}$ from the cartesian product

$$\mathbf{G}\times\mathbf{G} := \{(a,b) \mid a,b\in\mathbf{G}\}$$

into **G**. Note that ":=" means that the expression on the left is being defined as an abbreviation for the expression on the right. We write "$a*b$" to denote the image $*(a,b)$ of (a,b) under $*$. Abstract algebra has primarily grown out of the study of binary operations, and of the features common to many familiar binary operations. Binary operations abound in mathematics, as the examples below illustrate.

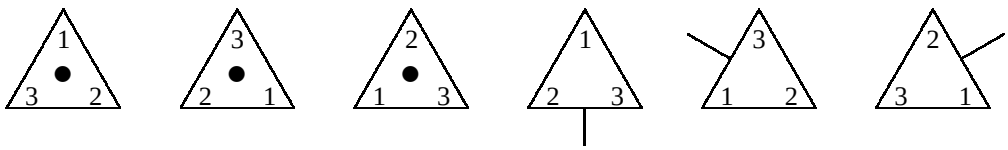
1. **Addition** $+$, **subtraction** $-$ and **multiplication** $\cdot$ are binary operations on the set **R** of real numbers and, suitably restricted, on the set **Z** of integers. Notice that **division** $\div$ is not a binary operation on either **R** or **Z** since $a\div b$ is not defined when $b=0$.

2. Let S be a set and let $P(S)$ denote the collection of subsets of S, called the **power set** of S. Then **intersection** $\cap$, **union** $\cup$, and **set difference** $\sim$ are binary operations on $P(S)$. Another important binary operation on $P(S)$ is the **symmetric difference**, $\oplus$, defined as

   $$A\oplus B := \{x\in S \mid x \text{ is in either } A \text{ or } B \text{ but not both.}\},$$

   that is, $A\oplus B = (A\cup B)\sim(A\cap B)$.

3. Let $\mathbf{S}_3$ denote the set of **permutations** of the set $\{1,2,3\}$, that is, one-to-one and onto functions from $\{1,2,3\}$ to itself. **Composition** $\circ$ forms a binary operation on $\mathbf{S}_3$ since the composition of two permutations is again a permutation. The set $\{1,2,3\}$ has exactly 6 permutations, illustrated below as rigid motions of an equilateral triangle.



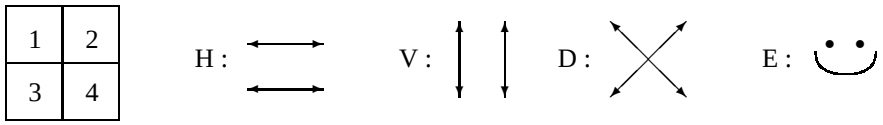
$e=\left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right)$ $a=\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$ $b=\left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)$ $c=\left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$ $d=\left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$ $f=\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$

Here a permutation g is represented by putting corner x in the $g(x)$ position, for $x = 1,2,3$. For example, a is achieved by starting in the e configuration and rotating the triangle clockwise 120 degrees. The product $a \circ f = d$ is realized by doing f first and then a: we flip the triangle over the diagonal through corner 3 (f), and then rotate it clockwise 120 degrees (a), as we have

$$(a \circ f)(1) = a(f(1)) = a(2) = 3 = d(1)$$
$$(a \circ f)(2) = a(f(2)) = a(1) = 2 = d(2)$$
$$(a \circ f)(3) = a(f(3)) = a(3) = 1 = d(3).$$

4. The set $\mathbf{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$ denotes the numbers on a clock, where 0 replaces 12. We define $a +_{12} b$ to be the hour that is b hours after hour a. For example, $10 +_{12} 7 = 5$ since 7 hours after 10 o'clock is 5 o'clock.

5. Consider a 2×2 "chess board" on which you are allowed to make four different moves:



H move horizontally (1 to 2, 2 to 1, 3 to 4 or 4 to 3),

V move vertically (1 to 3, 3 to 1, 2 to 4 or 4 to 2),

D move diagonally (1 to 4, 4 to 1, 2 to 3 or 3 to 2), or

E stay in place.

Let $\mathbf{K}_4 = \{E,H,V,D\}$ and let $X * Y$ be the move achieved by doing Y first and then doing X.

6. Recall that the **determinant** of a 2×2 matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is the number $|A| := ad - bc$. Let $\mathbf{M}_1$ be the set of 2×2 matrices with determinant 1 under the usual matrix multiplication $\bullet$ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ cp+ds & cq+ds \end{pmatrix}$$

A **binary system** consists of a set $\mathbf{G}$ together with a binary operation $* : \mathbf{G} \times \mathbf{G} \to \mathbf{G}$ on $\mathbf{G}$. If $\mathbf{G}$ is a finite set with n elements, we can fully define a binary operation $*$ with an n-by-n table. We list the elements of $\mathbf{G}$ as labels down the left side of the table and again across the top. Then the entry in the row labeled x and column labeled y is the value of $x * y$.

Constructing tables for a few sample finite binary systems provides a good opportunity to build some concrete intuition about their behavior before we begin to study them abstractly. We will make frequent reference to the examples below in the future.

Problem 1. *Using a separate sheet for each one, construct a table for the following binary systems:*

(i) $\mathbf{K}_4 = \{E,H,V,D\}$ *with* $*$,

(ii) $\mathbf{Z}_{12}$ *with* $+_{12}$*, the clock arithmetic,*

(iii) $\mathbf{P}_{abc}$ *with* $\oplus$*, the system of 8 subsets of the set* $\{a,b,c\}$ *under symmetric difference, and*

(iv) $\mathbf{S}_3$ *with* $\circ$*, the rigid motions of an equilateral triangle.* (*It will help to use a real triangle with a* $\bullet$ *on the top side!*)

Many operations have special properties that enhance our ability to do computations within them. A binary operation $*$ is **associative** if

$$a*(b*c) = (a*b)*c \quad \text{for every } a,b,c \in \mathbf{G}.$$

If $a,b,c \in \mathbf{G}$, then the expression "$a*b*c$" is in general ambiguous since it could mean either $a*(b*c)$ or $(a*b)*c$. When we know that $\mathbf{G}$ is associative, we generally omit the parentheses since $a*b*c$ will have the same value whichever way we interpret it.

We say that $\mathbf{G}$ is **commutative** if

$$a*b = b*a \quad \text{for every } a,b \in \mathbf{G}.$$

An element $e \in \mathbf{G}$ is an **identity** for $*$ if

$$e*a = a*e = a \quad \text{for every } a \in \mathbf{G}.$$

If e is an identity for $*$ and $a \in \mathbf{G}$, then an **inverse** for a is an element $b \in \mathbf{G}$ such that

$$a*b = b*a = e.$$

Our next definition isolates the most essential properties of binary systems.

Definition 1. *A* **group** *is a binary system* $\mathbf{G}$ *with* $*$ *for which*

(i) $*$ *is associative,*

(ii) *there is an identity element* $e \in \mathbf{G}$ *for* $*$*, and*

(iii) *each element of* $\mathbf{G}$ *has an inverse.*

For example, we can check that each of the binary systems of Problem 1 is a group. We call $\mathbf{K}_4$ the **Klein 4-Group**, $\mathbf{Z}_{12}$ the **group of integers modulo 12** and $\mathbf{S}_3$ the **symmetric group on 3 elements**. The fact that $\mathbf{P}_{abc}$ is associative is not obvious from the definition, but is a straightforward exercise in elementary set theory.

It turns out that most of what we will want to do does not require the commutative property. If the binary operation of a group $\mathbf{G}$ is commutative, we say that $\mathbf{G}$ is a **commutative group**, or an **abelian group** after the Norwegian mathematician Niels Abel (1802-1829).

Problem 2. *Which of the binary operations* $+,-,\cdot,\cap,\cup,\sim,\circ,+_{12},*,\bullet$ *are associative? For each one that is not, give a counterexample to show it is not.*

Problem 3. *Which of the binary operations* $+,-,\cdot,\cap,\cup,\sim,\circ,+_{12},*,\bullet$ *are commutative? For each one that is not, give a specific counterexample to show that it is not. Reviewing Problem 1, how can you tell from looking at a table if an operation is commutative?*

Problem 4. *What is the identity of each of the groups* $\mathbf{K}_4$*,* $\mathbf{Z}_{12}$*,* $\mathbf{P}_{abc}$ *and* $\mathbf{S}_3$*? List the elements of each group and, under each element, list its inverse.*

Problem 5. *Show that the product of two members of* $\mathbf{M}_1$ *is again a member of* $\mathbf{M}_1$*, and that* $\mathbf{M}_1$ *forms a group under matrix multiplication.*

Problem 6. *Let* **L** *be the binary system on the right. Is* **L** *commutative? Is it a group?*

$*$	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	3	4	1	0
3	3	4	0	2	1
4	4	2	1	0	3

Chapter 2

Consequences of the Axioms

What is truly fascinating about the three little axioms for a group—associativity, identity and inverses—is that together they imply so much. In this chapter we will look at a number of different immediate consequences of these axioms. We will refer to a consequence of these axioms as a "Lemma", a "Theorem" or a "Corollary". As you prove each of the following consequences, specify each use of one of the axioms.

We begin with a fact that does not even depend on the group axioms. Is it possible for a binary system to have two different identity elements? Try, for example, to fill in a table for a binary operation $*$ on a 3–element set $\{e_1, e_2, a\}$ in which both e_1 and e_2 are identity elements. If you have difficulty, look at exactly what is causing the difficulty and then prove the following theorem.

Theorem 7. *A binary system* **G** *with operation* $*$ *can have at most one identity element.*

Now try to fill in a table for a binary operation $*$ on the 4–element set $\{e, a, b, c\}$ in which e is the (unique) identity and b and c are both inverses for a. This time you should have no trouble, which tells you that any proof of the following theorem will necessarily have to make use the group axioms.

Theorem 8. *Let* **G** *be a group with identity e, and let a be an element of* **G** *with inverse b. If* $c \in G$ *and either* $a * c = e$ *or* $c * a = e$*, then* $c = b$*. In particular, a has only one inverse.*

Since the inverse of a group element a is unique, we will normally denote it by "a^{-1}". In this notation, Theorem 8 says that, if we already know that we are in a group, then we can show that b is the inverse of a by verifying either that $a * b = e$ or $b * a = e$; we don't need to verify both.

Corollary 9. *If* **G** *is a group with identity e and* $a, b \in$ **G***, then*

(i) $(a^{-1})^{-1} = a$

(ii) $(a * b)^{-1} = b^{-1} * a^{-1}$.

Let **G** be a binary system. We say the $e \in$ **G** is a **right identity** if $a * e = a$ for all $a \in$ **G**. An element $b \in$ **G** is a **right inverse** for a (with respect to e) if $a * b = e$. An element $f \in$ **G** is an **idempotent** if $f * f = f$.

Theorem 10. *Let* **G** *be an associative binary system with a right identity e such that each element has a right inverse. Then* **G** *is a group.*

[Hint: You need to show that e is also a left identity and that a right inverse is also a left inverse. Start by showing that e is the only idempotent in **G**.]

The examples of groups that we have computed will give us a laboratory to test hypotheses that might be true of groups in general. Notice that the two groups $\mathbf{K}_4$ and $\mathbf{P}_{abc}$ have the unusual property that each element is its own inverse. These two are among the commutative groups, but not every commutative group (for example $\mathbf{Z}_{12}$) has this property.

Corollary 11. *Let* **G** *be a group in which every element is its own inverse. Then* **G** *is commutative.*

Algebra in general grew out of the historical need to solve equations, and this need led specifically to the development of group theory where certain kinds of equations can always be solved.

Theorem 12. *If* **G** *is a group, $a,b \in \mathbf{G}$, then the equations $a*x = b$ and $y*a = b$ each have a unique solution, namely, $x = a^{-1}*b$, and $y = b*a^{-1}$.*

Cancellation is a technique that is often useful for solving equations, but it must be used judiciously. For example, in high school algebra we cannot conclude from $ab = ac$ that $b = c$ without first checking that $a \neq 0$. In general, for a binary operation $*$, we say that

$*$ is **left cancellative** if $a*b = a*c$ implies $b = c$, and

$*$ is **right cancellative** if $b*a = c*a$ implies $b = c$

for every choice of a,b,c.

Problem 13. *Give examples to show that multiplication of 2×2 matrices in general and composition of functions in general are neither left nor right cancellative.*

Theorem 14. *Every group is both left and right cancellative.*

If we examine the group tables that we constructed in Chapter 1, we notice something special about the rows and the columns. In each case, each row and each column is a permutation of the elements of the group. The rows and columns are precisely the functions from the group into itself obtained by left and right multiplication by a single element. What we have observed in these examples is true for all groups.

Theorem 15. *If* **G** *is a group and $a \in G$, then the two functions*

$$\ell_a(x) := a*x \quad \textit{and} \quad r_a(x) := x*a$$

are both permutations of G.

An essential goal of group theory is to discover all possible groups of each finite size. The theory we will develop later will help to do this, but we can already address a simple case. The following theorem can be proven from the axioms, but you might be able to apply what you have learned to give a simpler proof.

Theorem 16. *In the following sense, there is essentially only one group with three elements.*

(i) *There is at most one way to fill in a table for the set* $\{e,a,b\}$*, using* e *as the identity, which could possibly be a group.*

(ii) *The table of part* (i) *is in fact a group.* (*You will need several cases to establish associativity.*)

Associativity in groups allows us to unambiguously write down the product $a*b*c$ where a,b,c are elements of a group **G**. What about longer products such as $a*b*c*d*f$? This expression has quite a number of possible interpretations, for example, $((a*b)*(c*d))*f$ and $a*((b*c)*(d*f))$. Do these both represent the same element? They do, but this fact requires four applications of the associative property to prove:

$$\begin{aligned}((a*b)*(c*d))*f &= (a*b)*((c*d)*f) = (a*b)*(c*(d*f))\\ &= a*(b*(c*(d*f))) = a*((b*c)*(d*f)).\end{aligned}$$

If we could devise a similar argument for every pair of 5–element products, we would then be able to unambiguously write $a*b*c*d*f$.

More generally, is it possible to prove that the product $a_1a_2a_3\dots a_n$ is unambiguous? This task sounds rather daunting, as the number of possible products will grow rapidly as the number of factors extends beyond five. It turns out that it is nevertheless true, and that mathematical induction provides a simple proof. We first define the **left associated product** of $a_1,a_2,a_3,\dots,a_n$ to be

$$(\dots((a_1*a_2)*a_3)*\dots)*a_n.$$

Theorem 17. *Let* **G** *be an associative binary system, and choose elements* $a_1,a_2,a_3,\dots,a_n \in$ **G**. *Then every product of the elements* $a_1,a_2,a_3,\dots,a_n$*, in that order, is equal to the left associated product. In particular, we can unambiguously write down the product* $a_1*a_2*a_3*\cdots*a_n$.

Real number exponents satisfy two important rules:

$$a^m a^n = a^{m+n} \quad \text{and} \quad (a^m)^n = a^{mn}$$

where m and n are positive integers. If a is an element of a group **G** and $n \in \mathbb{Z}^+$ (the set of positive integers), we recursively define the **exponent** a^n as

$$a^1 := a \quad \text{and} \quad a^{n+1} := a^n * a.$$

Applying the above associativity theorem, we see that $a^n := a*a*\cdots*a$, the product of n a's. It is easy to check that the same rules of exponents hold with this definition.

We would like to extend the definition of exponents to give a meaning to "a^0" and "a^{-n}" in such a way that the rules of exponents will continue to hold. There is only one way that we could possibly do this. If $a^0*a^1 = a^{0+1}$, then we have $a^0*a = a$ so that, by Theorem 4, we must define

$$a^0 := e, \quad \text{the identity.}$$

Similarly, if $a^{-n}*a^n = a^{-n+n}$, then we have $a^{-n}*a^n = e$ so that, by Theorem 2, we have no choice but to define

$$a^{-n} := (a^n)^{-1}, \quad \text{the inverse of } a^n.$$

Lemma 18. *If* $\mathbf{G} = \langle G, * \rangle$ *is a group,* $a \in G$ *and* $n \in \mathbb{Z}^+$, *then* $a^{-n} = (a^{-1})^n$.

The proof of the following theorem requires examining a number of cases.

Theorem 19. *Let* $\mathbf{G} = \langle G, * \rangle$ *be a group,* $a \in G$, *and* $m, n \in \mathbf{Z}$. *Then*

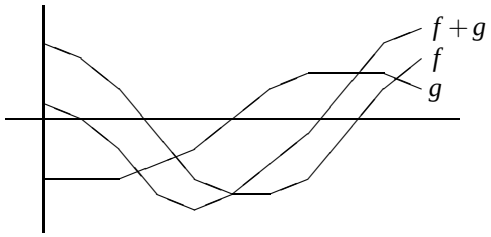
(i) $a^m * a^n = a^{m+n}$ *and*

(ii) $(a^m)^n = a^{mn}$.

For another familiar source of groups, recall that the axioms for a linear space require that vector addition be commutative and associative, and that there be a zero vector which is an additive identity. The other axioms imply that, for each point P of a linear space, the point $(-1)P$ is an additive inverse of P. Thus every linear space is a commutative group under addition.

The group operation in a vector space is normally denoted by the addition symbol +. For example, the vector space of all functions from the real numbers into the real numbers forms a commutative group $\mathbf{F}[\mathbf{R}, \mathbf{R}]$ where the sum of functions f and g is defined by

$$(f+g)(x) = f(x) + g(x).$$



When we refer to a commutative group whose operation is denoted by +, such as the additive group of $\mathbf{R}$ of real numbers, the additive group of n-by-m matrices, or the additive group $\mathbf{F}[\mathbf{R}, \mathbf{R}]$, it is rather awkward to use the multiplicative notation that we have been using for general groups. Instead, we introduce the **additive notation** for groups as follows.

	Multiplicative	Additive
product; sum	$a * b$ or ab	$a + b$
identity	$ea = ae = a$	$0 + a = a + 0 = a$
inverse	a^{-1}	$-a$
exponent	a^n	na
quotient; difference	ab^{-1}	$a - b$

In additive notation, for example, Theorem 19 says that, for all $a, b \in \mathbf{G}$ and $m, n \in \mathbf{Z}$, we have

(i) $ma + na = (m+n)a$

(ii) $n(ma) = (nm)a$.

While this may look at first glance like the distributive and associative properties, they are in fact the properties of exponents written in additive notation.

Chapter 3

Cyclic Groups

Let **G** be a group with operation $*$ and let **H** be a subset of **G**. We say that **H** is **closed under** $*$ if

$$a, b \in \mathbf{H} \quad \text{implies} \quad a * b \in \mathbf{H}.$$

If **H** is closed under $*$, then **H** also forms a binary system. If **H** turns out to be a group, we call it a **subgroup** of **G**. Notice that if **H** is closed under $*$, then **H** is automatically associative. Thus **H** is a subgroup of **G** if and only if

(i) **H** is closed under $*$,

(ii) the identity e of **G** is in **H** and

(iii) for each element b of **H**, the inverse b^{-1} is in **H**.

For example, the subgroups of the additive group **R** of **real numbers** include the additive group **Q** of **rational numbers** and the additive group **Z** of **integers**. Familiar subgroups of the additive group $\mathbf{F}(\mathbf{R},\mathbf{R})$ include the group of **continuous real valued functions** $\mathbf{C}(\mathbf{R},\mathbf{R})$, the group of **differentiable real valued functions** $\mathbf{D}(\mathbf{R},\mathbf{R})$ and the group of **polynomial functions** $\mathbf{P}(\mathbf{R},\mathbf{R})$:

$$\mathbf{P}(\mathbf{R},\mathbf{R}) \subseteq \mathbf{D}(\mathbf{R},\mathbf{R}) \subseteq \mathbf{C}(\mathbf{R},\mathbf{R}) \subseteq \mathbf{F}(\mathbf{R},\mathbf{R}).$$

Our next lemma gives a simple way to find a multitude of subgroups.

Lemma 20. *Let b be an element of the group* **G**. *Then the set* $\{b^n \mid n \in \mathbf{Z}\}$ [*the set* $\{nb \mid n \in \mathbf{Z}\}$ *in additive notation*] *of all powers* [*multiples*] *of b forms a subgroup of* **G**.

We use the notation

$$\mathbf{sg}(b) := \{b^n \mid n \in \mathbf{Z}\}$$

and call this the **cyclic subgroup of G generated by** b. If $\mathbf{G} = \mathbf{sg}(b)$ for some element $b \in G$, we say that **G** is a **cyclic group** and that b is a **cyclic generator** of **G**. For example, the additive group **Z** of integers is cyclic since every integer is a multiple of 1, that is, $\mathbf{Z} = \mathbf{sg}(1)$.

Lemma 21. *Every cyclic group is commutative.*

Thus, for example, $\mathbf{S}_3$ and $\mathbf{M}_1$ are *not* cyclic groups. Notice that each element of every group generates a cyclic subgroup. We will see that different elements can generate the same cyclic subgroup.

Lemma 22. *If* $\mathbf{H}$ *is a subgroup of* $\mathbf{G}$ *and* $b \in \mathbf{H}$*, then* $\mathbf{sg}(b) \subseteq \mathbf{H}$*.*

Problem 23. *Find the cyclic subgroup of* $\mathbf{Z}_{12}$ *generated by each of its elements. Show that* $\mathbf{Z}_{12}$ *is itself a cyclic group. Is there a subgroup* $\mathbf{H}$ *of* $\mathbf{Z}_{12}$ *that is not cyclic?*

We have seen a small number of different finite groups. How many different finite groups are there? For example, is there a group with 17 elements? a group with 64,539 elements? Looking closely at the group $\mathbf{Z}_{12}$ suggests some answers. Let n be an arbitrary positive integer and consider the set $\{0,1,2,3,\ldots,n-1\}$ of all possible remainders when we divide by n. Following the example of $\mathbf{Z}_{12}$ we define $+_n$ on this set by

$$a +_n b := \begin{cases} a+b & \text{if} \quad a+b < n; \\ a+b-n & \text{if} \quad a+b \geq n. \end{cases}$$

Clearly 0 is an identity for $+_n$ and $n-b$ is an inverse for b. Moreover, $+_n$ is associative since both $a +_n (b +_n c)$ and $(a +_n b) +_n c$ are the number we get by adding $a+b+c$ and then subtracting n until we get a number less than n. Thus

$$\mathbf{Z}_n := \langle \{0,1,2,\ldots,n-1\}; +_n \rangle$$

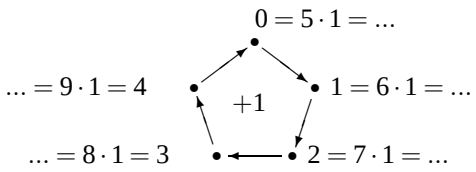
is a (commutative) group which we call the **group of integers modulo** n. This gives us at least one n-element group for *every* positive integer n.

Problem 24. *Show that* $\mathbf{Z}_5$ *is cyclic. Exactly which elements of* $\mathbf{Z}_5$ *are cyclic generators of* $\mathbf{Z}_5$*?*

Problem 25. *Show that the group* $\mathbf{Z}_n$ *is cyclic for each* $n \in \mathbb{Z}^+$*. Looking at the examples of* $\mathbf{Z}_5$ *and* $\mathbf{Z}_{12}$*, which elements of* $\mathbf{Z}_n$ *do you think are the cyclic generators of* $\mathbf{Z}_n$*? State your answer as a conjecture. Can you prove it?*

The cyclic group $\mathbf{Z}_5$ can be illustrated by the following diagram.

$\mathbf{Z}_5$:



This diagram certainly does support our choice of the term "cyclic" for this kind of group. We would like to show that every finite cyclic group looks like this. If a cyclic group has generator b, then it consists of all the powers

$$\ldots b^{-3}, b^{-2}, b^{-1}, b^0 = e, b, b^2, b^3, b^4, \ldots$$

of the element b. If the group happens to be finite, then this list must be highly redundant as it is in $\mathbf{Z}_5$. We will see that this redundancy must follow the above "cyclic" pattern.

Lemma 26. *Let b be an element of a group* **G**, *and let $n \in \mathbb{Z}^+$. Assume that the powers $e = b^0, b = b^1, b^2, b^3, b^4, \ldots, b^n$ are not all distinct, that is, there are integers i, j such that $b^i = b^j$ where $0 \leq i < j \leq n$. Then there is a positive integer $k \leq n$ such that $b^k = e$.*

We say that b has **infinite order** if all of the non-negative powers $e = b^0, b = b^1, b^2, b^3, b^4, \ldots$ are distinct. Otherwise, we say that b has **finite order** and we define the **order** of b, written $\circ(b)$, to be the smallest positive integer k such that $b^k = e$ [additively, $kb = 0$]. For example, each element of the additive group **Z** has infinite order while each element of a finite group must, according to Lemma 26, have finite order.

Problem 27. *Find the order of the following elements of the group* $\mathbf{M}_1$:

$$\text{(i) } A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{(ii) } B = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix} \quad \text{(iii) } C = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

Lemma 26 leads to several useful results. Recall that $\mathbf{H} \subseteq \mathbf{G}$ is a subgroup of **G** provided that it is closed, contains the identity and contains inverses. These criteria can be simplified for finite groups.

Theorem 28. *Let* **H** *be a finite non-empty subset of a group* **G**. *Then* **H** *is a subgroup of* **G** *provided only that it is closed.*

Corollary 29. *If* **G** *is a finite group and let $a \in \mathbf{G}$, then the subgroup generated by a consists of all positive powers of a:*

$$\mathbf{sg}(a) = \{a^k \mid k \in \mathbf{Z}^+\}.$$

We can now prove two important theorems about cyclic groups. We will need the following fundamental fact about the integers, which we will not prove here.

Long Division Lemma *Let m be an integer and let d (the* **divisor**) *be a positive integer. Then there are unique integers q (the* **quotient**) *and r (the* **remainder**) *such that*

$$m = qd + r \quad \textit{with} \quad 0 \leq r < d.$$

Let $m, d \in \mathbf{Z}$. We say that d **divides** m, written $d|m$, if there is a $q \in \mathbf{Z}$ such that $m = qd$. We generally use Long Division to find out if $d|m$ by dividing m by d and seeing if the remainder is 0. Use this strategy to prove the following lemma.

Lemma 30. *Assume $b \in \mathbf{G}$ has finite order, and let $m, i, j \in \mathbb{Z}$. Then*

(i) $b^m = e$ *if and only if* $\circ(b)|m$, *and*

(ii) $b^i = b^j$ *if and only if* $\circ(b)|i - j$.

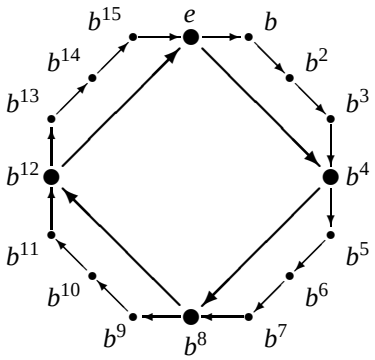
Theorem 31. *Let b be an element of a group* **G**, *and assume that b has finite order k. Then the cyclic subgroup of* **G** *generated by b has exactly k distinct elements, namely,*

$$\mathbf{sg}(b) = \{e, b, b^2, b^3, \ldots, b^{k-1}\} \textit{ with } b^k = e.$$

This theorem tells us that a finite cyclic group is accurately described by the adjective "cyclic". Using this information, we can fill in the entire group table for $\mathbf{sg}(b)$. Thus every group element of order k generates a cyclic group that look exactly like the cyclic group $\mathbf{Z}_k$. The next theorem tells us that what we discovered about $\mathbf{Z}_{12}$ in Problem 23 is true of every cyclic group.

Theorem 32. *Every subgroup of a cyclic group is cyclic.*

Proof: (Hint) Let $\mathbf{G} = \mathbf{sg}(b)$ be cyclic, and let $\mathbf{H}$ be a subgroup of $\mathbf{G}$. Choose an integer n for which you believe that $\mathbf{H} = \mathbf{sg}(b^n)$. Then show that $\mathbf{sg}(b^n) \subseteq \mathbf{H}$ and that $\mathbf{H} \subseteq \mathbf{sg}(b^n)$.



The fact that $\mathbf{Z}$ is a cyclic group leads to some useful properties of the integers. For example, we know that, for each non-negative integer n, the multiples of n form a cyclic subgroup of $\mathbf{Z}$. Theorem 32 tells us that these are the *only* subgroups of $\mathbf{Z}$. Let $m, n \in \mathbf{Z}$ where m and n are not both 0. We say that d is the **greatest common divisor** of m and n, written $d = \gcd(m,n)$, if d is the largest positive integer that divides both m and n.

Lemma 33. *Assume $m, n \in \mathbf{Z}$ where m and n are not both 0. Then $d := \gcd(m,n)$ is the smallest positive integer that can be expressed in the form $mx + ny$ where $x, y \in \mathbf{Z}$.*

Proof: (Outline) Show that $\mathbf{H} := \{mx + ny \mid x, y \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ and apply Theorem 32.

We say that $m, n \in \mathbf{Z}$ are **relatively prime** if $\gcd(m,n) = 1$.

Theorem 34. *Integers $m, n \in \mathbf{Z}$ are relatively prime if and only if there are integers $x, y \in \mathbf{Z}$ such that $mx + ny = 1$.*

We now have the machinery we need to prove the conjecture of Problem 25.

Theorem 35. *Let $\mathbf{G} = \mathbf{sg}(b)$ be a finite cyclic group where $\circ(b) = k$. Then b^m is a cyclic generator of $\mathbf{G}$ if and only if m and k are relatively prime.*

Chapter 4

LaGrange's Theorem

By the **order** of a finite group **G**, written $\circ(\mathbf{G})$, we mean the number of elements in **G**. In this chapter we will see how numerical properties of $\circ(\mathbf{G})$ imply algebraic properties of the group **G** itself.

Theorem 31 tells us that a cyclic group of order k consists of the first k powers of the generator, where the operation is done by adding the powers modulo k. Thus all finite cyclic groups of the same order have virtually identical tables. Theorem 16 tells us that all groups of order 3 are cyclic, and therefore look alike. Clearly the same is true for groups of order 1 or 2. On the other hand, $\mathbf{K}_4$ is a non-cyclic group of order 4. These observations raise the following question.

Question *For which positive integers n is it true that every group of order n is cyclic?*

The smallest value of n for which we do not yet have an answer is $n = 5$.

Theorem 36. *Every group* **G** *of order 5 is cyclic, and therefore looks exactly like* $\mathbf{Z}_5$.

Proof: (Outline) Let b be any element of **G** other than the identity. Explain why $\circ(b)$ must be either 2,3,4 or 5.

(i) Show that if $\circ(b) = 4$, then **G** would have at least 8 elements. [Fill in the first 4 rows of the table listing the elements as e, b, b^2, b^3. Then add a 5th column for a new element c and explain why $c,\ d := b * c,\ f := b^2 * c,\ g := b^3 * c$ would be 4 distinct new elements.]

(ii) Show that if $\circ(b) = 3$, then **G** would have at least 6 elements. [Fill in the first 3 rows of the table listing the elements as e, b, b^2. Then add a 4th column for a new element c and explain why $c,\ d := b * c,\ f := b^2 * c$ would be 3 distinct new elements.]

(iii) Show that if $\circ(b) = 2$, then **G** would have at least 6 elements. [Fill in the first 2 rows of the table listing the elements as e, b. Then add a 3rd column for a new element c and explain why $c,\ d := b * c$ would be 2 distinct new elements. Add columns for c and d and fill in the 2 columns below them. Now let f be the 5th element and explain why $f,\ g := b * f$ would again be 2 distinct new elements.]

Theorem 37. *Every group* **G** *of order 7 is cyclic, and therefore looks exactly like* $\mathbf{Z}_7$.

Proof: (Outline) Follow the strategy of Theorem 36, adding the necessary additional cases.

What about groups of order 9? Here is a helpful observation. The Cartesian plane $\mathbf{R}^2$, viewed as an additive group, is obtained by taking ordered pairs (a,b) from the additive group of real numbers $\mathbf{R}$ and defining the operation of $\mathbf{R}^2$ by applying the operation of $\mathbf{R}$ in each coordinate:

$$(a_1,b_1)+(a_2,b_2) := (a_1+a_2,\ b_1+b_2).$$

The same idea works with any pair of groups $\mathbf{H}=\langle H;*_H\rangle$ and $\mathbf{K}=\langle K;*_K\rangle$. We define the **Cartesian product** of $\mathbf{H}$ and $\mathbf{K}$ to be the group

$$\mathbf{H}\times\mathbf{K}=\langle H\times K;*\rangle$$

whose elements are ordered pairs (h,k), where $h\in H$ and $k\in K$, and whose operation is done by applying the operations of $\mathbf{H}$ and $\mathbf{K}$ in each coordinate:

$$(h_1,k_1)*(h_2,k_2)=(h_1*_H h_2,\ k_1*_K k_2).$$

Theorem 38. *If* **H** *and* **K** *are groups, then* $\mathbf{H}\times\mathbf{K}$ *is a group. If they are both finite, then* $\mathbf{H}\times\mathbf{K}$ *is finite and* $\circ(\mathbf{H}\times\mathbf{K})=\circ(\mathbf{H})\cdot\circ(\mathbf{K})$.

Problem 39. *Use the Cartesian product to construct a group of order 9 that is not cyclic.*

Problem 40. *For exactly which of the values* $n=1,2,3,4,5,6,7,8,9$ *is it true that every group of order n is cyclic? Make a conjecture as to when in general it is true that every group of order n is cyclic.*

We will settle this question by proving a more general theorem about finite groups due to J. L. LaGrange (1736-1813). First we need some more empirical data. Use Theorem 28 to find all of the subgroups of the four groups in the table below, and list each of their orders. What does this table suggest about the relationship between the order of a finite finite group and the orders of its subgroups?

G	$\circ(\mathbf{G})$	$\circ(\mathbf{H})$ for subgroups **H** of **G**
$\mathbf{S}_3$		
$\mathbf{Z}_{12}$		
$\mathbf{P}_{abc}$		
$\mathbf{K}_4$		

To see why this relationship might hold in general, consider the subgroup $\mathbf{H}:=\{0,4,8\}$ of $\mathbf{Z}_{12}$. We can generate new elements of $\mathbf{Z}_{12}$ from $\mathbf{H}$ by applying the operation. If we start with $1\notin\mathbf{H}$, then $\{0+1,4+1,8+1\}=\{1,5,9\}$ gives us 3 new elements of $\mathbf{Z}_{12}$. Choosing $2\notin\{0,4,8,1,5,9\}$, we obtain 3 more new elements $\{0+2,4+2,8+2\}=\{2,6,10\}$. Doing the same thing with $3\notin\{1,4,8,1,5,9,2,6,10\}$ will give us the last 3 elements of $\mathbf{Z}_{12}$. What we find is that $\mathbf{Z}_{12}$ is the disjoint union of 4 sets, each having the same number of elements as **H**:

$$\mathbf{Z}_{12}=\{0,4,8\}\cup\{1,5,9\}\cup\{2,6,10\}\cup\{3,7,11\}.$$

Thus $\circ(\mathbf{Z}_{12})=4(\circ(\mathbf{H}))$ and therefore $\circ(\mathbf{H})|\circ(\mathbf{Z}_{12})$.

In general we say that a collection $\mathscr{P}$ of subsets of a set A is a **partition** of A if every element of A is in exactly one of these sets, that is,

- each element of A is in some set of $\mathscr{P}$ (in symbols, $\bigcup \mathscr{P} = A$) and
- two different sets X and Y in $\mathscr{P}$ have empty intersection. (We say X and Y are **disjoint**.)

We will now see that every subgroup of every group produces a partition like the one we have seen in $\mathbf{Z}_{12}$.

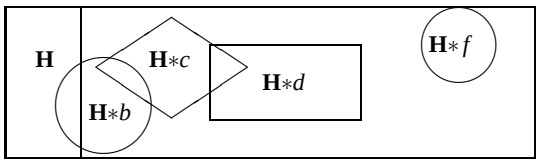
Let $\mathbf{H}$ be a subgroup of a group $\mathbf{G}$. For each element $b \in \mathbf{G}$ we define the **right coset** generated by b to be the set

$$\mathbf{H} * b := \{h * b \mid h \in \mathbf{H}\}.$$

$+$	0	4	8	1	5	9	2	6	10	3	7	11
0	0	4	8	1	5	9	2	6	10	3	7	11
4	4	8	0	5	9	1	6	10	2	7	11	3
8	8	0	4	9	1	5	10	2	6	11	3	7

In the above example, the right cosets of $\mathbf{H} := \{0,4,8\}$ form a partition of $\mathbf{Z}_{12}$. The right coset generated by each element occurs immediately below it in the table for $\mathbf{Z}_{12}$.

We would like to know if the collection $\mathscr{P}$ of right cosets of an arbitrary subgroup $\mathbf{H}$ of an arbitrary group $\mathbf{G}$ form a partition like the one we have seen in $\mathbf{Z}_{12}$. At the moment, all we know about the right cosets of $\mathbf{H}$ is that they are a collection of subsets of $\mathbf{G}$. One coset is $\mathbf{H} = \mathbf{H} * e$ itself. This might be illustrated as follows.



The next two lemmas tell us that this picture is not very accurate.

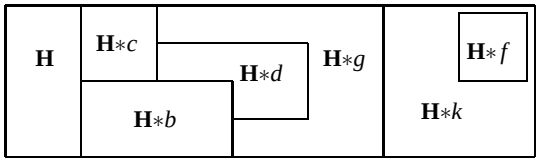
Lemma 41. *If $b \in \mathbf{G}$, then b is in the right coset $\mathbf{H} * b$ that it generates. In particular, every element of $\mathbf{G}$ is in some right coset.*

Lemma 42. *Let $b, c \in \mathbf{G}$.*

(i) *If $c \in \mathbf{H} * b$, then $\mathbf{H} * c = \mathbf{H} * b$.*

(ii) *If $c \notin \mathbf{H} * b$, then $(\mathbf{H} * c) \cap (\mathbf{H} * b) = \varnothing$.*

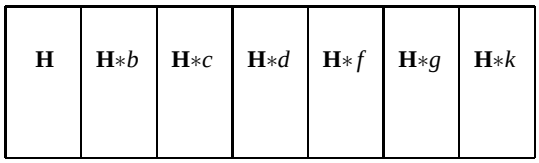
Together, the above two lemmas tell us that the right cosets of a subgroup $\mathbf{H}$ form a partition of the group $\mathbf{G}$, as is illustrated in the more accurate illustration below.



Using additional group properties, we can see that each right coset of **H** look, as a set, just like **H**.

Lemma 43. *If $b \in \mathbf{G}$, then $r_b : \mathbf{H} \to \mathbf{H} * b$ (defined as $r_b(x) := x * b$) is one-to-one and onto. In particular, if* **H** *is finite, then every right coset of* **H** *has the same number of elements as* **H**.

This leads us to a yet more accurate picture, which tells us exactly why the order of **H** should divide the order of **G**. If the number of right cosets of **H** in **G** is finite, we call this number the **index** of **H** in **G** and denote it by $[\mathbf{G} : \mathbf{H}]$.



Lagrange's Theorem 44. *If* **G** *is a finite group and* **H** *is a subgroup of* **G**, *then* $\circ(\mathbf{G}) = [\mathbf{G} : \mathbf{H}] \cdot \circ(\mathbf{H})$. *In particular,* $\circ(\mathbf{H}) | \circ(\mathbf{G})$, *and* $[\mathbf{G} : \mathbf{H}]$ *is also the number of left cosets of* **H** *in* **G**.

Corollary 45. *If* **G** *is a finite group and* $b \in \mathbf{G}$, *then* $\circ(b) | \circ(\mathbf{G})$.

Corollary 46. *If* **G** *is a finite group of order n and* $b \in \mathbf{G}$, *then* $b^n = e$.

We can now see why it was true that every 5 or 7 element group must be cyclic and, with no additional effort, why the same must be true for every group of prime order.

Theorem 47. *Every group of prime order is cyclic.*

In contrast to Theorem 47, we can use the idea of Problem 39 to exhibit non-cyclic groups of order n for many non-prime values of n. (Hint: Show that if $n = p^2 q$ where p is a prime, then $\mathbf{Z}_p \times \mathbf{Z}_{pq}$ is not cyclic.)

Theorem 48. *If every group of order $n > 1$ is cyclic, then n is either prime or a product of distinct primes.*

Problem 49. *Partition the numbers from 1 to 60 into three sets as follows.*

$A := \{n \mid$ *You can prove that every group of order n is cyclic.*$\}$,

$B := \{n \mid$ *You can exhibit a group of order n that is not cyclic.*$\}$

$C := \{n \mid$ *Neither of the above is true.*$\}$

Chapter 5

Equivalence Relations

Assume that you go to buy a new car. You examine the possible choices, and gradually narrow the scope of your search. You are concerned about the particular make and model of a car, its particular assortment of added features and perhaps even its particular color. But among all the cars that are presently for sale, you will consider ones of the same make, model, features and color to be "equivalent" since they are, for you, totally indistinguishable. Auto companies produce thousands of individual cars every year, but only a handful of essentially different kinds. Fortunately you only need to choose among the handful of different kinds, not among the thousands of different individual cars. Once you choose a particular class of "equivalent" cars (for example, blue Subaru Foresters with manual transmission that have no extra added features), you will be happy with whichever member of that "equivalence class" that you can buy at an acceptable price.

In this chapter we will examine what it means for two things to be in some useful sense "equivalent". This notion turns out to have important applications in mathematics and science, and particularly in group theory. There are many occasions when we want to describe certain objects as being "equivalent". For example, two equations in variables x and y can be thought of as equivalent if they have the same sets of solutions. Thus $y = 3x + 4$ and $6x = 2y - 8$ are equivalent. Two computer programs might be thought of as "equivalent" if they always produce the same output from the same input. In a different context, we might think of two compound sentences in propositional logic to be "equivalent" if they have the same truth tables. For example, the truth table below shows that every implication is

p	q	$p \rightarrow q$	$\neg q \rightarrow \neg p$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Table 5.1: 1 is True; 0 is False

equivalent to its contrapositive.

The significance of truth table equivalence can be easily seen if we limit our attention to the set of compound sentences with a single variable p. There are still infinitely many

different compound sentences that we can write down, for example,

$$((p \vee p) \wedge (\neg p \implies (p \wedge p))) \implies ((\neg p \vee p) \wedge p).$$

But there are only four possible different truth tables, given by the four compound sentences p, $\neg p$, $p \vee \neg p$ and $p \wedge \neg p$. Thus every compound sentence with one variable p is equivalent

p	p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
0	0	1	1	0
1	1	0	1	0

to one of these four.

All of the above notions of "equivalent" have something in common. In each case there is a set (cars, equations, programs, compound propositional sentences) which is broken up into disjoint bunches so that two members are "equivalent" exactly when they are in the same bunch. In each case the bunches form a partition of the underlying set.

A partition of a set A, which consists of a set of subsets of A, is often a rather awkward thing to talk about. It is usually much more convenient to talk about the associated relation of being "equivalent" among certain pairs of elements of A. In order to discuss this idea, we define a **binary relation** on a set A to be a subset $\equiv$ of $A \times A$. For $x, y \in A$ we often write "$x \equiv y$" to mean that $(x,y) \in \equiv$. For example, the less than or equal to relation $\leq$ on the set $\mathbf{R}$ of real numbers is formally defined as

$$\leq = \{\, (x,y) \mid x \text{ is less than or equal to } y \,\}.$$

We normally prefer to write "$3 \leq 7$" instead of the rather strange looking, but formally correct, "$(3,7) \in \leq$". The equality relation $=$ on A is defined as $a = b$ if a and b represent the same element of A.

Associated with any partition $\mathscr{P}$ of A is a relation $\equiv_{\mathscr{P}}$ of "equivalence" on A: elements x and y of A are "equivalent", that is, $x \equiv_{\mathscr{P}} y$, if x and y are in the same member of $\mathscr{P}$. A relation $\equiv_{\mathscr{P}}$ that arises out of a partition $\mathscr{P}$ in this way is called an **equivalence relation** on A. In this case the member of $\mathscr{P}$ containing an element $x \in A$ is called the **equivalence class** of x.

Consider, for example, the set A of children in the elementary schools. For certain purposes it is helpful to think of two children as being equivalent if they were born in the same year. We then have one grade for each equivalence class. If Charlie is in the fourth grade, his equivalence class is the fourth grade class. Or we might think of two children as equivalent if they are working at the same grade level in mathematics. We could then partition the children into different math classes, each working at a different level. Alternately, we could think of two children as equivalent if they have the same favorite hobby, and then partition them into clubs that each consist of children with a particular hobby. But sometimes we just need to realize that each child is unique, and focus on the partition with a single child in each equivalence class. These are all different partitions, or equivalence relations, on the same set A. There is no right meaning of "equivalence"; rather, each notion of equivalence is useful in a different context.

We would like to determine when a binary relation $\equiv$ is the equivalence relation associated with some partition. For example, is the relation $\leq$ on the numbers is an equivalence

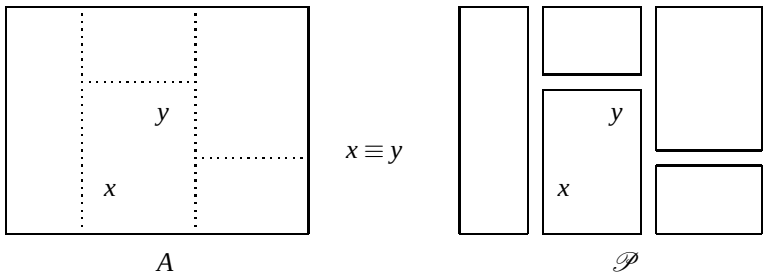
relation? It is easy to see that every equivalence relation on A must have three simple properties: a relation $\equiv$ on A is

- **reflexive** if $x \equiv x$ for any $x \in A$;
- **symmetric** if $y \equiv x$ whenever $x \equiv y$;
- **transitive** if $x \equiv z$ whenever $x \equiv y$ and $y \equiv z$.

If $\equiv$ is the equivalence relation $\equiv_{\mathscr{P}}$ for some partition $\mathscr{P}$, then it will certainly have these properties. The relation $\leq$, for example, is clearly not symmetric since $4 \leq 9$ but $9 \not\leq 4$. Thus $\leq$ is not an equivalence relation.

Conveniently, it turns out that every binary relation $\equiv$ on A which has these three simple properties is the equivalence relation associated with some partition. To see this, we define—for a binary relation $\equiv$ on A and an element $x \in A$—the **$\equiv$–class** of x to be the set

$$[x] = \{y \mid y \in A \text{ and } x \equiv y\}.$$



Equivalence Relation Theorem *Let $\equiv$ be a binary relation on the set A. If $\equiv$ is reflexive, symmetric and transitive, then the set $\mathscr{P}$ of $\equiv$–classes is a partition of A and $\equiv$ is the equivalence relation $\equiv_{\mathscr{P}}$ associated with $\mathscr{P}$.*

In the first four problems, verify that the relation is an equivalence relation and then describe its equivalence classes, which should form a partition of A.

Problem 50. *A is the set of points (x,y) in the plane. $(x,y) \equiv (x',y')$ if (x,y) and (x',y') are the same distance from the origin.*

Problem 51. *$x \equiv y$ if x and y are integers and $x-y$ is a multiple of 3.*

Problem 52. *$x \equiv y$ if x and y are integers and $x+y$ is even.*

Problem 53. *Let $\mathbf{S} = \{a,b,c,d,e,f,g,h\}$, let $\mathbf{T} = \{a,b,c\}$ and let A be the set of all (2^8) subsets of $\mathbf{S}$. For $X,Y \in A$, we define $X \equiv Y$ if X and Y have the same intersection with $\mathbf{T}$.*

Problem 54. *Let $A = \{0,1\}^5$ be the set of 32 different five-tuples of 0s and 1s, that is, all sequences (a,b,c,d,e) where $a,b,c,d,e \in \{0,1\}$. For $x,y \in A$, define $x \equiv y$ to mean that x and y have the same number of 1s. Show that $\equiv$ is an equivalence relation and write down all the members of each of the different $\equiv$–classes.*

Every function $f : A \to B$ induces a natural equivalence relation on its domain. For $x, y \in A$, we say that x is f–equivalent to y if $f(x) = f(y)$. The classes of this equivalence relation are called **f-classes** of A. For example, the equivalence classes of Problem 50 are exactly the f-classes where $f(x,y) := \sqrt{x^2 + y^2}$.

Problem 55. *For each equivalence relation $\equiv$ above, define a function f on A so that the $\equiv$-classes are exactly the f-classes.*

Let **G** be a group and let **H** be a subgroup of **G**. We have seen that the right (and left) cosets of **H** (both) partition **G**. These partitions can be described as equivalence relations that **H** induces on **G**. For $a, b \in \mathbf{G}$, we define

$$a \sim_H b \text{ iff } ab^{-1} \in \mathbf{H} \quad \text{and} \quad {}_H\!\sim b \text{ iff } a^{-1}b \in \mathbf{H}.$$

Theorem 56. *If* **H** *is a subgroup of* **G**, *then*

(i) $\sim_H$ *is an equivalence relation on* **G**, *and the* $\sim_H$*–classes are exactly the right cosets of* **H**, *i.e.,* $a \sim_H b \Leftrightarrow \mathbf{H}a = \mathbf{H}b$;

(ii) ${}_H\!\sim$ *is an equivalence relation on* **G**, *and the* ${}_H\!\sim$*–classes are exactly the left cosets of* **H**, *i.e.,* ${}_H\!\sim b \Leftrightarrow a\mathbf{H} = b\mathbf{H}$.

There is a standard and important notion of equivalence between sets. Let A denote the collection of all sets. For $X, Y \in A$, we say that X and Y are the **same size** if there is a bijection (one-to-one and onto function) $f : X \to Y$ from X to Y. Thus finite sets X and Y are the same size if and only if they have the same number of elements, but in general they need not be finite.

Lemma 57. *Let X, Y and Z be sets.*

(i) *The identity function $i_X : X \to X$, with $i_X(x) = x$, is a bijection.*

(ii) *If $f : X \to Y$ is a bijection, then $f^{-1} : Y \to X$ is a bijection.*

(iii) *If $f : X \to Y$ and $g : Y \to Z$ are bijections, then $g \circ f : X \to Z$ is a bijection.*

Theorem 58. *If X is a set, the set $\mathbf{S}_X$ of all bijections from X to itself (called the* **permutations** *of X) is a group under composition.*

Theorem 59. *Being the same size is an equivalence relation on the class of all sets.*

What are the equivalence classes of sets in Theorem 59?

Chapter 6

Isomorphic Groups

There is a very natural and important equivalence relation on the class of all groups, that is, a natural sense in which we can view two groups as being "equivalent". Recall that we proved in Chapter 4 that every 7–element group **G** is cyclic, and interpreted this to say that **G** "looks exactly like $\mathbf{Z}_7$." Thus any two 7–element groups look exactly like each other and, in this sense, can be thought of as equivalent. We would like to give a precise meaning to the assertion that two groups "look exactly alike".

As another example, consider the group $\mathbf{K}_4$ and the 4–element subgroup $\mathbf{H} := \{\varnothing, a, c, ac\}$ of the group $\mathbf{P}_{abc}$.

$\mathbf{K}_4$

$*$	E	H	V	D
E	E	H	V	D
H	H	E	D	V
V	V	D	E	H
D	D	V	H	E

$\mathbf{H}$

$\bigoplus$	$\varnothing$	a	c	ac
$\varnothing$	$\varnothing$	a	c	ac
a	a	$\varnothing$	ac	c
c	c	ac	$\varnothing$	a
ac	ac	c	a	$\varnothing$

We see here is that, although the elements of the two groups are totally different kinds of objects (chess board moves and sets of letters), the tables of the groups look alike. Notice that, if we were to change the order the the elements are listed in the tables, they would no longer look alike. So the equivalence in question has to do with a particular way of pairing the elements:

$$\mathrm{E} \mapsto \varnothing,\ \mathrm{H} \mapsto a,\ \mathrm{V} \mapsto c,\ \mathrm{D} \mapsto ac.$$

Let us call this function h. Then $h : \mathbf{K}_4 \to \mathbf{H}$ is a bijection, that is, a one-to-one and onto function. Moreover, under h the two tables match in the following sense. If X,Y,Z $\in K_4$ and X$*$Y = Z, then h(X)$\bigoplus$ h(Y) = h(Z).

These ideas can be applied to any groups. Let $\mathbf{G}$ be a group with operation $*$ and let $\mathbf{G}'$ be a group with operation $\circ$. A **homomorphism** from $\mathbf{G}$ to $\mathbf{G}'$ is a function $h : \mathbf{G} \to \mathbf{G}'$ with the property that, for all $x,y,z \in \mathbf{G}$,

$$x * y = z \text{ implies } h(x) \circ h(y) = h(z).$$

A function $h : \mathbf{G} \to \mathbf{G}'$ is called an **isomorphism** if it is a homomorphism that is a bijection. We say that groups $\mathbf{G}$ and $\mathbf{G}'$ are **isomorphic** if there is an isomorphism from $\mathbf{G}$ onto $\mathbf{G}'$, and we express this in symbols as $\mathbf{G} \cong \mathbf{G}'$.

Lemma 60. *A function $h : \mathbf{G} \to \mathbf{G}'$ is a homomorphism if and only if, for all $x,y \in \mathbf{G}$, we have*

$$h(x * y) = h(x) \circ h(y).$$

Lemma 30 will be useful for proving the following fact.

Lemma 61. *Two finite cyclic groups of the same order are isomorphic.*

Logarithms were invented by John Napier in order to exploit a special isomorphism between two familiar and important groups:

Lemma 62. *Let $\mathbf{R}^+$ denote the group of all real numbers under addition, and let $\mathbf{R}^\times$ denote the group of all positive real numbers under multiplication. Then $\mathbf{R}^\times \cong \mathbf{R}^+$.*

Homomorphisms, and therefore also isomorphisms, preserve more than just the binary operation.

Theorem 63. *Let $\mathbf{G}$ and $\mathbf{G}'$ be groups with identities $e \in \mathbf{G}$ and $e' \in \mathbf{G}'$, and let $h : \mathbf{G} \to \mathbf{G}'$ be a homomorphism. Then*

(i) $h(e) = e'$,

(ii) $h(x^{-1}) = h(x)^{-1}$ *for each* $x \in \mathbf{G}$,

(iii) *if* $\mathbf{H}$ *is a subgroup of* $\mathbf{G}$, *then* $h(\mathbf{H})$ *is a subgroup of* $\mathbf{G}'$.

(iv) *if* $\mathbf{K}$ *is a subgroup of* $\mathbf{G}'$, *then* $h^{-1}(\mathbf{K}) := \{a \in G \mid h(a) \in \mathbf{K}\}$ *is a subgroup of* $\mathbf{G}$.

As a special case of part (iv), the subgroup $h^{-1}(\{e'\})$ of $\mathbf{G}$ is called the **kernel** of h and is denoted by $\mathbf{K}_h$. This subgroup is useful for recognizing when a homomorphism is an isomorphism. Applying part (i) we see that, if h happens to be one-to-one, then $\mathbf{K}_h = \{e\}$. The converse is also true.

Lemma 64. *Let $h : \mathbf{G} \to \mathbf{G}'$ be a homomorphism. Then h is one-to-one if and only if $\mathbf{K}_h = \{e\}$.*

Theorem 65. *Isomorphism is an equivalence relation on the class of all groups, that is, for all groups $\mathbf{G}$, $\mathbf{G}'$ and $\mathbf{G}''$,*

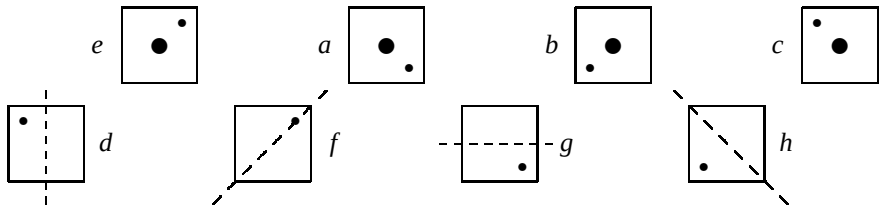
(i) $\mathbf{G} \cong \mathbf{G}$,

(ii) $\mathbf{G} \cong \mathbf{G}'$ *implies* $\mathbf{G}' \cong \mathbf{G}$, *and*

(iii) $\mathbf{G} \cong \mathbf{G}'$ *and* $\mathbf{G}' \cong \mathbf{G}''$ *implies* $\mathbf{G} \cong \mathbf{G}''$.

...

We will now digress briefly to present an important class of finite non-commutative groups. For a positive integer $n \geq 3$, the **dihedral n-group $\mathbf{D}_n$** consists of the rigid motions of a regular n-sided polygon. Since the regular n-gon has n top side orientations and n bottom side orientations, the order of $\mathbf{D}_n$ is $2n$. In case $n = 3$, the group $\mathbf{D}_3$ is the familiar 6-element group $\mathbf{S}_3$. The 8-element dihedral 4-group, $\mathbf{D}_4$, is illustrated below:



Notice that the 4 top side orientations are obtained by successive rotations of the square, while the 4 bottom side orientations can be realized by flip d followed by successive clockwise rotations. In algebraic language, this says that the set $\{a,d\}$ **generates $\mathbf{D}_4$**, as we have

$$b = a^2,\ c = a^3,\ e = a^4;\ f = ad,\ g = a^2d,\ h = a^3d.$$

Instead of listing the elements of $\mathbf{D}_4$ as

$$\mathbf{D}_4 = \{e,a,b,c,d,f,g,h\},$$

we find that the listing

$$\mathbf{D}_4 = \{e,a,a^2,a^3,d,ad,a^2d,a^3d\}$$

provides much more informative names for the elements.

In fact, these names allow us to give a complete description of the group if we remember a small bit of additional information. Clearly, a has order 4 and d has order 2. Going back to the square itself, we can compute the product $da = h = a^3d$. Thus we can describe $\mathbf{D}_4$ by giving **generators** and **defining relations** as

$$\mathbf{D}_4 = \mathbf{sg}\{a,d \mid a^4 = e = d^2,\ da = a^3d\}. \qquad (\star)$$

This means that $\mathbf{D}_4$ consists of all products of a's and d's subject only to the constraints implied by the defining relations. From this information we can deduce that $\mathbf{D}_4$ has the 8

elements listed, and we can fill in the complete table for $\mathbf{D}_4$. For example, to compute the product of a^3d and a^2d, we have

$$(a^3d)(a^2d) = a^3(da)ad = a^3(a^3d)ad = a^6(da)d$$
$$= a^6(a^3d)d = a^9d^2 = a(a^4)(a^4)(d^2) = aeee = a$$

The strategy here is to use $da = a^3d$ to express the product as a power of a times a power of d, and then to use $a^4 = e = d^2$ to reduce the exponents. Similarly, for any positive integer n, we can describe $\mathbf{D}_n$ as

$$D_n = \mathbf{sg}\{a,d \mid a^n = e = d^2,\ da = a^{n-1}d\}.$$

where a has order n and b as order 2, and $ba = a^{n-1}b$.

Problem 66. *Using $(\star)$, fill out a table for $\mathbf{D}_4$ without referring to the square itself.*

Problem 67. *Using the description*

$$\mathbf{S}_3 = \mathbf{sg}\{a,c \mid a^3 = e = c^2,\ ca = a^2c\},$$

list the distinct elements of $\mathbf{S}_3$ and fill out its table without referring to the triangle.

...

The notion of isomorphism allows us to articulate a fundamental goal of group theory. Given a property P that a group may or may not have, we seek a **representation theorem** for this property. What this means is that we would like to find a set of specific well understood groups that have property P, and then prove that every group with property P is isomorphic to a group in our set. For example, let P be the property of having prime order p. A well understood group of order p is the group $\mathbf{Z}_p$. If $\mathbf{G}$ has property P, then $\mathbf{G}$ is cyclic by Theorem 47 and consequently $\mathbf{G} \cong \mathbf{Z}_p$ by Lemma 61. This gives us a nice representation theorem.

Theorem *Every group of prime order p is isomorphic to $\mathbf{Z}_p$.*

In order to prove the following representation theorems, you will need to spend some time examining elements of the group, considering their possible orders, and looking at the subgroups they generate. Recall that, if p and q are both prime, then the only divisors of pq are $1, p, q$ and pq.

Theorem 68. *Let p and q be distinct primes. Then every commutative group of order pq is cyclic and is therefore isomorphic to $\mathbf{Z}_{pq}$.*

Lemma 69. *Let p be a prime. Then every commutative group of order p^2 is isomorphic to either the cyclic group $\mathbf{Z}_{p^2}$ or to the direct product $\mathbf{Z}_p \times \mathbf{Z}_p$.*

It turns out that there is a beautiful representation theory for all finite *commutative* groups which extends the three previous results. The final theorem, which we won't prove here, states that *every finite commutative group is isomorphic to a direct product of cyclic groups*.

Representation of non-commutative groups is a fascinating subject that proves to be much more difficult. In fact, a full description of all finite groups is not yet known. A well

known representation theorem for all groups was first discovered by Sir Arthur Cayley (1821-1895). In Theorem 15 we saw that the left multiplication function ℓ associates each element a of a group $\mathbf{G}$ with a permutation ℓ_a of $\mathbf{G}$. Thus $\ell : \mathbf{G} \to \mathbf{S}_\mathbf{G}$. In fact, ℓ is a one-to-one homomorphism:

Cayley Representation Theorem 70. *Every group* $\mathbf{G}$ *is isomorphic to a subgroup of the permutation group* $\mathbf{S}_X$ *for some set* X*, namely, for* $X = \mathbf{G}$.

In the remainder of this chapter we will prove two important theorems which, together with what we have, will provide a full description of finite groups of many small orders. Our next theorem extends Theorem 68 to all groups in the case that $p = 2$.

Theorem 71. *Let* q *be a prime. Then every group of order* $2q$ *is isomorphic to either the cyclic group* $\mathbf{Z}_{2q}$ *or to the dihedral group* $\mathbf{D}_q$.

The Lemma 69 is called a "lemma" because, as we will now see, it can be extended to all groups by utilizing some new techniques. Elements a and b of a group $\mathbf{G}$ are said to be **conjugate** if there is an element $x \in \mathbf{G}$ such that $b = x^{-1}ax$. In this case we write $a \equiv_c b$ and say that a **is conjugate to** b.

Theorem 72. *For a group* $\mathbf{G}$*, the relation* $\equiv_c$ *is an equivalence relation.*

Theorem 73. *For a group* $\mathbf{G}$*,*

(i) *Conjugacy is the equality relation if and only if* $\mathbf{G}$ *is commutative.*

(ii) *Conjugate elements of* $\mathbf{G}$ *have the same order.*

Problem 74. *Find all of the conjugate classes of* $\mathbf{S}_3$.

The $\equiv_c$–classes of $\mathbf{G}$ are called the **conjugate classes** of $\mathbf{G}$.

If a is an element of the group $\mathbf{G}$, the **normalizer** of a is defined to be the set

$$\mathbf{N}_a := \{x \in \mathbf{G} \mid xa = ax\}$$

of elements that commute with a.

Lemma 75. *The normalizer of an element of a group is a subgroup.*

Lemma 76. *Let* $\mathbf{G}$ *be a group with* $a, x, y \in \mathbf{G}$*. Then* $\mathbf{N}_a x = \mathbf{N}_a y$ *if and only if* $x^{-1}ax = y^{-1}ay$*.* [*In words, two elements are in the same right coset of the normalizer of a if and only if they produce the same conjugate of* a.]

Recall that if $\mathbf{H}$ is a subgroup of a finite group $\mathbf{G}$, then the **index** of $\mathbf{H}$ in $\mathbf{G}$ is the number $[\mathbf{G} : \mathbf{H}]$ of right (or left) cosets of $\mathbf{H}$ in $\mathbf{G}$. LaGrange's Theorem now tells us something important about conjugate classes.

Lemma 77. *Let* $\mathbf{G}$ *be a finite group with* $a \in \mathbf{G}$*. Then the order of the conjugate class of* a *is equal to the index of the normalizer of* a*, that is,* $\circ([a]_{\equiv_c}) = [\mathbf{G} : \mathbf{N}_a]$*. In particular,* $\circ([a]_{\equiv_c}) \mid \circ(\mathbf{G})$.

(Show that the set of conjugates of a and the set of right cosets of $\mathbf{N}_a$ are the *same size*.)

A subgroup always contains at least one element, the identity, and the conjugate class of a always contains at least the one element a. If one of these sets contains only this one element it is said to be **trivial**; otherwise it is **non-trivial**. The **center** of a group $\mathbf{G}$ is defined as

$$Z(\mathbf{G}) := \{b \in \mathbf{G} \mid ba = ab \text{ for all } a \in \mathbf{G}\},$$

the elements b of $\mathbf{G}$ that commute with every element of $\mathbf{G}$. In other words, $Z(\mathbf{G})$ in the intersection of all of the normalizers of elements of $\mathbf{G}$.

Lemma 78. *The center $Z(\mathbf{G})$ is a subgroup of $\mathbf{G}$ which is exactly the union of the trivial conjugate classes of G.*

Now let $\mathbf{G}$ be a finite group and let $a_1, a_2, \ldots, a_m \in \mathbf{G}$ be a list of representatives of the distinct non-trivial conjugate classes of $\mathbf{G}$. Then we can partition $\mathbf{G}$ into its trivial and non-trivial conjugate classes as

$$\mathbf{G} = Z(\mathbf{G}) \cup [a_1]_{\equiv_c} \cup [a_2]_{\equiv_c} \cup \cdots \cup [a_m]_{\equiv_c}.$$

It follows that the order of $\mathbf{G}$ is the sum of the number of elements in each piece of this partition. This assertion yields an important numerical property of a group that is called the **Class Equation** of $\mathbf{G}$:

$$\circ(\mathbf{G}) = \circ(Z(\mathbf{G})) + \circ([a_1]_{\equiv_c}) + \circ([a_2]_{\equiv_c}) + \cdots + \circ([a_m]_{\equiv_c}).$$

Lemma 79. *If the order of a group is a power of a prime, then the group has a non-trivial center.*

Theorem 80. *Let p be a prime. Then every group of order p^2 is commutative, and is therefore isomorphic to either the cyclic group $\mathbf{Z}_{p^2}$ or to the direct product $\mathbf{Z}_p \times \mathbf{Z}_p$.*

Problem 81. *For which of the numbers n from 1 to 25 do you now know, up to isomorphism, all of the groups of order n? Make a list which gives, for each such number n, all of the non-isomorphic n–element groups.*

Chapter 7

Normal Subgroups & Quotients

Imagine that you arrive late to algebra class one day, somewhat more tired than usual, and you sit down in back where you hope not to be noticed. You see the professor up front holding a square with a black dot in the center of one side and talking about a new group $\mathbf{D}_4$. But, in your present state and location, you don't see the little dot in the corner. To you the elements of the subgroup $\mathbf{N} := \{e, a, a^2, a^3\}$ all appear to be equivalent and indistinguishable, as do also the elements of the right coset $\mathbf{N}d = \{d, ad, a^2d, a^3d\}$. To you it appears that the professor is presenting a 2-element group $\mathbf{G} = \{N, Nd\}$. When asked to fill out a table for the group, you quickly whip out the a nice little group table below. It has $\mathbf{N}$ as its identity and is isomorphic to $\mathbf{Z}_2$.

$*$	N	Nd
N	N	Nd
Nd	Nd	N

It is only after a few idle minutes while your fellow students continue hard at work that you look over at what they are doing and discover your error. But wait a minute. Haven't you just found a neat way to make a new group from the right cosets of a subgroup?!

Let $\mathbf{G}$ be any group with a subgroup $\mathbf{N}$, and let $\mathbf{G}/\mathbf{N}$ denote the set of right cosets of $\mathbf{N}$ in $\mathbf{G}$. [We use this notation because the *number* of right cosets of $\mathbf{N}$ in $\mathbf{G}$ is $\circ(\mathbf{G})/\circ(\mathbf{N})$ when $\mathbf{G}$ is finite.] Define a binary operation $\cdot$ on $\mathbf{G}/\mathbf{N}$ by

$$\mathbf{N}x \cdot \mathbf{N}y := \mathbf{N}xy \quad \text{for all} \quad x, y \in \mathbf{G}. \tag{$\star\star$}$$

In words, the product of the right coset of x and the right coset of y is the right coset of xy. Notice that $\mathbf{G}/\mathbf{N}$ inherits group properties from $\mathbf{G}$:

- $\cdot$ is associative since $\mathbf{N}x \cdot (\mathbf{N}y \cdot \mathbf{N}z) = \mathbf{N}x \cdot \mathbf{N}yz = \mathbf{N}x(yz) = \mathbf{N}(xy)z = \mathbf{N}xy \cdot \mathbf{N}z = (\mathbf{N}x \cdot \mathbf{N}y) \cdot \mathbf{N}z$,
- $\mathbf{N}e \cdot \mathbf{N}x = \mathbf{N}ex = \mathbf{N}x = \mathbf{N}xe = \mathbf{N}x \cdot \mathbf{N}e$, so $\mathbf{N} = \mathbf{N}e$ is an identity,
- $\mathbf{N}x \cdot \mathbf{N}x^{-1} = \mathbf{N}xx^{-1} = \mathbf{N}e = \mathbf{N}x^{-1}x = \mathbf{N}x^{-1} \cdot \mathbf{N}x$, so $\mathbf{N}x^{-1}$ is the inverse of $\mathbf{N}x$.

By gum, $\mathbf{G}/\mathbf{N}$ is a group! We call $\mathbf{G}/\mathbf{N}$ the **quotient group** of **G modulo N** (or **G mod N** for short).

Problem 82. *List the distinct right cosets of the subgroup* $\mathbf{N} := \{7n \mid n \in \mathbf{Z}\}$ *of* $\mathbf{Z}$ *and construct a table for the quotient group* $\mathbf{Z}/\mathbf{N}$ *(the* **integers modulo** 7*).*

Problem 83. *List the distinct right cosets of the subgroup* $\mathbf{N} := \{0,3,6,9\}$ *of* $\mathbf{Z}_{12}$ *and construct a table for the quotient group* $\mathbf{Z}_{12}/\mathbf{N}$.

Problem 84. *List the distinct right cosets of the subgroup* $\mathbf{N} := \{e,c\}$ *of* $\mathbf{S}_3$ *and construct a table for the quotient group* $\mathbf{S}_3/\mathbf{N}$.

Now, if you were careful you should have run into some difficulty with the last quotient group $\mathbf{S}_3/\mathbf{N}$. What, for example, is the product of the right cosets $\mathbf{N}a = \{a, a^2c\}$ and $\mathbf{N}a^2 = \{a^2, ac\}$? On the one hand, we have

$$\mathbf{N}a \cdot \mathbf{N}a^2 = \mathbf{N}a^3 = \mathbf{N}e = \mathbf{N}.$$

On the other hand, $\mathbf{N}a = \mathbf{N}a^2c$ and $\mathbf{N}a^2 = \mathbf{N}ac$, so that

$$\mathbf{N}a \cdot \mathbf{N}a^2 = \mathbf{N}a^2c \cdot \mathbf{N}ac = \mathbf{N}(a^2c)(ac) = \mathbf{N}a \neq \mathbf{N}!$$

It appears that the "product" of the cosets $\mathbf{N}a$ and $\mathbf{N}a^2$ changes depending on which names (representatives) we choose for these cosets. In a case like this we say here that the "operation" $\cdot$ on $\mathbf{S}_3/\mathbf{N}$ is **not well defined**, that is, it is simply nonsense.

Definition *A subgroup* $\mathbf{N}$ *of a group* $\mathbf{G}$ *is called a* **normal subgroup** *of* $\mathbf{G}$ *if the representative operation* $\cdot$ *on* $\mathbf{G}/\mathbf{N}$ *given by* $(\star\star)$ *is* ***well defined****, that is,*

$$\textit{if } \mathbf{N}x_1 = \mathbf{N}x_2 \textit{ and } \mathbf{N}y_1 = \mathbf{N}y_2, \textit{ then } \mathbf{N}x_1y_1 = \mathbf{N}x_2y_2$$

for all $x_1, x_2, y_1, y_2 \in \mathbf{G}$.

Problem 85. *Verify that* $\mathbf{N} := \{e, a, a^2, a^3\}$ *is a normal subgroup of* $\mathbf{D}_4$.

We can now stop to summarize what we have found.

Theorem *Let* $\mathbf{N}$ *be a subgroup of the group* $\mathbf{G}$. *If* $\mathbf{N}$ *is a normal subgroup, then* $\mathbf{G}/\mathbf{N}$ *is a group with operation* $\cdot$ *defined by* $(\star\star)$. *If* $\mathbf{N}$ *is not normal, then* $(\star\star)$ *does not define a binary operation at all.*

What we need to know, then, is how to tell whether or not a subgroup $\mathbf{N}$ is normal. There are several different ways to do this.

Theorem 86. *For a group* $\mathbf{G}$ *and a subgroup* $\mathbf{N}$, *these are equivalent.*

(i) $\mathbf{N}$ *is a normal subgroup of* $\mathbf{G}$.

(ii) $\mathbf{N}x = x\mathbf{N}$ *for all* $x \in \mathbf{G}$ (*every right coset is a left coset*).

(iii) *For all* $x \in \mathbf{G}$ *and* $a \in \mathbf{N}$, *the conjugate* $x^{-1}ax$ *is in* $\mathbf{N}$.

Corollary 87. *Every subgroup of a commutative group is normal.*

Corollary 88. *Every subgroup of a group of index two is normal.*

Corollary 89. *The center of every group is a normal subgroup.*

Corollary 90. *The kernel of every homomorphism is a normal subgroup.*

When we form the quotient $\mathbf{G}/\mathbf{N}$ of $\mathbf{G}$ by a normal subgroup $\mathbf{N}$, we think of collapsing, and thereby eliminating, the elements of $\mathbf{N}$. It is sometimes possible to start with a group that is in some sense "bad", then gather the "bad" elements into a normal subgroup. By dividing out this normal subgroup, we get a quotient group that is "good" since it has no "bad" elements left.

For example, being commutative is surely a "good" property for a group. If $\mathbf{G}$ is a group and $a, b \in \mathbf{G}$, the **commutator** of a and b is defined as

$$[a,b] := a^{-1}b^{-1}ab.$$

Lemma 91. *For elements a, b, x in a group $\mathbf{G}$,*

(i) $[a,b] = e$ *if and only if a and b commute.*

(ii) $[a,b]^{-1} = [b,a]$ (*The inverse of a commutator is a commutator.*),

(iii) $x^{-1}[a,b]x = [x^{-1}ax, x^{-1}bx]$ (*The conjugate of a commutator is the commutator of the conjugates.*)

If you prefer commutative groups, then you have to think of commutators (other than e) as "bad" elements. Let $[\mathbf{G},\mathbf{G}]$ denote the set of all commutators and finite products of commutators of elements of $\mathbf{G}$.

Lemma 92. *If $\mathbf{G}$ is a group, then $[\mathbf{G},\mathbf{G}]$ is a normal subgroup of $\mathbf{G}$* (*called the* **commutator subgroup** *of $\mathbf{G}$*).

Because each commutator different from e witnesses the failure of two elements to commute, the size of the commutator subgroup is a measure of how non-commutative $\mathbf{G}$ is. Thus, by (i), $[\mathbf{G},\mathbf{G}] = \{e\}$ if and only if $\mathbf{G}$ is commutative, and a larger commutator subgroup indicates more non-commuting elements. When we form the quotient group $\mathbf{G}/[\mathbf{G},\mathbf{G}]$, we collapse all of the witnesses of failure of commutativity to the identity. The result is a group with no witnesses to failure of commutativity.

Theorem 93. *For every group $\mathbf{G}$, the quotient $\mathbf{G}/[\mathbf{G},\mathbf{G}]$ of $\mathbf{G}$ by its commutator subgroup is a commutative group.*

Another illustration of quotient groups comes from an extension of Problem 53 and the group $\mathbf{P}_{abc}$ with operation $\oplus$. Let $S = \{a,b,c,d,e,f,g,h\}$, $T = \{a,b,c\}$ and $U = \{d,e,f,g,h\}$. Problem 53 asks us to think of T as the "important" elements of S, and think of U as the "unimportant" elements of S. We then think of two members of $\mathbf{P}_S$ as being equivalent if they contain the same important elements.

Like $\mathbf{P}_{abc}$, the collection of subsets $\mathbf{P}_S$ of S, subsets $\mathbf{P}_T$ of T and subsets $\mathbf{P}_U$ of U each form a group under symmetric difference $\oplus$.

Problem 94. *Define $f : \mathbf{P}_S \to \mathbf{P}_T$ by $f(X) := X \cap T$. Thus $f(X)$ consists of the "important" elements of X.*

(i) *Show that f is a homomorphism from $\mathbf{P}_S$ onto $\mathbf{P}_T$.* (*This says that the sum of the important elements in X and the important elements in Y is exactly the important elements in $X \oplus Y$.*)

(ii) *Show that* $\mathbf{P}_U$ *is the kernel of* f.

(iii) *For* $X,Y \in \mathbf{P}_S$, *show that* $f(X) = f(Y)$ *if and only if* X *and* Y *are in the same coset of* $\mathbf{P}_U$.

(iv) *Show the* $\mathbf{P}_S/\mathbf{P}_U \cong \mathbf{P}_T$. (*Be sure that your isomorphism is well defined.*)

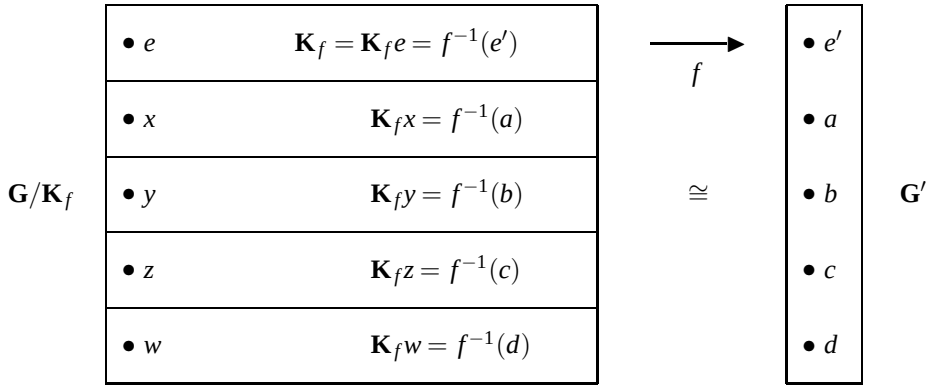
We will see that the conclusion of Problem 94 is quite general. A group $\mathbf{G}'$ is said to be a **homomorphic image** of a group $\mathbf{G}$ if there is a homomorphism $f : \mathbf{G} \to \mathbf{G}'$ from $\mathbf{G}$ onto $\mathbf{G}'$.

Theorem 95. *Every quotient of a group* $\mathbf{G}$ *is a homomorphic image of* $\mathbf{G}$. *More specifically, if* $\mathbf{N}$ *is a normal subgroup of* $\mathbf{G}$, *then the* **natural homomorphism** $h : \mathbf{G} \to \mathbf{G}/\mathbf{N}$, *given by* $h(x) := \mathbf{N}x$, *is a homomorphism from* $\mathbf{G}$ *onto* $\mathbf{G}/\mathbf{N}$.

Lemma 96. *Let* $f : \mathbf{G} \to \mathbf{G}'$ *be a homomorphism,* $x,y \in \mathbf{G}$. *Then* $f(x) = f(y)$ *if and only if* $\mathbf{K}_f x = \mathbf{K}_f y$.

We can now prove that every homomorphic image of a group is isomorphic to a quotient of that group.

The Isomorphism Theorem 97. *If* $f : \mathbf{G} \to \mathbf{G}'$ *is an onto homomorphism, then* $\mathbf{G}/\mathbf{K}_f \cong \mathbf{G}'$.



(For example, if $xy = w$, then $\mathbf{K}_f x \cdot \mathbf{K}_f y = \mathbf{K}_f w$ and $ab = d$.)

Wow – quotient groups – what a great idea! And in the end, they turn out to be exactly the same as homomorphic images. But just as you are thinking this, there is an unsettling disturbance.

"You – yes, you in the back there! Can you come up to the board and show us your table for $\mathbf{D}_4$?"

"Well, no Professor, I'm sorry – I can't. But I've just found a really neat way to patch together a whole bunch of new groups! Can I put that up instead?"

Chapter 8

Other Algebras

A slightly more sophisticated way to view a **group G** is to think of it as consisting of a set G together with a binary operation $* : G \times G \to G$, a unary operation $^{-1} : G \to G$ and a constant $e \in G$,

$$\mathbf{G} = \langle G; *, ^{-1}, e \rangle,$$

where $*$ is associative, e is an identity, and x^{-1} is an inverse of x for each $x \in G$. It turns out that there are many different familiar algebraic systems that are similar to groups and can be studied in much the same way that we have studied groups. An **algebra**

$$\mathbf{A} = \langle A; \circ, *, +, \ldots, ^{-1}, \alpha, \neg, \ldots, e, 0, 1, \ldots \rangle$$

consists of a set A, a collection $\circ, *, +, \ldots$ of binary operations on A, a collection $^{-1}, \alpha, \neg, \ldots$ of unary operations on A, and a set $e, 0, 1, \ldots$ of distinguished constants from A.

Many central notions from group theory extend to all algebras. For example, an algebra

$$\mathbf{B} = \langle B; \circ, *, +, \ldots, ^{-1}, \alpha, \neg, \ldots, e, 0, 1, \ldots \rangle$$

is a **subalgebra** of **A** if it is closed under each of the operations of **A**, that is,

- if $x, y \in B$ and $*$ is a binary operation of **A**, then $x * y \in B$;
- if $x \in B$ and $'$ is a unary operation of **A**, then $x' \in B$, and
- if e is a constant of **A**, then $e \in B$.

Notice that a subset of a group forms a subgroup in the usual sense if and only if it is a subalgebra in this sense.

Similarly, a function h from an algebra **A** to an algebra **B** is a **homomorphism** if it preserves each of the operations, that is,

- $h(x * y) = h(x) * h(y)$ for each binary operation $*$ and all $x, y \in A$;
- $h(x') = h(x)'$ for each unary operation $'$ and all $x \in A$;
- $h(e_A) = e_B$ where e_A is a constant of **A** and e_B is the corresponding constant of **B**.

Algebras **A** and **B** are **isomorphic** if there is a bijection $h : \mathbf{A} \to \mathbf{B}$ which is a homomorphism.

As we did with groups, we like to study classes of algebras with a fixed type of operations satisfying a fixed set of axioms. In this chapter we will introduce three such examples.

RINGS

Our childhood experience with mathematics begins with the arithmetic of the integers and the rational numbers. These are two of many familiar examples of another kind of algebra. A **ring with identity** is an algebra $\mathbf{R} = \langle R; +, \cdot, -, 0, 1\rangle$ with two binary operations $+, \cdot$, a unary operation $-$ and two constants 0 and 1 such that

1. $\langle R; +, -, 0\rangle$ is a commutative group,
2. for all $x, y, z \in R$,
   - $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
   - $1 \cdot x = x = x \cdot 1$,
   - $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

The third condition is expressed in words by saying that, "The operation $\cdot$ **distributes** over $+$." Note that since $\cdot$ may not be commutative, we must verify both distributive properties.

Lemma 98. *If* **R** *is a ring with identity and* $x \in R$*, then* $x \cdot 0 = 0 = 0 \cdot x$ *and* $-x = (-1) \cdot x$.

Problem 99. *Assume that* $\mathbf{R}^{+\cdot}$*, the real numbers with the usual operations, is a ring with identity. Show that each of the following is a ring with identity.* (*In each case you will need to tell what* 0 *and* 1 *are.*)

Z, *the set of integers with the usual operations.*

C, *the set of complex numbers with the usual operations,* $(a + bi) + (c + di) := (a + c) + (b + d)i$ *and* $(a + bi) \cdot (c + di) := (ac - bd) + (bc + ad)i$.

M, *the set of 2-by-2 matrices over* **Z** *with the usual matrix addition and multiplication.*

$\mathbf{P_S} := \langle \mathbf{P}_S; \oplus, \cap, -, \varnothing\rangle$ *where S is a set,* $\mathbf{P}_S$ *is the collection of subsets of S, and* $-X := X$ *for* $X \in P_S$.

F, *the set of real valued functions defined on the set of real numbers, with the usual addition and multiplication,* $(f + g)(x) := f(x) + g(x)$ *and* $(f \cdot g)(x) := f(x)g(x)$.

Problem 100. *Show that* **Z** *is a subring of* $\mathbf{R}^{+\cdot}$ *which is a subring of* **C**.

Problem 101. *Let a be a real number, and define* $h_a : \mathbf{F} \to \mathbf{R}^{+\cdot}$ *by* $h_a(f) := f(a)$. *Show that* h_a *is a ring homomorphism.*

Problem 102. *Let T be a subset of a set S and define* $h : \mathbf{P_S} \to \mathbf{P_T}$ *by* $h(X) := X \cap T$. *Show that h is a ring homomorphism. Show that the multiplication operation* $\cap$ *is well defined on the set of cosets* $\mathbf{P_S}/\mathbf{K}_h$*, and that* $\mathbf{P_S}/\mathbf{K}_h$ *is itself a ring with identity that is isomorphic to* $\mathbf{P_T}$.

LINEAR SPACES

In a college Linear Algebra course we learn about systems called "linear spaces". A **linear space** is an algebra $\mathbf{L} = \langle L; +, -, \mathbf{0}, a\rangle_{a\in R}$ with a binary operation $+$, a unary operation $-$, and a unary operation a for each real number $a \in R$ such that

1. $\langle L; +, -, \mathbf{0}\rangle$ is a commutative group,
2. for all $X, Y \in L$ and $a, b \in R$,
   - $a(X+Y) = aX + aY$,
   - $(a+b)X = aX + bX$,
   - $a(bX) = (ab)X$ and
   - $aX = \mathbf{0}$ if and only if $a = 0$ or $X = \mathbf{0}$.

The study of linear spaces is called **linear algebra**. There are many familiar linear spaces: the Euclidean plane $\mathbf{R}^2$, Euclidean 3-space $\mathbf{R}^3$, Euclidean n-space $\mathbf{R}^n$, the space of real valued functions on any fixed domain, the space of solutions to a homogeneous differential equation, the space of n-by-m matrices, etc.

A subalgebra of a linear space $\mathbf{L}$ is called a **subspace**. The smallest subalgebra of $\mathbf{L}$ containing a set $S \subseteq L$ is called the **span** of S, written $\mathrm{Span}(S)$. A generating set for $\mathbf{L}$ is called a **spanning set**. A homomorphism from one linear space to another is called a **linear transformation**.

Theorem 103. *Let* $\mathbf{L}$ *be a linear space, let* $\mathbf{M}$ *be any subspace of* $\mathbf{L}$*, and let* $\mathbf{L}/\mathbf{M}$ *be the set of right cosets of* $\mathbf{M}$ (*which forms a group under* $+$ *since* $\mathbf{M}$ *is a normal subgroup*). *Then scalar multiplication is always well defined on* $\mathbf{L}/\mathbf{M}$ *as*

$$a(\mathbf{M}+X) := \mathbf{M}+aX,$$

and $\langle \mathbf{L}/\mathbf{M}; +, -, 0, a\rangle_{a\in R}$ *is itself a linear space* (*called the* **quotient space**).

BOOLEAN ALGEBRA

Modern algebra became a viable subject beyond group theory in the 1850's when George Boole showed how the laws of logical inference can be codified into an algebraic system in which the elements are statements. What we have come to call a **Boolean algebra** is an algebra $\mathbf{B} = \langle B; \vee, \wedge, ', 0, 1\rangle$ with two binary operations **join** $\vee$ and **meet** $\wedge$, a unary operation of **complementation** $'$, and constants 0 and 1 such that, for all $x, y \in B$,

1. $\vee$ and $\wedge$ are both commutative and associative, and each distributes over the other,
2. $x \vee x = x$ and $x \wedge x = x$,
3. $x \vee (y \wedge x) = x$ and $x \wedge (y \vee x) = x$,
4. $x \vee 1 = 1$ and $x \wedge 0 = 0$,
5. $x \vee x' = 1$ and $x \wedge x' = 0$.

There are two important and familiar examples of Boolean algebras.

Let S be a set and let $\mathbf{P}(S)$ denote the collection of all subsets of S. Then $\cup$ and $\cap$ are binary operations on $\mathbf{P}(S)$, complementation $\sim$ is a unary operation on $\mathbf{P}(S)$, and $\varnothing$ and S are special elements of $\mathbf{P}(S)$. The proof of the following theorem has many parts, all of which are normally done in a foundations course in mathematics.

Theorem 104. *If S is a set, then $\mathbf{P}(\mathbf{S}) := \langle \mathbf{P}(S); \cup, \cap, \sim, \varnothing, S\rangle$ is a Boolean algebra.*

Formulating propositional logic as a Boolean algebra requires an extra step that we draw from our experience with quotient groups. Consider any fixed set of propositional variables $p, q, r, \ldots$, each representing a fixed statement. If we use $\vee$ for "or", $\wedge$ for "and", $'$ for "not", 0 for "False" and 1 for "True", we can combine propositional variables to for compound sentences such as

$$((p \vee 1) \wedge r)' \vee (q' \wedge (p \vee r)).$$

If C denotes the set of all compound sentences, then $\vee$ and $\wedge$ are binary operations on C while $'$ is a unary operation and 0 and 1 are constants in C. This gives us an algebra

$$\mathbf{C} := \langle C; \vee, \wedge, ', 0, 1\rangle.$$

Is $\mathbf{C}$ a Boolean algebra? For example, is $\wedge$ commutative? We have $(q \vee r), p \in C$ so, for commutativity, we would need to know that

$$(q \vee r) \wedge p = p \wedge (q \vee r).$$

Is this the case? While these two compound sentences seem to make the same assertion ("p is true and either q or r is true."), they are not really the same member of C. So $\wedge$ is not commutative. But the two compound sentences are equivalent in a natural sense: they have the same true tables.

These observations lead us to the following construction. For $x, y \in C$, we say that $x \equiv y$ if x and y have the same truth tables. We check that $\equiv$ is an equivalence relation and define

$$B = C/\equiv = \{[x] \mid x \in C\}$$

to be the set of equivalence classes of C.

Theorem 105. *The representative operations $\vee$, $\wedge$ and $'$ are well defined on B by $[x] \vee [y] := [x \vee y]$, $[x] \wedge [y] := [x \wedge y]$ and $[x]' := [x']$, and the quotient algebra*

$$\mathbf{B} := \langle B; \vee, \wedge, ', [0], [1]\rangle$$

is a Boolean algebra.

These operations on the equivalence classes are well defined in exactly the same sense that a group operation is well defined on the cosets of a normal subgroup. The resulting Boolean algebra $\mathbf{B}$ is called the **Lindenbaum-Tarski algebra** for propositional logic. It allows us to understand mathematical logic through algebra.