CHAPTER 2

Groups

Il est peu de notions en mathématiques qui soient plus primitives que celle de loi de composition.

—Nicolas Bourbaki

2.1 LAWS OF COMPOSITION

A *law of composition* on a set S is any rule for combining pairs a, b of elements of S to get another element, say p, of S. Some models for this concept are addition and multiplication of real numbers. Matrix multiplication on the set of $n \times n$ matrices is another example.

Formally, a law of composition is a function of two variables, or a map

$$S \times S \to S.$$

Here $S \times S$ denotes, as always, the *product set*, whose elements are pairs a, b of elements of S.

The element obtained by applying the law to a pair a, b is usually written using a notation resembling one used for multiplication or addition:

$$p = ab, \quad a \times b, \quad a \circ b, \quad a + b,$$

or whatever, a choice being made for the particular law in question. The element p may be called the product or the sum of a and b, depending on the notation chosen.

We will use the product notation ab most of the time. Anything done with product notation can be rewritten using another notation such as addition, and it will continue to be valid. The rewriting is just a change of notation.

It is important to note right away that ab stands for a certain element of S, namely for the element obtained by applying the given law to the elements denoted by a and b. Thus if the law is matrix multiplication and if $a = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$, then ab denotes the matrix $\begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}$. Once the product ab has been evaluated, the elements a and b cannot be recovered from it.

With multiplicative notation, a law of composition is *associative* if the rule

$$(ab)c = a(bc) \quad \text{(associative law)} \tag{2.1.1}$$

holds for all a, b, c in S, where $(ab)c$ means first multiply (apply the law to) a and b, then multiply the result ab by c. A law of composition is *commutative* if

$$ab = ba \quad \textit{(commutative law)} \tag{2.1.2}$$

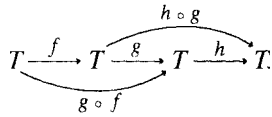
holds for all a and b in S. Matrix multiplication is associative, but not commutative.

It is customary to reserve additive notation $a + b$ for commutative laws – laws such that $a + b = b + a$ for all a and b. Multiplicative notation carries no implication either way concerning commutativity.

The associative law is more fundamental than the commutative law, and one reason for this is that composition of functions is associative. Let T be a set, and let g and f be maps (or functions) from T to T. Let $g \circ f$ denote the composed map $t \rightsquigarrow g(f(t))$: first apply f, then g. The rule

$$g, f \rightsquigarrow g \circ f$$

is a law of composition on the set of maps $T \to T$. This law is associative. If f, g, and h are three maps from T to T, then $(h \circ g) \circ f = h \circ (g \circ f)$:



Both of the composed maps send an element t to $h(g(f(t)))$.

When T contains two elements, say $T = \{a, b\}$, there are four maps $T \to T$:

i: the *identity* map, defined by $i(a) = a$, $i(b) = b$;

τ: the *transposition*, defined by $\tau(a) = b$, $\tau(b) = a$;

α: the constant function $\alpha(a) = \alpha(b) = a$;

β: the constant function $\beta(a) = \beta(b) = b$.

The law of composition on the set $\{i, \tau, \alpha, \beta\}$ of maps $T \to T$ can be exhibited in a *multiplication table*:

(2.1.3)

	i	τ	α	β
i	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β

,

which is to be read in this way:

	f
	$\vdots$
g	$\cdots$ $g \circ f$

Thus $\tau \circ \alpha = \beta$, while $\alpha \circ \tau = \alpha$. Composition of functions is not a commutative law.

Going back to a general law of composition, suppose we want to define the product of a string of n elements of a set: $a_1a_2 \cdots a_n = ?$ There are various ways to do this using the given law, which tells us how to multiply two elements. For instance, we could first use the law to find the product a_1a_2, then multiply this element by a_3, and so on:

$$((a_1a_2)a_3)a_4 \cdots .$$

There are several other ways to form a product with the elements in the given order, but if the law is *associative*, then all of them yield the same element of S. This allows us to speak of the product of an arbitrary string of elements.

Proposition 2.1.4 Let an associative law of composition be given on a set S. There is a unique way to define, for every integer n, a product of n elements $a_1, \ldots, a_n$ of S, denoted temporarily by $[a_1 \cdots a_n]$, with the following properties:

(i) The product $[a_1]$ of one element is the element itself.

(ii) The product $[a_1a_2]$ of two elements is given by the law of composition.

(iii) For any integer i in the range $1 \leq i < n$, $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \ldots a_n]$.

The right side of equation (iii) means that the two products $[a_1 \ldots a_i]$ and $[a_{i+1} \ldots a_n]$ are formed first, and the results are then multiplied using the law of composition.

Proof. We use induction on n. The product is defined by (i) and (ii) for $n \leq 2$, and it does satisfy (iii) when $n = 2$. Suppose that we have defined the product of r elements when $r \leq n - 1$, and that it is the unique product satisfying (iii). We then define the product of n elements by the rule

$$[a_1 \cdots a_n] = [a_1 \cdots a_{n-1}][a_n],$$

where the terms on the right side are those already defined. If a product satisfying (iii) exists, then this formula gives the product because it is (iii) when $i = n - 1$. So if the product of n elements exists, it is unique. We must now check (iii) for $i < n - 1$:

$$\begin{aligned}
[a_1 \cdots a_n] &= [a_1 \cdots a_{n-1}][a_n] && \text{(our definition)} \\
&= ([a_1 \cdots a_i][a_{i+1} \cdots a_{n-1}])[a_n] && \text{(induction hypothesis)} \\
&= [a_1 \cdots a_i]([a_{i+1} \cdots a_{n-1}][a_n]) && \text{(associative law)} \\
&= [a_1 \cdots a_i][a_{i+1} \cdots a_n] && \text{(induction hypothesis).}
\end{aligned}$$

This completes the proof. We will drop the brackets from now on and denote the product by $a_1 \cdots a_n$. □

An *identity* for a law of composition is an element e of S such that

$$ea = a \quad \text{and} \quad ae = a, \quad \text{for all } a \text{ in } S. \tag{2.1.5}$$

There can be at most one identity, for if e and e' are two such elements, then since e is an identity, $ee' = e'$, and since e' is an identity, $e = ee'$. Thus $e = ee' = e'$.

Both matrix multiplication and composition of functions have an identity. For $n \times n$ matrices it is the identity matrix I, and for the set of maps $T \to T$ it is the identity map – the map that carries each element of T to itself.

• The identity element will often be denoted by 1 if the law of composition is written multiplicatively, and by 0 if the law is written additively. These elements do not need to be related to the *numbers* 1 and 0, but they share the property of being identity elements for their laws of composition.

Suppose that a law of composition on a set S, written multiplicatively, is associative and has an identity 1. An element a of S is *invertible* if there is another element b such that

$$ab = 1 \quad \text{and} \quad ba = 1,$$

and if so, then b is called the *inverse* of a. The inverse of an element is usually denoted by a^{-1}, or when additive notation is being used, by $-a$.

We list without proof some elementary properties of inverses. All but the last have already been discussed for matrices. For an example that illustrates the last statement, see Exercise 1.3.

- If an element a has both a left inverse ℓ and a right inverse r, i.e., if $\ell a = 1$ and $ar = 1$, then $\ell = r$, a is invertible, r is its inverse.
- If a is invertible, its inverse is unique.
- Inverses multiply in the opposite order: If a and b are invertible, so is the product ab, and $(ab)^{-1} = b^{-1}a^{-1}$.
- An element a may have a left inverse or a right inverse, though it is not invertible.

Power notation may be used for an associative law: With $n > 0$, $a^n = a \cdots a$ (n factors), $a^{-n} = a^{-1} \cdots a^{-1}$, and $a^0 = 1$. The usual rules for manipulation of powers hold: $a^r a^s = a^{r+s}$ and $(a^r)^s = a^{rs}$. When additive notation is used for the law of composition, the power notation a^n is replaced by the notation $na = a + \cdots + a$.

Fraction notation $\frac{b}{a}$ is not advisable unless the law of composition is commutative, because it isn't clear from the notation whether the fraction stands for ba^{-1} or for $a^{-1}b$, and these two elements may be different.

2.2 GROUPS AND SUBGROUPS

A *group* is a set G together with a law of composition that has the following properties:

- The law of composition is associative: $(ab)c = a(bc)$ for all a, b, c in G.
- G contains an identity element 1, such that $1a = a$ and $a1 = a$ for all a in G.
- Every element a of G has an inverse, an element b such that $ab = 1$ and $ba = 1$.

An *abelian group* is a group whose law of composition is commutative.

For example, the set of nonzero real numbers forms an abelian group under multiplication, and the set of all real numbers forms an abelian group under addition. The set of invertible $n \times n$ matrices, the general linear group, is a very important group in which the law of composition is matrix multiplication. It is not abelian unless $n = 1$.

When the law of composition is evident, it is customary to denote a group and the set of its elements by the same symbol.

The *order* of a group G is the number of elements that it contains. We will often denote the order by $|G|$:

(2.2.1) $$|G| = \text{number of elements, the order of } G.$$

If the order is finite, G is said to be a *finite group*. If not, G is an *infinite group*. The same terminology is used for any set. The order $|S|$ of a set S is the number of its elements.

Here is our notation for some familiar infinite abelian groups:

(2.2.2)

$\mathbb{Z}^+$:	the set of integers, with addition as its law of composition – the additive group of integers,
$\mathbb{R}^+$:	the set of real numbers, with addition as its law of composition – the additive group of real numbers;
$\mathbb{R}^\times$:	the set of nonzero real numbers, with multiplication as its law of composition – the multiplicative group,
$\mathbb{C}^+$, $\mathbb{C}^\times$:	the analogous groups, where the set $\mathbb{C}$ of complex numbers replaces the set $\mathbb{R}$ of real numbers.

Warning: Others might use the symbol $\mathbb{R}^+$ to denote the set of *positive* real numbers. To be unambiguous, it might be better to denote the additive group of reals by $(\mathbb{R}, +)$, thus displaying its law of composition explicitly. However, our notation is more compact. Also, the symbol $\mathbb{R}^\times$ denotes the multiplicative group of *nonzero* real numbers. The set of all real numbers is not a group under multiplication because 0 isn't invertible. □

Proposition 2.2.3 Cancellation Law. Let a, b, c be elements of a group G whose law of composition is written multiplicatively. If $ab = ac$ or if $ba = ca$, then $b = c$. If $ab = a$ or if $ba = a$, then $b = 1$.

Proof. Multiply both sides of $ab = ac$ on the left by a^{-1} to obtain $b = c$. The other proofs are analogous. □

Multiplication by a^{-1} is essential for this proof. The Cancellation Law needn't hold when the element a is not invertible. For instance,

$$\begin{bmatrix} 1 & 1 \\ & \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 2 & \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ & \end{bmatrix}\begin{bmatrix} 3 & \\ & 1 \end{bmatrix}.$$

Two basic examples of groups are obtained from laws of composition that we have considered – multiplication of matrices and composition of functions – by leaving out the elements that are not invertible.

- The $n \times n$ *general linear group* is the group of all invertible $n \times n$ matrices. It is denoted by

(2.2.4) $$GL_n = \{n \times n \text{ invertible matrices } A\}.$$

If we want to indicate that we are working with real or with complex matrices, we write $GL_n(\mathbb{R})$ or $GL_n(\mathbb{C})$, according to the case.

Let M be the set of maps from a set T to itself. A map $f: T \to T$ has an inverse function if and only if it is bijective, in which case we say f is a *permutation* of T. The permutations of T form a group, the law being composition of maps. As in section 1.5, we use multiplicative notation for the composition of permutations, writing qp for $q \circ p$.

- The group of permutations of the set of indices $\{\mathbf{1}, \mathbf{2}, \ldots, \mathbf{n}\}$ is called the *symmetric group*, and is denoted by S_n:

(2.2.5) S_n is the group of permutations of the indices $\mathbf{1}, \mathbf{2}, \ldots, \mathbf{n}$.

There are $n!$ ('n factorial' $= 1 \cdot 2 \cdot 3 \cdots n$) permutations of a set of n elements, so the symmetric group S_n is a finite group of order $n!$.

The permutations of a set $\{a, b\}$ of two elements are the identity i and the transposition τ (see 2.1.3). They form a group of order two. If we replace a by **1** and b by **2**, we see that this is the same group as the symmetric group S_2. There is essentially only one group G of order two. To see this, we note that one of its elements must be the identity 1; let the other element be g. The multiplication table for the group contains the four products 11, $1g$, $g1$, and gg. All except gg are determined by the fact that 1 is the identity element. Moreover, the Cancellation Law shows that $gg \neq g$. The only possibility is $gg = 1$. So the multiplication table is completely determined. There is just one group law.

We describe the symmetric group S_3 next. This group, which has order six, serves as a convenient example because it is the smallest group whose law of composition isn't commutative. We will refer to it often. To describe it, we pick two particular permutations in terms of which we can write all others. We take the cyclic permutation (**123**), and the transposition (**12**), and label them as x and y, respectively. The rules

$$x^3 = 1, \quad y^2 = 1, \quad yx = x^2y \tag{2.2.6}$$

are easy to verify. Using the cancellation law, one sees that the six elements $1, x, x^2, y, xy, x^2y$ are distinct. So they are the six elements of the group:

$$S_3 = \{1, x, x^2; y, xy, x^2y\}. \tag{2.2.7}$$

In the future, we will refer to (2.2.6) and (2.2.7) as our "usual presentation" of the symmetric group S_3. Note that S_3 is not a commutative group, because $yx \neq xy$.

The rules (2.2.6) suffice for computation. Any product of the elements x and y and of their inverses can be shown to be equal to one of the products (2.2.7) by applying the rules repeatedly. To do so, we move all occurrences of y to the right side using the last rule, and we use the first two rules to keep the exponents small. For instance,

$$x^{-1}y^3x^2y = x^2yx^2y = x^2(yx)xy = x^2(x^2y)xy = xyxy = x(x^2y)y = 1. \tag{2.2.8}$$

One can write out a multiplication table for S_3 with the aid of the rules (2.2.6), and because of this, those rules are called *defining relations* for the group. We study defining relations in Chapter 7.

We stop here. The structure of S_n becomes complicated very rapidly as n increases.

One reason that the general linear groups and the symmetric groups are important is that many other groups are contained in them as subgroups. A subset H of a group G is a *subgroup* if it has the following properties:

(2.2.9)

- *Closure*: If a and b are in H, then ab is in H.
- *Identity*: 1 is in H.
- *Inverses*: If a is in H, then a^{-1} is in H.

These conditions are explained as follows: The first one tells us that the law of composition on the group G defines a law of composition on H, called the *induced law*. The second and third conditions say that H is a group with respect to this induced law. Notice that (2.2.9)

mentions all parts of the definition of a group except for the associative law. We don't need to mention associativity. It carries over automatically from G to the subset H.

Notes: (i) In mathematics, it is essential to learn the definition of each term. An intuitive feeling will not suffice. For example, the set T of invertible real (upper) triangular 2×2 matrices is a subgroup of the general linear group GL_2, and there is only one way to verify this, namely to go back to the definition. It is true that T is a subset of GL_2. One must verify that the product of invertible triangular matrices is triangular, that the identity is triangular, and that the inverse of an invertible triangular matrix is triangular. Of course these points are very easy to check.

(ii) Closure is sometimes mentioned as one of the axioms for a group, to indicate that the product ab of elements of G is again an element of G. We include closure as a part of what is meant by a law of composition. Then it doesn't need to be mentioned separately in the definition of a group. □

Examples 2.2.10

(a) The set of complex numbers of absolute value 1, the set of points on the unit circle in the complex plane, is a subgroup of the multiplicative group $\mathbb{C}^\times$ called the *circle group*.

(b) The group of real $n \times n$ matrices with determinant 1 is a subgroup of the general linear group GL_n, called the *special linear group*. It is denoted by SL_n:

(2.2.11) $SL_n(\mathbb{R})$ is the set of real $n \times n$ matrices A with determinant equal to 1.

The defining properties (2.2.9) are often very easy to verify for a particular subgroup, and we may not carry the verification out.

• Every group G has two obvious subgroups: the group G itself, and the *trivial subgroup* that consists of the identity element alone. A subgroup is a *proper subgroup* if it is not one of those two.

2.3 SUBGROUPS OF THE ADDITIVE GROUP OF INTEGERS

We review some elementary number theory here, in terms of subgroups of the additive group $\mathbb{Z}^+$ of integers. To begin, we list the axioms for a subgroup when additive notation is used in the group: A subset S of a group G with law of composition written additively is a subgroup if it has these properties:

(2.3.1)

- *Closure*: If a and b are in S, then $a + b$ is in S.
- *Identity*: 0 is in S.
- *Inverses*: If a is in S then $-a$ is in S.

Let a be an integer different from 0. We denote the subset of $\mathbb{Z}$ that consists of all multiples of a by $\mathbb{Z}a$:

(2.3.2) $$\mathbb{Z}a = \{n \in \mathbb{Z} \mid n = ka \text{ for some } k \text{ in } \mathbb{Z}\}.$$

This is a subgroup of $\mathbb{Z}^+$. Its elements can also be described as the integers divisible by a.

Theorem 2.3.3 Let S be a subgroup of the additive group $\mathbb{Z}^+$. Either S is the trivial subgroup $\{0\}$, or else it has the form $\mathbb{Z}a$, where a is the smallest positive integer in S.

Proof. Let S be a subgroup of $\mathbb{Z}^+$. Then 0 is in S, and if 0 is the only element of S then S is the trivial subgroup. So that case is settled. Otherwise, S contains an integer n different from 0, and either n or $-n$ is positive. The third property of a subgroup tells us that $-n$ is in S, so in either case, S contains a positive integer. We must show that S is equal to $\mathbb{Z}a$, when a is the smallest positive integer in S.

We first show that $\mathbb{Z}a$ is a subset of S, in other words, that ka is in S for every integer k. If k is a positive integer, then $ka = a + a + \cdots + a$ (k terms). Since a is in S, closure and induction show that ka is in S. Since inverses are in S, $-ka$ is in S. Finally, $0 = 0a$ is in S.

Next we show that S is a subset of $\mathbb{Z}a$, that is, every element n of S is an integer multiple of a. We use division with remainder to write $n = qa + r$, where q and r are integers and where the remainder r is in the range $0 \leq r < a$. Since $\mathbb{Z}a$ is contained in S, qa is in S, and of course n is in S. Since S is a subgroup, $r = n - qa$ is in S too. Now by our choice, a is the smallest positive integer in S, while the remainder r is in the range $0 \leq r < a$. The only remainder that can be in S is 0. So $r = 0$ and n is the integer multiple qa of a. □

There is a striking application of Theorem 2.3.3 to subgroups that contain *two* integers a and b. The set of all integer combinations $ra + sb$ of a and b,

$$S = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} \mid n = ra + sb \text{ for some integers } r, s\} \tag{2.3.4}$$

is a subgroup of $\mathbb{Z}^+$. It is called the subgroup *generated by* a and b because it is the smallest subgroup that contains both a and b. Let's assume that a and b aren't both zero, so that S is not the trivial subgroup $\{0\}$. Theorem 2.3.3 tells us that this subgroup S has the form $\mathbb{Z}d$ for some positive integer d; it is the set of integers divisible by d. The generator d is called the *greatest common divisor* of a and b, for reasons that are explained in parts **(a)** and **(b)** of the next proposition. The greatest common divisor of a and b is sometimes denoted by $\gcd(a, b)$.

Proposition 2.3.5 Let a and b be integers, not both zero, and let d be their greatest common divisor, the positive integer that generates the subgroup $S = \mathbb{Z}a + \mathbb{Z}b$. So $\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$. Then

(a) d divides a and b.

(b) If an integer e divides both a and b, it also divides d.

(c) There are integers r and s such that $d = ra + sb$.

Proof. Part **(c)** restates the fact that d is an element of S. Next, a and b are elements of S and $S = \mathbb{Z}d$, so d divides a and b. Finally, if an integer e divides both a and b, then e divides the integer combination $ra + sb = d$. □

Note: If e divides a and b, then e divides any integer of the form $ma + nb$. So **(c)** implies **(b)**. But **(b)** does not imply **(c)**. As we shall see, property **(c)** is a powerful tool. □

One can compute a greatest common divisor easily by repeated division with remainder: For example, if $a = 314$ and $b = 136$, then

$$314 = 2 \cdot 136 + 42\,, \quad 136 = 3 \cdot 42 + 10\,, \quad 42 = 4 \cdot 10 + 2.$$

Using the first of these equations, one can show that any integer combination of 314 and 136 can also be written as an integer combination of 136 and the remainder 42, and vice versa. So $\mathbb{Z}(314) + \mathbb{Z}(136) = \mathbb{Z}(136) + \mathbb{Z}(42)$, and therefore $\gcd(314, 136) = \gcd(136, 42)$. Similarly, $\gcd(136, 42) = \gcd(42, 10) = \gcd(10, 2) = 2$. So the greatest common divisor of 314 and 136 is 2. This iterative method of finding the greatest common divisor of two integers is called the *Euclidean Algorithm*.

If integers a and b are given, a second way to find their greatest common divisor is to factor each of them into prime integers and then to collect the common prime factors. Properties **(a)** and **(b)** of Proposition 2.3.5 are easy to verify using this method. But without Theorem 2.3.3, property **(c)**, that the integer determined by this method is an integer combination of a and b wouldn't be clear at all. Let's not discuss this point further here. We come back to it in Chapter 12.

Two nonzero integers a and b are said to be *relatively prime* if the only positive integer that divides both of them is 1. Then their greatest common divisor is 1: $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}$.

Corollary 2.3.6 A pair a, b of integers is relatively prime if and only if there are integers r and s such that $ra + sb = 1$. □

Corollary 2.3.7 Let p be a prime integer. If p divides a product ab of integers, then p divides a or p divides b.

Proof. Suppose that the prime p divides ab but does not divide a. The only positive divisors of p are 1 and p. Since p does not divide a, $\gcd(a, p) = 1$. Therefore there are integers r and s such that $ra + sp = 1$. We multiply by b: $rab + spb = b$, and we note that p divides both rab and spb. So p divides b. □

There is another subgroup of $\mathbb{Z}^+$ associated to a pair a, b of integers, namely the intersection $\mathbb{Z}a \cap \mathbb{Z}b$, the set of integers contained both in $\mathbb{Z}a$ and in $\mathbb{Z}b$. We assume now that neither a nor b is zero. Then $\mathbb{Z}a \cap \mathbb{Z}b$ is a subgroup. It is not the trivial subgroup $\{0\}$ because it contains the product ab, which isn't zero. So $\mathbb{Z}a \cap \mathbb{Z}b$ has the form $\mathbb{Z}m$ for some positive integer m. This integer m is called the *least common multiple* of a and b, sometimes denoted by $\text{lcm}(a, b)$, for reasons that are explained in the next proposition.

Proposition 2.3.8 Let a and b be integers different from zero, and let m be their least common multiple – the positive integer that generates the subgroup $S = \mathbb{Z}a \cap \mathbb{Z}b$. So $\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$. Then

(a) m is divisible by both a and b.

(b) If an integer n is divisible by a and by b, then it is divisible by m.

Proof. Both statements follow from the fact that an integer is divisible by a and by b if and only if it is contained in $\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$. □

Corollary 2.3.9 Let $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$ be the greatest common divisor and least common multiple of a pair a, b of positive integers, respectively. Then $ab = dm$.

Proof. Since b/d is an integer, a divides ab/d. Similarly, b divides ab/d. So m divides ab/d, and dm divides ab. Next, we write $d = ra + sb$. Then $dm = ram + sbm$. Both terms

on the right are divisible by ab, so ab divides dm. Since ab and dm are positive and each one divides the other, $ab = dm$. □

2.4 CYCLIC GROUPS

We come now to an important abstract example of a subgroup, the *cyclic subgroup* generated by an arbitrary element x of a group G. We use multiplicative notation. The cyclic subgroup H generated by x is the set of all elements that are powers of x:

$$H = \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, \ldots\}. \tag{2.4.1}$$

This is the smallest subgroup of G that contains x, and it is often denoted by $\langle x \rangle$. But to interpret (2.4.1) correctly, we must remember that the notation x^n represents an element of the group that is obtained in a particular way. Different powers may represent the same element. For example, if G is the multiplicative group $\mathbb{R}^\times$ and $x = -1$, then all elements in the list are equal to 1 or to -1, and H is the set $\{1, -1\}$.

There are two possibilities: Either the powers x^n represent distinct elements, or they do not. We analyze the case that the powers of x are not distinct.

Proposition 2.4.2 Let $\langle x \rangle$ be the cyclic subgroup of a group G generated by an element x, and let S denote the set of integers k such that $x^k = 1$.

(a) The set S is a subgroup of the additive group $\mathbb{Z}^+$.

(b) Two powers $x^r = x^s$, with $r \geq s$, are equal if and only if $x^{r-s} = 1$, i.e., if and only if $r - s$ is in S.

(c) Suppose that S is not the trivial subgroup. Then $S = \mathbb{Z}n$ for some positive integer n. The powers $1, x, x^2, \ldots, x^{n-1}$ are the distinct elements of the subgroup $\langle x \rangle$, and the order of $\langle x \rangle$ is n.

Proof. **(a)** If $x^k = 1$ and $x^\ell = 1$, then $x^{k+\ell} = x^k x^\ell = 1$. This shows that if k and ℓ are in S, then $k + \ell$ is in S. So the first property (2.3.1) for a subgroup is verified. Also, $x^0 = 1$, so 0 is in S. Finally, if k is in S, i.e., $x^k = 1$, then $x^{-k} = (x^k)^{-1} = 1$ too, so $-k$ is in S.

(b) This follows from the Cancellation Law 2.2.3.

(c) Suppose that $S \neq \{0\}$. Theorem 2.3.3 shows that $S = \mathbb{Z}n$, where n is the smallest positive integer in S. If x^k is an arbitrary power, we divide k by n, writing $k = qn + r$ with r in the range $0 \leq r < n$. Then $x^{qn} = 1^q = 1$, and $x^k = x^{qn}x^r = x^r$. Therefore x^k is equal to one of the powers $1, x, \ldots, x^{n-1}$. It follows from **(b)** that these powers are distinct, because x^n is the smallest positive power equal to 1. □

The group $\langle x \rangle = \{1, x, \ldots, x^{n-1}\}$ described by part **(c)** of this proposition is called a *cyclic group of order n*. It is called cyclic because repeated multiplication by x cycles through the n elements.

An element x of a group has *order n* if n is the smallest positive integer with the property $x^n = 1$, which is the same thing as saying that the cyclic subgroup $\langle x \rangle$ generated by x has order n.

With the usual presentation of the symmetric group S_3, the element x has order 3, and y has order 2. In any group, the identity element is the only element of order 1.

If $x^n \neq 1$ for all $n > 0$, one says that x has *infinite order*. The matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order in $GL_2(\mathbb{R})$, while $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ has order 6.

When x has infinite order, the group $\langle x \rangle$ is said to be *infinite cyclic*. We won't have much to say about that case.

Proposition 2.4.3 Let x be an element of finite order n in a group, and let k be an integer that is written as $k = nq + r$ where q and r are integers and r is in the range $0 \leq r < n$.

- $x^k = x^r$.
- $x^k = 1$ if and only if $r = 0$.
- Let d be the greatest common divisor of k and n. The order of x^k is equal to n/d. □

One may also speak of the subgroup of a group G generated by a subset U. This is the smallest subgroup of G that contains U, and it consists of all elements of G that can be expressed as a product of a string of elements of U and of their inverses. A subset U of G is said to *generate* G if every element of G is such a product. For example, we saw in (2.2.7) that the set $U = \{x, y\}$ generates the symmetric group S_3. The elementary matrices generate GL_n (1.2.16). In both of these examples, inverses aren't needed. That isn't always true. An infinite cyclic group $\langle x \rangle$ is generated by the element x, but negative powers are needed to fill out the group.

The *Klein four group* V, the group consisting of the four matrices

$$\begin{bmatrix} \pm 1 & \\ & \pm 1 \end{bmatrix}, \tag{2.4.4}$$

is the simplest group that is not cyclic. Any two of its elements different from the identity generate V. The *quaternion group* H is another example of a small group. It consists of the eight matrices

$$H = \{\pm \mathbf{1}, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}, \tag{2.4.5}$$

where

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

These matrices can be obtained from the *Pauli matrices* of physics by multiplying by i. The two elements $\mathbf{i}$ and $\mathbf{j}$ generate H. Computation leads to the formulas

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}, \ \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \ \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}. \tag{2.4.6}$$

2.5 HOMOMORPHISMS

Let G and G' be groups, written with multiplicative notation. A *homomorphism* $\varphi: G \to G'$ is a map from G to G' such that for all a and b in G,

$$\varphi(ab) = \varphi(a)\varphi(b). \tag{2.5.1}$$

The left side of this equation means

first multiply a and b in G, then send the product to G' using the map φ,

while the right side means

first send a and b individually to G' using the map φ, then multiply their images in G'.

Intuitively, a homomorphism is a map that is compatible with the laws of composition in the two groups, and it provides a way to relate different groups.

Examples 2.5.2 The following maps are homomorphisms:

(a) the determinant function $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$ (1.4.10),
(b) the sign homomorphism $\sigma: S_n \to \{\pm 1\}$ that sends a permutation to its sign (1.5.11),
(c) the exponential map $\exp: \mathbb{R}^+ \to \mathbb{R}^\times$ defined by $x \rightsquigarrow e^x$,
(d) the map $\varphi: \mathbb{Z}^+ \to G$ defined by $\varphi(n) = a^n$, where a is a given element of G,
(e) the absolute value map $|\ |: \mathbb{C}^\times \to \mathbb{R}^\times$.

In examples **(c)** and **(d)**, the law of composition is written additively in the domain and multiplicatively in the range. The condition (2.5.1) for a homomorphism must be rewritten to take this into account. It becomes

$$\varphi(a + b) = \varphi(a)\varphi(b).$$

The formula showing that the exponential map is a homomorphism is $e^{a+b} = e^a e^b$.

The following homomorphisms need to be mentioned, though they are less interesting. The *trivial homomorphism* $\varphi: G \to G'$ between any two groups maps every element of G to the identity in G'. If H is a subgroup of G, the *inclusion map* $i: H \to G$ defined by $i(x) = x$ for x in H is a homomorphism.

Proposition 2.5.3 Let $\varphi: G \to G'$ be a group homomorphism.

(a) If $a_1, \ldots, a_k$ are elements of G, then $\varphi(a_1 \cdots a_k) = \varphi(a_1) \cdots \varphi(a_k)$.
(b) φ maps the identity to the identity: $\varphi(1_G) = 1_{G'}$.
(c) φ maps inverses to inverses: $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof. The first assertion follows by induction from the definition. Next, since $1 \cdot 1 = 1$ and since φ is a homomorphism, $\varphi(1)\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)$. We cancel $\varphi(1)$ from both sides (2.2.3) to obtain $\varphi(1) = 1$. Finally, $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1) = 1$. Hence $\varphi(a^{-1})$ is the inverse of $\varphi(a)$. □

A group homomorphism determines two important subgroups: its image and its kernel.

• The *image* of a homomorphism $\varphi: G \to G'$, often denoted by $\operatorname{im}\varphi$, is simply the image of φ as a map of sets:

$$\operatorname{im}\varphi = \{x \in G' \mid x = \varphi(a) \text{ for some } a \text{ in } G\}, \tag{2.5.4}$$

Another notation for the image would be $\varphi(G)$.

The image of the map $\mathbb{Z}^+ \to G$ that sends $n \rightsquigarrow a^n$ is the cyclic subgroup $\langle a \rangle$ generated by a.

The image of a homomorphism is a subgroup of the range. We will verify closure and omit the other verifications. Let x and y be elements of the image. This means that there are elements a and b in G such that $x = \varphi(a)$ and $y = \varphi(b)$. Since φ is a homomorphism, $xy = \varphi(a)\varphi(b) = \varphi(ab)$. So xy is equal to $\varphi(something)$. It is in the image too.

• The *kernel* of a homomorphism is more subtle and also more important. The kernel of φ, often denoted by $\ker \varphi$, is the set of elements of G that are mapped to the identity in G':

$$\ker \varphi = \{a \in G \mid \varphi(a) = 1\}. \tag{2.5.5}$$

The kernel is a subgroup of G because, if a and b are in the kernel, then $\varphi(ab) = \varphi(a)\varphi(b) = 1 \cdot 1 = 1$, so ab is in the kernel, and so on.

The kernel of the determinant homomorphism $GL_n(\mathbb{R}) \to \mathbb{R}^\times$ is the special linear group $SL_n(\mathbb{R})$ (2.2.11). The kernel of the sign homomorphism $S_n \to \{\pm 1\}$ is called the *alternating group*. It consists of the even permutations, and is denoted by A_n:

(2.5.6) The alternating group A_n is the group of even permutations.

The kernel is important because it controls the entire homomorphism. It tells us not only which elements of G are mapped to the identity in G', but also which pairs of elements have the same image in G'.

• If H is a subgroup of a group G and a is an element of G, the notation aH will stand for the set of all products ah with h in H:

$$aH = \{g \in G \mid g = ah \text{ for some } h \text{ in } H\}. \tag{2.5.7}$$

This set is called a *left coset* of H in G, the word "left" referring to the fact that the element a appears on the left.

Proposition 2.5.8 Let $\varphi: G \to G'$ be a homomorphism of groups, and let a and b be elements of G. Let K be the kernel of φ. The following conditions are equivalent:

- $\varphi(a) = \varphi(b)$,
- $a^{-1}b$ is in K,
- b is in the coset aK,
- The cosets bK and aK are equal.

Proof. Suppose that $\varphi(a) = \varphi(b)$. Then $\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b) = 1$. Therefore $a^{-1}b$ is in the kernel K. To prove the converse, we turn this argument around. If $a^{-1}b$ is in K, then $1 = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b)$, so $\varphi(a) = \varphi(b)$. This shows that the first two bullets are equivalent. Their equivalence with the other bullets follows. □

Corollary 2.5.9 A homomorphism $\varphi: G \to G'$ is injective if and only if its kernel K is the trivial subgroup $\{1\}$ of G.

Proof. If $K = \{1\}$, Proposition 2.5.8 shows that $\varphi(a) = \varphi(b)$ only when $a^{-1}b = 1$, i.e., $a = b$. Conversely, if φ is injective, then the identity is the only element of G such that $\varphi(a) = 1$, so $K = \{1\}$. □

The kernel of a homomorphism has another important property that is explained in the next proposition. If a and g are elements of a group G, the element gag^{-1} is called the *conjugate* of a by g.

Definition 2.5.10 A subgroup N of a group G is a *normal subgroup* if for every a in N and every g in G, the conjugate gag^{-1} is in N.

Proposition 2.5.11 The kernel of a homomorphism is a normal subgroup.

Proof. If a is in the kernel of a homomorphism $\varphi: G \to G'$ and if g is any element of G, then $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(g)1\varphi(g)^{-1} = 1$. Therefore gag^{-1} is in the kernel too. □

Thus the special linear group $SL_n(\mathbb{R})$ is a normal subgroup of the general linear group $GL_n(\mathbb{R})$, and the alternating group A_n is a normal subgroup of the symmetric group S_n. Every subgroup of an abelian group is normal, because if G is abelian, then $gag^{-1} = a$ for all a and all g in the group. But subgroups of nonabelian groups needn't be normal. For example, in the symmetric group S_3, with its usual presentation (2.2.7), the cyclic subgroup $\langle y \rangle$ of order two is not normal, because y is in G, but $xyx^{-1} = x^2y$ isn't in $\langle y \rangle$.

- The *center* of a group G, which is often denoted by Z, is the set of elements that commute with every element of G:

$$Z = \{z \in G \mid zx = xz \text{ for all } x \in G\}. \tag{2.5.12}$$

It is always a normal subgroup of G. The center of the special linear group $SL_2(\mathbb{R})$ consists of the two matrices $I, -I$. The center of the symmetric group S_n is trivial if $n \geq 3$.

Example 2.5.13 A homomorphism $\varphi: S_4 \to S_3$ between symmetric groups.

There are three ways to partition the set of four indices $\{1, 2, 3, 4\}$ into pairs of subsets of order two, namely

$$\Pi_1 : \{1, 2\} \cup \{3, 4\}, \quad \Pi_2 : \{1, 3\} \cup \{2, 4\}, \quad \Pi_3 : \{1, 4\} \cup \{2, 3\}. \tag{2.5.14}$$

An element of the symmetric group S_4 permutes the four indices, and by doing so it also permutes these three partitions. This defines the map φ from S_4 to the group of permutations of the set $\{\Pi_1, \Pi_2, \Pi_3\}$, which is the symmetric group S_3. For example, the 4-cycle $p = (1234)$ acts on subsets of order two as follows:

$$\begin{array}{lll} \{1, 2\} \rightsquigarrow \{2, 3\} & \{1, 3\} \rightsquigarrow \{2, 4\} & \{1, 4\} \rightsquigarrow \{1, 2\} \\ \{2, 3\} \rightsquigarrow \{3, 4\} & \{2, 4\} \rightsquigarrow \{1, 3\} & \{3, 4\} \rightsquigarrow \{1, 4\}. \end{array}$$

Looking at this action, one sees that p acts on the set $\{\Pi_1, \Pi_2, \Pi_3\}$ of partitions as the transposition $(\Pi_1 \Pi_3)$ that fixes Π_2 and interchanges Π_1 and Π_3.

If p and q are elements of S_4, the product pq is the composed permutation $p \circ q$, and the action of pq on the set $\{\Pi_1, \Pi_2, \Pi_3\}$ is the composition of the actions of q and p. Therefore $\varphi(pq) = \varphi(p)\varphi(q)$, and φ is a homomorphism.

The map is surjective, so its image is the whole group S_3. Its kernel can be computed. It is the subgroup of S_4 consisting of the identity and the three products of disjoint transpositions:

$$K = \{1,\ (12)(34),\ (13)(24),\ (14)(23)\}. \tag{2.5.15}$$

□

2.6 ISOMORPHISMS

An *isomorphism* $\varphi: G \to G'$ from a group G to a group G' is a bijective group homomorphism – a bijective map such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all a and b in G.

Examples 2.6.1

- The exponential map e^x is an isomorphism, when it is viewed as a map from the additive group $\mathbb{R}^+$ to its image, the multiplicative group of positive real numbers.
- If a is an element of infinite order in a group G, the map sending $n \rightsquigarrow a^n$ is an isomorphism from the additive group $\mathbb{Z}^+$ to the infinite cyclic subgroup $\langle a \rangle$ of G.
- The set $\mathcal{P}$ of $n \times n$ permutation matrices is a subgroup of GL_n, and the map $S_n \to \mathcal{P}$ that sends a permutation to its associated matrix (1.5.7) is an isomorphism. □

Corollary 2.5.9 gives us a way to verify that a homomorphism $\varphi: G \to G'$ is an isomorphism. To do so, we check that $\ker \varphi = \{1\}$, which implies that φ is injective, and also that $\operatorname{im} \varphi = G'$, that is, φ is surjective.

Lemma 2.6.2 If $\varphi: G \to G'$ is an isomorphism, the inverse map $\varphi^{-1}: G' \to G$ is also an isomorphism.

Proof. The inverse of a bijective map is bijective. We must show that for all x and y in G', $\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$. We set $a = \varphi^{-1}(x)$, $b = \varphi^{-1}(y)$, and $c = \varphi^{-1}(xy)$. What has to be shown is that $ab = c$, and since φ is bijective, it suffices to show that $\varphi(ab) = \varphi(c)$. Since φ is a homomorphism,

$$\varphi(ab) = \varphi(a)\varphi(b) = xy = \varphi(c).$$

□

This lemma shows that when $\varphi: G \to G'$ is an isomorphism, we can make a computation in either group, then use φ or φ^{-1} to carry it over to the other. So, for computation with the group law, the two groups have identical properties. To picture this conclusion intuitively, suppose that the elements of one of the groups are put into unlabeled boxes, and that we have an oracle that tells us, when presented with two boxes, which box contains their product. We will have no way to decide whether the elements in the boxes are from G or from G'.

Two groups G and G' are said to be *isomorphic* if there exists an isomorphism φ from G to G'. We sometimes indicate that two groups are isomorphic by the symbol $\approx$

$$G \approx G' \text{ means that } G \text{ is isomorphic to } G'. \tag{2.6.3}$$

Since isomorphic groups have identical properties, it is often convenient to identify them with each other when speaking informally. For instance, we often blur the distinction between the symmetric group S_n and the isomorphic group $\mathcal{P}$ of permutation matrices.

- The groups isomorphic to a given group G form what is called the *isomorphism class* of G.

Any two groups in an isomorphism class are isomorphic. When one speaks of *classifying groups*, what is meant is to describe these isomorphism classes. This is too hard to do for all groups, but we will see that every group of prime order p is cyclic. So all groups of order p are isomorphic. There are two isomorphism classes of groups of order 4 (2.11.5) and five isomorphism classes of groups of order 12 (7.8.1).

An interesting and sometimes confusing point about isomorphisms is that there exist isomorphisms $\varphi : G \to G$ from a group G to itself. Such an isomorphism is called an *automorphism*. The identity map is an automorphism, of course, but there are nearly always others. The most important type of automorphism is conjugation: Let g be a fixed element of a group G. *Conjugation by* g is the map φ from G to itself defined by

$$\varphi(x) = gxg^{-1}. \tag{2.6.4}$$

This is an automorphism because, first of all, it is a homomorphism:

$$\varphi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi(x)\varphi(y),$$

and second, it is bijective because it has an inverse function – conjugation by g^{-1}.

If the group is abelian, conjugation by any element g is the identity map: $gxg^{-1} = x$. But any noncommutative group has nontrivial conjugations, and so it has automorphisms different from the identity. For instance, in the symmetric group S_3, presented as usual, conjugation by y interchanges x and x^2.

As was said before, the element gxg^{-1} is the *conjugate* of x by g, and two elements x and x' of a group G are *conjugate* if $x' = gxg^{-1}$ for some g in G. The conjugate gxg^{-1} behaves in much the same way as the element x itself; for example, it has the same order in the group. This follows from the fact that it is the image of x by an automorphism. (See the discussion following Lemma 2.6.2.)

Note: One may sometimes wish to determine whether or not two elements x and y of a group G are conjugate, i.e., whether or not there is an element g in G such that $y = gxg^{-1}$. It is almost always simpler to rewrite the equation to be solved for g as $yg = gx$. □

- The *commutator* $aba^{-1}b^{-1}$ is another element associated to a pair a, b of elements of a group.

The next lemma follows by moving things from one side of an equation to the other.

Lemma 2.6.5 Two elements a and b of a group commute, $ab = ba$, if and only if $aba^{-1} = b$, and this is true if and only if $aba^{-1}b^{-1} = 1$. □

2.7 EQUIVALENCE RELATIONS AND PARTITIONS

A fundamental mathematical construction starts with a set S and forms a new set by equating certain elements of S. For instance, we may divide the set of integers into two classes, the

even integers and the odd integers. The new set we obtain consists of two elements that could be called *Even* and *Odd*. Or, it is common to view congruent triangles in the plane as equivalent geometric objects. This very general procedure arises in several ways that we discuss here.

- A *partition* Π of a set S is a subdivision of S into nonoverlapping, nonempty subsets:

(2.7.1) $S =$ union of disjoint nonempty subsets.

The two sets *Even* and *Odd* partition the set of integers. With the usual notation, the sets

(2.7.2) $$\{1\}, \{y, xy, x^2y\}, \{x, x^2\}$$

form a partition of the symmetric group S_3.

- An *equivalence relation* on a set S is a relation that holds between certain pairs of elements of S. We may write it as $a \sim b$ and speak of it as *equivalence* of a and b. An equivalence relation is required to be:

(2.7.3)

- *transitive*: If $a \sim b$ and $b \sim c$, then $a \sim c$.
- *symmetric*: If $a \sim b$, then $b \sim a$.
- *reflexive*: For all a, $a \sim a$.

Congruence of triangles is an example of an equivalence relation on the set of triangles in the plane. If A, B, and C are triangles, and if A is congruent to B and B is congruent to C, then A is congruent to C, etc.

Conjugacy is an equivalence relation on a group. Two group elements are conjugate, $a \sim b$, if $b = gag^{-1}$ for some group element g. We check transitivity: Suppose that $a \sim b$ and $b \sim c$. This means that $b = g_1 a g_1^{-1}$ and $c = g_2 b g_2^{-1}$ for some group elements g_1 and g_2. Then $c = g_2(g_1 a g_1^{-1})g_2^{-1} = (g_2 g_1)a(g_2 g_1)^{-1}$, so $a \sim c$.

The concepts of a partition of S and an equivalence relation on S are logically equivalent, though in practice one may be presented with just one of the two.

Proposition 2.7.4 An equivalence relation on a set S determines a partition of S, and conversely.

Proof. Given a partition of S, the corresponding equivalence relation is defined by the rule that $a \sim b$ if a and b lie in the same subset of the partition. The axioms for an equivalence relation are obviously satisfied. Conversely, given an equivalence relation, one defines a partition this way: The subset that contains a is the set of all elements b such that $a \sim b$. This subset is called the *equivalence class* of a. We'll denote it by C_a here:

(2.7.5) $$C_a = \{b \in S \mid a \sim b\}.$$

The next lemma completes the proof of the proposition. ∎

Lemma 2.7.6 Given an equivalence relation on a set S, the subsets of S that are equivalence classes partition S.

Proof. This is an important point, so we will check it carefully. We must remember that the notation C_a stands for a subset defined in a certain way. The partition consists of the subsets, and several notations may describe the same subset.

The reflexive axiom tells us that a is in its equivalence class. Therefore the class C_a is nonempty, and since a can be any element, the union of the equivalence classes is the whole set S. The remaining property of a partition that must be verified is that equivalence classes are disjoint. To show this, we show:

(2.7.7) If C_a and C_b have an element in common, then $C_a = C_b$.

Since we can interchange the roles of a and b, it will suffice to show that if C_a and C_b have an element, say d, in common, then $C_b \subset C_a$, i.e., any element x of C_b is also in C_a. If x is in C_b, then $b \sim x$. Since d is in both sets, $a \sim d$ and $b \sim d$, and the symmetry property tells us that $d \sim b$. So we have $a \sim d$, $d \sim b$, and $b \sim x$. Two applications of transitivity show that $a \sim x$, and therefore that x is in C_a. □

For example, the relation on a group defined by $a \sim b$ if a and b are elements of the same order is an equivalence relation. The corresponding partition is exhibited in (2.7.2) for the symmetric group S_3.

If a partition of a set S is given, we may construct a new set $\overline{S}$ whose elements are the subsets. We imagine putting the subsets into separate piles, and we regard the piles as the elements of our new set $\overline{S}$. It seems advisable to have a notation to distinguish a subset from the element of the set $\overline{S}$ (the pile) that it represents. If U is a subset, we will denote by $[U]$ the corresponding element of $\overline{S}$. Thus if S is the set of integers and if *Even* and *Odd* denote the subsets of even and odd integers, respectively, then $\overline{S}$ contains the two elements $[Even]$ and $[Odd]$.

We will use this notation more generally. When we want to regard a subset U of S as an element of a set of subsets of S, we denote it by $[U]$.

When an equivalence relation on S is given, the equivalence classes form a partition, and we obtain a new set $\overline{S}$ whose elements are the equivalence classes $[C_a]$. We can think of the elements of this new set in another way, as the set obtained by changing what we mean by equality among elements. If a and b are in S, we interpret $a \sim b$ to mean that a and b become equal in $\overline{S}$, because $C_a = C_b$. With this way of looking at it, the difference between the two sets S and $\overline{S}$ is that in $\overline{S}$ more elements have been declared "equal," i.e., equivalent. It seems to me that we often treat congruent triangles this way in school.

For any equivalence relation, there is a natural surjective map

(2.7.8) $$\pi : S \to \overline{S}$$

that maps an element a of S to its equivalence class: $\pi(a) = [C_a]$. When we want to regard $\overline{S}$ as the set obtained from S by changing the notion of equality, it will be convenient to denote the element $[C_a]$ of $\overline{S}$ by the symbol $\bar{a}$. Then the map π becomes

$$\pi(a) = \bar{a}$$

We can work in $\overline{S}$ with the symbols used for elements of S, but with bars over them to remind us of the new rule:

(2.7.9) If a and b are in S, then $\overline{a} = \overline{b}$ means $a \sim b$.

A disadvantage of this bar notation is that many symbols represent the same element of $\overline{S}$. Sometimes this disadvantage can be overcome by choosing a particular element, a *representative element*, in each equivalence class. For example, the even and the odd integers are often represented by $\overline{0}$ and $\overline{1}$:

(2.7.10) $$\{[Even], [Odd]\} = \{\overline{0}, \overline{1}\}.$$

Though the pile picture may be easier to grasp at first, the second way of viewing $\overline{S}$ is often better because the bar notation is easier to manipulate algebraically.

The Equivalence Relation Defined by a Map

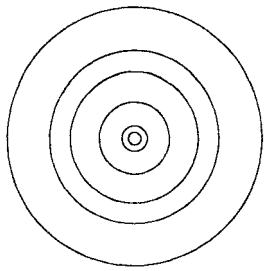
Any map of sets $f: S \to T$ gives us an equivalence relation on its domain S. It is defined by the rule $a \sim b$ if $f(a) = f(b)$.

- The *inverse image* of an element t of T is the subset of S consisting of all elements s such that $f(s) = t$. It is denoted symbolically as

(2.7.11) $$f^{-1}(t) = \{s \in S \mid f(s) = t\}.$$

This is symbolic notation. Please remember that unless f is bijective, f^{-1} will not be a map. The inverse images are also called the *fibres* of the map f, and the fibres that are not empty are the equivalence classes for the relation defined above.

Here the set $\overline{S}$ of equivalence classes has another incarnation, as the image of the map. The elements of the image correspond bijectively to the nonempty fibres, which are the equivalence classes.



(2.7.12) Some Fibres of the Absolute Value Map $\mathbb{C}^\times \to \mathbb{R}^\times$.

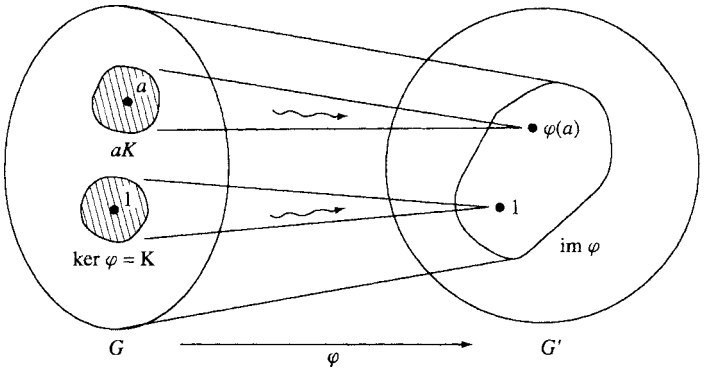
Example 2.7.13 If G is a finite group, we can define a map $f: G \to \mathbb{N}$ to the set $\{1, 2, 3, \ldots\}$ of natural numbers, letting $f(a)$ be the order of the element a of G. The fibres of this map are the sets of elements with the same order (see (2.7.2), for example). □

We go back to a group homomorphism $\varphi: G \to G'$. The equivalence relation on G defined by φ is usually denoted by $\equiv$, rather than by $\sim$, and is referred to as *congruence*:

(2.7.14) $$a \equiv b \text{ if } \varphi(a) = \varphi(b).$$

We have seen that elements a and b of G are congruent, i.e., $\varphi(a) = \varphi(b)$, if and only if b is in the coset aK of the kernel K (2.5.8).

Proposition 2.7.15 Let K be the kernel of a homomorphism $\varphi: G \to G'$. The fibre of φ that contains an element a of G is the coset aK of K. These cosets partition the group G, and they correspond to elements of the image of φ. □



(2.7.16) A Schematic Diagram of a Group Homomorphism.

2.8 COSETS

As before, if H is a subgroup of G and if a is an element of G, the subset

(2.8.1) $$aH = \{ah \mid h \text{ in } H\}.$$

is called a *left coset*. The subgroup H is a particular left coset because $H = 1H$.

The cosets of H in G are equivalence classes for the congruence relation

(2.8.2) $$a \equiv b \text{ if } b = ah \text{ for some } h \text{ in } H.$$

This is very simple, but let's verify that congruence is an equivalence relation.

Transitivity: Suppose that $a \equiv b$ and $b \equiv c$. This means that $b = ah$ and $c = bh'$ for some elements h and h' of H. Therefore $c = ahh'$. Since H is a subgroup, hh' is in H, and thus $a \equiv c$.

Symmetry: Suppose $a \equiv b$, so that $b = ah$. Then $a = bh^{-1}$ and h^{-1} is in H, so $b \equiv a$.

Reflexivity: $a = a1$ and 1 is in H, so $a \equiv a$.

Notice that we have made use of all the defining properties of a subgroup here: closure, inverses, and identity.

Corollary 2.8.3 The left cosets of a subgroup H of a group G partition the group.

Proof. The left cosets are the equivalence classes for the congruence relation (2.8.2). □

Keep in mind that the notation aH defines a certain subset of G. As with any equivalence relation, several notations may define the same subset. For example, in the symmetric group S_3, with the usual presentation (2.2.6), the element y generates a cyclic subgroup $H = \langle y \rangle$ of order 2. There are three left cosets of H in G:

$$H = \{1, y\} = yH, \quad xH = \{x, xy\} = xyH, \quad x^2H = \{x^2, x^2y\} = x^2yH. \tag{2.8.4}$$

These sets do partition the group.

Recapitulating, let H be a subgroup of a group G and let a and b be elements of G. The following are equivalent:

(2.8.5)

- $b = ah$ for some h in H, or, $a^{-1}b$ is an element of H,
- b is an element of the left coset aH,
- the left cosets aH and bH are equal.

The number of left cosets of a subgroup is called the *index* of H in G. The index is denoted by

$$[G:H]. \tag{2.8.6}$$

Thus the index of the subgroup $\langle y \rangle$ of S_3 is 3. When G is infinite, the index may be infinite too.

Lemma 2.8.7 All left cosets aH of a subgroup H of a group G have the same order.

Proof. Multiplication by a defines a map $H \to aH$ that sends $h \rightsquigarrow ah$. This map is bijective because its inverse is multiplication by a^{-1}. □

Since the cosets all have the same order, and since they partition the group, we obtain the important *Counting Formula*

$$\begin{aligned} |G| &= |H|\,[G:H] \\ (\textit{order of } G) &= (\textit{order of } H)(\textit{number of cosets}), \end{aligned} \tag{2.8.8}$$

where, as always, $|G|$ denotes the order of the group. The equality has the obvious meaning if some terms are infinite. For the subgroup $\langle y \rangle$ of S_3, the formula reads $6 = 2 \cdot 3$.

It follows from the counting formula that the terms on the right side of (2.8.8) divide the left side. One of these facts is called Lagrange's Theorem:

Theorem 2.8.9 Lagrange's Theorem. Let H be a subgroup of a finite group G. The order of H divides the order of G. □

Corollary 2.8.10 The order of an element of a finite group divides the order of the group.

Proof. The order of an element a of a group G is equal to the order of the cyclic subgroup $\langle a \rangle$ generated by a (Proposition 2.4.2). □

Corollary 2.8.11 Suppose that a group G has prime order p. Let a be any element of G other than the identity. Then G is the cyclic group $\langle a \rangle$ generated by a.

Proof. The order of an element $a \neq 1$ is greater than 1 and it divides the order of G, which is the prime integer p. So the order of a is equal to p. This is also the order of the cyclic subgroup $\langle a \rangle$ generated by a. Since G has order p, $\langle a \rangle = G$. □

This corollary classifies groups of prime order p. They form one isomorphism class, the class of the cyclic groups of order p.

The counting formula can also be applied when a homomorphism $\varphi: G \to G'$ is given. As we have seen (2.7.15), the left cosets of the kernel $\ker \varphi$ are the nonempty fibres of the map φ. They are in bijective correspondence with the elements of the image.

$$[G:\ker \varphi] = |\operatorname{im} \varphi|. \tag{2.8.12}$$

Corollary 2.8.13 Let $\varphi: G \to G'$ be a homomorphism of finite groups. Then

- $|G| = |\ker \varphi| \cdot |\operatorname{im} \varphi|$,
- $|\ker \varphi|$ divides $|G|$, and
- $|\operatorname{im} \varphi|$ divides both $|G|$ and $|G'|$.

Proof. The first formula is obtained by combining (2.8.8) and (2.8.12), and it implies that $|\ker \varphi|$ and $|\operatorname{im} \varphi|$ divide $|G|$. Since the image is a subgroup of G', Lagrange's theorem tells us that its order divides $|G'|$ too. □

For example, the sign homomorphism $\sigma: S_n \to \{\pm 1\}$ (2.5.2)**(b)** is surjective, so its image has order 2. Its kernel, the alternating group A_n, has order $\frac{1}{2}n!$. Half of the elements of S_n are even permutations, and half are odd permutations.

The Counting Formula 2.8.8 has an analogue when a chain of subgroups is given.

Proposition 2.8.14 Multiplicative Property of the Index. Let $G \supset H \supset K$ be subgroups of a group G. Then $[G:K] = [G:H][H:K]$.

Proof. We will assume that the two indices on the right are finite, say $[G:H] = m$ and $[H:K] = n$. The reasoning when one or the other is infinite is similar. We list the m cosets of H in G, choosing representative elements for each coset, say as $g_1H, \ldots, g_mH$. Then $g_1H \cup \cdots \cup g_mH$ is a partition of G. Similarly, we choose representative elements for each coset of K in H, obtaining a partition $H = h_1K \cup \cdots \cup h_nK$. Since multiplication by g_i is an invertible operation, $g_iH = g_ih_1K \cup \cdots \cup g_ih_nK$ will be a partition of the coset g_iH. Putting these partitions together, G is partitioned into the mn cosets g_ih_jK. □

Right Cosets

Let us go back to the definition of cosets. We made the decision to work with left cosets aH. One can also define right cosets of a subgroup H and repeat the above discussion for them.

The right cosets of a subgroup H of a group G are the sets

$$Ha = \{ha \mid h \in H\}. \tag{2.8.15}$$

They are equivalence classes for the relation (*right congruence*)

$$a \equiv b \text{ if } b = ha, \text{ for some } h \text{ in } H.$$

Right cosets also partition the group G, but they aren't always the same as left cosets. For instance, the right cosets of the subgroup $\langle y \rangle$ of S_3 are

$$H = \{1, y\} = Hy, \quad Hx = \{x, x^2y\} = Hx^2y, \quad Hx^2 = \{x^2, xy\} = Hxy. \tag{2.8.16}$$

This isn't the same as the partition (2.8.4) into left cosets. However, if a subgroup is normal, its right and left cosets are equal.

Proposition 2.8.17 Let H be a subgroup of a group G. The following conditions are equivalent:

(i) H is a normal subgroup: For all h in H and all g in G, ghg^{-1} is in H.
(ii) For all g in G, $gHg^{-1} = H$.
(iii) For all g in G, the left coset gH is equal to the right coset Hg.
(iv) Every left coset of H in G is a right coset.

Proof. The notation gHg^{-1} stands for the set of all elements ghg^{-1}, with h in H.

Suppose that H is normal. So **(i)** holds, and it implies that $gHg^{-1} \subset H$ for all g in G. Substituting g^{-1} for g shows that $g^{-1}Hg \subset H$ as well. We multiply this inclusion on the left by g and on the right by g^{-1} to conclude that $H \subset gHg^{-1}$. Therefore $gHg^{-1} = H$. This shows that **(i)** implies **(ii)**. It is clear that **(ii)** implies **(i)**. Next, if $gHg^{-1} = H$, we multiply this equation on the right by g to conclude that $gH = Hg$. This shows that **(ii)** implies **(iii)**. One sees similarly that **(iii)** implies **(ii)**. Since **(iii)** implies **(iv)** is obvious, it remains only to check that **(iv)** implies **(iii)**.

We ask: Under what circumstances can a left coset be equal to a right coset? We recall that the right cosets partition the group G, and we note that the left coset gH and the right coset Hg have an element in common, namely $g = g \cdot 1 = 1 \cdot g$. So if the left coset gH is equal to any right coset, that coset must be Hg. □

Proposition 2.8.18

(a) If H is a subgroup of a group G and g is an element of G, the set gHg^{-1} is also a subgroup.
(b) If a group G has just one subgroup H of order r, then that subgroup is normal.

Proof. **(a)** Conjugation by g is an automorphism of G (see (2.6.4)), and gHg^{-1} is the image of H. **(b)** See (2.8.17): gHg^{-1} is a subgroup of order r. □

Note: If H is a subgroup of a finite group G, the counting formulas using right cosets or left cosets are the same, so the number of left cosets is equal to the number of right cosets. This is also true when G is infinite, though the proof can't be made by counting (see Exercise M.8). □

2.9 MODULAR ARITHMETIC

This section contains a brief discussion of one of the most important concepts in number theory, congruence of integers. If you have not run across this concept before, you will want to read more about it. See, for instance, [Stark]. We work with a fixed positive integer n throughout the section.

- Two integers a and b are said to be *congruent modulo n*

$$a \equiv b \text{ modulo } n, \tag{2.9.1}$$

if n divides $b - a$, or if $b = a + nk$ for some integer k. For instance, $2 \equiv 17$ modulo 5.

It is easy to check that congruence is an equivalence relation, so we may consider the equivalence classes, called *congruence classes*, that it defines. We use bar notation, and denote the congruence class of an integer a modulo n by the symbol $\bar{a}$. This congruence class is the set of integers

$$\bar{a} = \{\ldots, a - n, a, a + n, a + 2n, \ldots\}. \tag{2.9.2}$$

If a and b are integers, the equation $\bar{a} = \bar{b}$ means that $a \equiv b$ modulo n, or that n divides $b - a$. The congruence class $\bar{0}$ is the subgroup

$$\bar{0} = \mathbb{Z}n = \{\ldots, -n, 0, n, 2n, \ldots\} = \{kn \mid k \in \mathbb{Z}\}$$

of the additive group $\mathbb{Z}^+$. The other congruence classes are the cosets of this subgroup. Please note that $\mathbb{Z}n$ is not a right coset – it is a subgroup of $\mathbb{Z}^+$. The notation for a coset of a subgroup H analogous to aH, but using additive notation for the law of composition, is $a + H = \{a + h \mid h \in H\}$. To simplify notation, we denote the subgroup $\mathbb{Z}n$ by H. Then the cosets of H, the congruence classes, are the sets

$$a + H = \{a + kn \mid k \in \mathbb{Z}\}. \tag{2.9.3}$$

The n integers $0, 1, \ldots, n - 1$ are representative elements for the n congruence classes.

Proposition 2.9.4 There are n congruence classes modulo n, namely $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. The index $[\mathbb{Z}:\mathbb{Z}n]$ of the subgroup $\mathbb{Z}n$ in $\mathbb{Z}$ is n. □

Let $\bar{a}$ and $\bar{b}$ be congruence classes represented by integers a and b. Their *sum* is defined to be the congruence class of $a + b$, and their *product* is the class of ab. In other words, by definition,

$$\bar{a} + \bar{b} = \overline{a + b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}. \tag{2.9.5}$$

This definition needs some justification, because the same congruence class can be represented by many different integers. Any integer a' congruent to a modulo n represents the same class as a does. So it had better be true that if $a' \equiv a$ and $b' \equiv b$, then $a' + b' \equiv a + b$ and $a'b' \equiv ab$. Fortunately, this is so.

Lemma 2.9.6 If $a' \equiv a$ and $b' \equiv b$ modulo n, then $a' + b' \equiv a + b$ and $a'b' \equiv ab$ modulo n.

Proof. Assume that $a' \equiv a$ and $b' \equiv b$, so that $a' = a + rn$ and $b' = b + sn$ for some integers r and s. Then $a' + b' = a + b + (r + s)n$. This shows that $a' + b' \equiv a + b$. Similarly, $a'b' = (a + rn)(b + sn) = ab + (as + rb + rns)n$, so $a'b' \equiv ab$. □

The associative, commutative, and distributive laws hold for addition and multiplication of congruence classes because they hold for addition and multiplication of integers. For example, the distributive law is verified as follows:

$$\begin{aligned}
\bar{a}(\bar{b} + \bar{c}) &= \bar{a}\overline{(b + c)} = \overline{a(b + c)} && \textit{(definition of + and } \times \textit{ for congruence classes)} \\
&= \overline{ab + ac} && \textit{(distributive law in the integers)} \\
&= \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c} && \textit{(definition of + and } \times \textit{ for congruence classes).}
\end{aligned}$$

The verifications of other laws are similar, and we omit them.

The set of congruence classes modulo n may be denoted by any one of the symbols $\mathbb{Z}/\mathbb{Z}n$, $\mathbb{Z}/n\mathbb{Z}$, or $\mathbb{Z}/(n)$. Addition, subtraction, and multiplication in $\mathbb{Z}/\mathbb{Z}n$ can be made explicit by working with integers and taking remainders after division by n. That is what the formulas (2.9.5) mean. They tell us that the map

$$\mathbb{Z} \to \mathbb{Z}/\mathbb{Z}n \tag{2.9.7}$$

that sends an integer a to its congruence class $\bar{a}$ is compatible with addition and multiplication. Therefore computations can be made in the integers and then carried over to $\mathbb{Z}/\mathbb{Z}n$ at the end. However, computations are simpler if the numbers are kept small. This can be done by computing the remainder after some part of a computation has been made.

Thus if $n = 29$, so that $\mathbb{Z}/\mathbb{Z}n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{28}\}$, then $(\overline{35})(\overline{17} + \bar{7})$ can be computed as $\overline{35} \cdot \overline{24} = \bar{6} \cdot (-\bar{5}) = -\overline{30} = -\bar{1}$.

In the long run, the bars over the numbers become a nuisance. They are often left off. When omitting bars, one just has to remember this rule:

(2.9.8) To say $a = b$ in $\mathbb{Z}/\mathbb{Z}n$ means that $a \equiv b$ modulo n.

Congruences modulo a prime integer have special properties, which we discuss at the beginning of the next chapter.

2.10 THE CORRESPONDENCE THEOREM

Let $\varphi: G \to \mathcal{G}$ be a group homomorphism, and let H be a subgroup of G. We may *restrict* φ to H, obtaining a homomorphism

$$\varphi|_H : H \to \mathcal{G}. \tag{2.10.1}$$

This means that we take the same map φ but restrict its domain: So by definition, if h is in H, then $[\varphi|_H](h) = \varphi(h)$. (We've added brackets around the symbol $\varphi|_H$ for clarity.) The restriction is a homomorphism because φ is one, and the kernel of $\varphi|_H$ is the intersection of the kernel of φ with H:

$$\ker(\varphi|_H) = (\ker \varphi) \cap H. \tag{2.10.2}$$

This is clear from the definition of the kernel. The image of $\varphi|_H$ is the same as the image $\varphi(H)$ of H under the map φ.

The Counting Formula may help to describe the restriction. According to Corollary (2.8.13), the order of the image divides both $|H|$ and $|\mathcal{G}|$. If $|H|$ and $|\mathcal{G}|$ have no common factor, $\varphi(H) = \{1\}$, so H is contained in the kernel.

Example 2.10.3 The image of the sign homomorphism $\sigma: S_n \to \{\pm 1\}$ has order 2. If a subgroup H of the symmetric group S_n has odd order, it will be contained in the kernel of σ, the alternating group A_n of even permutations. This will be so when H is the cyclic subgroup generated by a permutation q that is an element of odd order in the group. Every permutation whose order in the group is odd, such as an n-cycle with n odd, is an even permutation. A permutation that has even order in the group may be odd or even. □

Proposition 2.10.4 Let $\varphi: G \to \mathcal{G}$ be a homomorphism with kernel K and let $\mathcal{H}$ be a subgroup of $\mathcal{G}$. Denote the inverse image $\varphi^{-1}(\mathcal{H})$ by H. Then H is a subgroup of G that contains K. If $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$, then H is a normal subgroup of G. If φ is surjective and if H is a normal subgroup of G, then $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$.

For example, let φ denote the determinant homomorphism $GL_n(\mathbb{R}) \to \mathbb{R}^\times$. The set of positive real numbers is a subgroup of $\mathbb{R}^\times$; it is normal because $\mathbb{R}^\times$ is abelian. Its inverse image, the set of invertible matrices with positive determinant, is a normal subgroup of $GL_n(\mathbb{R})$.

Proof. This proof is simple, but we must keep in mind that φ^{-1} is not a map. By definition, $\varphi^{-1}(\mathcal{H}) = H$ is the set of elements x of G such that $\varphi(x)$ is in $\mathcal{H}$. First, if x is in the kernel K, then $\varphi(x) = 1$. Since 1 is in $\mathcal{H}$, x is in H. Thus H contains K. We verify the conditions for a subgroup.

Closure: Suppose that x and y are in H. Then $\varphi(x)$ and $\varphi(y)$ are in $\mathcal{H}$. Since $\mathcal{H}$ is a subgroup, $\varphi(x)\varphi(y)$ is in $\mathcal{H}$. Since φ is a homomorphism, $\varphi(x)\varphi(y) = \varphi(xy)$. So $\varphi(xy)$ is in $\mathcal{H}$, and xy is in H.

Identity: 1 is in H because $\varphi(1) = 1$ is in $\mathcal{H}$.

Inverses: Let x be an element of H. Then $\varphi(x)$ is in $\mathcal{H}$, and since $\mathcal{H}$ is a subgroup, $\varphi(x)^{-1}$ is also in $\mathcal{H}$. Since φ is a homomorphism, $\varphi(x)^{-1} = \varphi(x^{-1})$, so $\varphi(x^{-1})$ is in $\mathcal{H}$, and x^{-1} is in H.

Suppose that $\mathcal{H}$ is a normal subgroup. Let x and g be elements of H and G, respectively. Then $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1}$ is a conjugate of $\varphi(x)$, and $\varphi(x)$ is in $\mathcal{H}$. Because $\mathcal{H}$ is normal, $\varphi(gxg^{-1})$ is in $\mathcal{H}$, and therefore gxg^{-1} is in H.

Suppose that φ is surjective, and that H is a normal subgroup of G. Let a be in $\mathcal{H}$, and let b be in $\mathcal{G}$. There are elements x of H and y of G such that $\varphi(x) = a$ and $\varphi(y) = b$. Since H is normal, yxy^{-1} is in H, and therefore $\varphi(yxy^{-1}) = bab^{-1}$ is in $\mathcal{H}$. □

Theorem 2.10.5 Correspondence Theorem. Let $\varphi: G \to \mathcal{G}$ be a *surjective* group homomorphism with kernel K. There is a bijective correspondence between subgroups of $\mathcal{G}$ and subgroups of G that contain K:

$$\{\text{subgroups of } G \text{ that contain } K\} \longleftrightarrow \{\text{subgroups of } \mathcal{G}\}.$$

This correspondence is defined as follows:

$$\text{a subgroup } H \text{ of } G \text{ that contains } K \rightsquigarrow \text{its image } \varphi(H) \text{ in } \mathcal{G},$$
$$\text{a subgroup } \mathcal{H} \text{ of } \mathcal{G} \rightsquigarrow \text{its inverse image } \varphi^{-1}(\mathcal{H}) \text{ in } G.$$

If H and $\mathcal{H}$ are corresponding subgroups, then H is normal in G if and only if $\mathcal{H}$ is normal in $\mathcal{G}$.

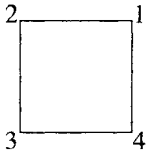
If H and $\mathcal{H}$ are corresponding subgroups, then $|H| = |\mathcal{H}||K|$.

Example 2.10.6 We go back to the homomorphism $\varphi: S_4 \to S_3$ that was defined in Example 2.5.13, and its kernel K (2.5.15).

The group S_3 has six subgroups, four of them proper. With the usual presentation, there is one proper subgroup of order 3, the cyclic group $\langle x \rangle$, and there are three subgroups of order 2, including $\langle y \rangle$. The Correspondence Theorem tells us that there are four proper subgroups of S_4 that contain K. Since $|K| = 4$, there is one subgroup of order 12 and there are three of order 8.

We know a subgroup of order 12, namely the alternating group A_4. That is the subgroup that corresponds to the cyclic group $\langle x \rangle$ of S_3.

The subgroups of order 8 can be explained in terms of symmetries of a square. With vertices of the square labeled as in the figure below, a counterclockwise rotation through the angle $\pi/2$ corresponds to the 4-cycle **(1234)**. Reflection about the diagonal through the vertex 1 corresponds to the transposition **(24)**. These two permutations generate a subgroup of order 8. The other subgroups of order 8 can be obtained by labeling the vertices in other ways.



There are also some subgroups of S_4 that do not contain K. The Correspondence Theorem has nothing to say about those subgroups. □

Proof of the Correspondence Theorem. Let H be a subgroup of G that contains K, and let $\mathcal{H}$ be a subgroup of $\mathcal{G}$. We must check the following points:

- $\varphi(H)$ is a subgroup of $\mathcal{G}$.
- $\varphi^{-1}(\mathcal{H})$ is a subgroup of G, and it contains K.
- $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$ if and only if $\varphi^{-1}(\mathcal{H})$ is a normal subgroup of G.
- *(bijectivity of the correspondence)* $\varphi(\varphi^{-1}(\mathcal{H})) = \mathcal{H}$ and $\varphi^{-1}(\varphi(H)) = H$.
- $|\varphi^{-1}(\mathcal{H})| = |\mathcal{H}||K|$.

Since $\varphi(H)$ is the image of the homomorphism $\varphi|_H$, it is a subgroup of $\mathcal{G}$. The second and third bullets form Proposition 2.10.4.

Concerning the fourth bullet, the equality $\varphi(\varphi^{-1}(\mathcal{H})) = \mathcal{H}$ is true for any surjective map of sets $\varphi: S \to S'$ and any subset $\mathcal{H}$ of S'. Also, $H \subset \varphi^{-1}(\varphi(H))$ is true for any map

φ of sets and any subset H of S. We omit the verification of these facts. Then the only thing remaining to be verified is that $H \supset \varphi^{-1}(\varphi(H))$. Let x be an element of $\varphi^{-1}(\varphi(H))$. We must show that x is in H. By definition of the inverse image, $\varphi(x)$ is in $\varphi(H)$, say $\varphi(x) = \varphi(a)$, with a in H. Then $a^{-1}x$ is in the kernel K (2.5.8), and since H contains K, $a^{-1}x$ is in H. Since both a and $a^{-1}x$ are in H, x is in H too.

We leave the proof of the last bullet as an exercise. □

2.11 PRODUCT GROUPS

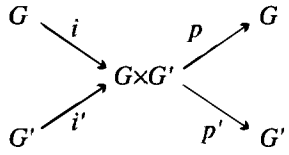
Let G, G' be two groups. The product set $G \times G'$, the set of pairs of elements (a, a') with a in G and a' in G', can be made into a group by component-wise multiplication – that is, multiplication of pairs is defined by the rule

$$(a, a') \cdot (b, b') = (ab, a'b'). \tag{2.11.1}$$

The pair (1, 1) is the identity, and the inverse of (a, a') is (a^{-1}, a'^{-1}). The associative law in $G \times G'$ follows from the fact that it holds in G and in G'.

The group obtained in this way is called the *product* of G and G' and is denoted by $G \times G'$. It is related to the two factors G and G' in a simple way that we can sum up in terms of some homomorphisms

(2.11.2)



They are defined by $i(x) = (x, 1)$, $i'(x') = (1, x')$, $p(x, x') = x$, $p'(x, x') = x'$. The injective homomorphisms i and i' may be used to identify G and G' with their images, the subgroups $G \times 1$ and $1 \times G'$ of $G \times G'$. The maps p and p' are surjective, the kernel of p is $1 \times G'$, and the kernel of p' is $G \times 1$. These are the *projections*.

It is obviously desirable to decompose a given group G as a product, that is, to find groups H and H' such that G is isomorphic to the product $H \times H'$. The groups H and H' will be simpler, and the relation between $H \times H'$ and its factors is easily understood. It is rare that a group is a product, but it does happen occasionally.

For example, it is rather surprising that a cyclic group of order 6 can be decomposed: A cyclic group C_6 of order 6 is isomorphic to the product $C_2 \times C_3$ of cyclic groups of orders 2 and 3. To see this, say that $C_2 = \langle y \rangle$ and $C_3 = \langle z \rangle$, with $y^2 = 1$ and $z^3 = 1$, and let x denote the element (y, z) of the product group $C_2 \times C_3$. The smallest positive integer k such that $x^k = (y^k, z^k)$ is the identity $(1, 1)$ is $k = 6$. So x has order 6. Since $C_2 \times C_3$ also has order 6, it is equal to the cyclic group $\langle x \rangle$. The powers of x, in order, are

$$(1, 1),\ (y, z),\ (1, z^2),\ (y, 1),\ (1, z),\ (y, z^2). \qquad \square$$

There is an analogous statement for a cyclic group of order rs, whenever the two integers r and s have no common factor.

Proposition 2.11.3 Let r and s be relatively prime integers. A cyclic group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s. □

On the other hand, a cyclic group of order 4 is *not* isomorphic to a product of two cyclic groups of order 2. Every element of $C_2 \times C_2$ has order 1 or 2, whereas a cyclic group of order 4 contains two elements of order 4.

The next proposition describes product groups.

Proposition 2.11.4 Let H and K be subgroups of a group G, and let $f: H \times K \to G$ be the multiplication map, defined by $f(h, k) = hk$. Its image is the set $HK = \{hk | h \in H, k \in K\}$.

(a) f is injective if and only if $H \cap K = \{1\}$.

(b) f is a homomorphism from the product group $H \times K$ to G if and only if elements of K commute with elements of H: $hk = kh$.

(c) If H is a normal subgroup of G, then HK is a subgroup of G.

(d) f is an isomorphism from the product group $H \times K$ to G if and only if $H \cap K = \{1\}$, $HK = G$, and also H and K are normal subgroups of G.

It is important to note that the multiplication map may be bijective though it isn't a group homomorphism. This happens, for instance, when $G = S_3$, and with the usual notation, $H = \langle x \rangle$ and $K = \langle y \rangle$.

Proof. **(a)** If $H \cap K$ contains an element $x \neq 1$, then x^{-1} is in H, and $f(x^{-1}, x) = 1 = f(1, 1)$, so f is not injective. Suppose that $H \cap K = \{1\}$. Let (h_1, k_1) and (h_2, k_2) be elements of $H \times K$ such that $h_1k_1 = h_2k_2$. We multiply both sides of this equation on the left by h_1^{-1} and on the right by k_2^{-1}, obtaining $k_1k_2^{-1} = h_1^{-1}h_2$. The left side is an element of K and the right side is an element of H. Since $H \cap K = \{1\}$, $k_1k_2^{-1} = h_1^{-1}h_2 = 1$. Then $k_1 = k_2$, $h_1 = h_2$, and $(h_1, k_1) = (h_2, k_2)$.

(b) Let (h_1, k_1) and (h_2, k_2) be elements of the product group $H \times K$. The product of these elements in the product group $H \times K$ is (h_1h_2, k_1k_2), and $f(h_1h_2, k_1k_2) = h_1h_2k_1k_2$, while $f(h_1, k_1)f(h_2, k_2) = h_1k_1h_2k_2$. These elements are equal if and only if $h_2k_1 = k_1h_2$.

(c) Suppose that H is a normal subgroup. We note that KH is a union of the left cosets kH with k in K, and that HK is a union of the right cosets Hk. Since H is normal, $kH = Hk$, and therefore $HK = KH$. Closure of HK under multiplication follows, because $HKHK = HHKK = HK$. Also, $(hk)^{-1} = k^{-1}h^{-1}$ is in $KH = HK$. This proves closure of HK under inverses.

(d) Suppose that H and K satisfy the conditions given. Then f is both injective and surjective, so it is bijective. According to **(b)**, it is an isomorphism if and only if $hk = kh$ for all h in H and k in K. Consider the commutator $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. Since K is normal, the left side is in K, and since H is normal, the right side is in H. Since $H \cap K = \{1\}$, $hkh^{-1}k^{-1} = 1$, and $hk = kh$. Conversely, if f is an isomorphism, one may verify the conditions listed in the isomorphic group $H \times K$ instead of in G. □

We use this proposition to classify groups of order 4:

Proposition 2.11.5 There are two isomorphism classes of groups of order 4, the class of the cyclic group C_4 of order 4 and the class of the Klein Four Group, which is isomorphic to the product $C_2 \times C_2$ of two groups of order 2.

Proof. Let G be a group of order 4. The order of any element x of G divides 4, so there are two cases to consider:

Case 1: G contains an element of order 4. Then G is a cyclic group of order 4.

Case 2: Every element of G except the identity has order 2.

In this case, $x = x^{-1}$ for every element x of G. Let x and y be two elements of G. Then xy has order 2, so $xyx^{-1}y^{-1} = (xy)(xy) = 1$. This shows that x and y commute (2.6.5), and since these are arbitrary elements, G is abelian. So every subgroup is normal. We choose distinct elements x and y in G, and we let H and K be the cyclic groups of order 2 that they generate. Proposition 2.11.4**(d)** shows that G is isomorphic to the product group $H \times K$. □

2.12 QUOTIENT GROUPS

In this section we show that a law of composition can be defined on the set of cosets of a *normal* subgroup N of any group G. This law makes the set of cosets of a normal subgroup into a group, called a *quotient group*.

Addition of congruence classes of integers modulo n is an example of the quotient construction. Another familiar example is addition of angles. Every real number represents an angle, and two real numbers represent the same angle if they differ by an integer multiple of 2π. The group N of integer multiples of 2π is a subgroup of the additive group $\mathbb{R}^+$ of real numbers, and angles correspond naturally to (additive) cosets $\theta + N$ of N in G. The group of angles is the quotient group whose elements are the cosets.

The set of cosets of a normal subgroup N of a group G is often denoted by G/N.

(2.12.1) $\qquad G/N$ is the set of cosets of N in G.

When we regard a coset C as an element of the set of cosets, the bracket notation $[C]$ may be used. If $C = aN$, we may also use the bar notation to denote the element $[C]$ by $\bar{a}$, and then we would denote the set of cosets by $\overline{G}$:

$$\overline{G} = G/N.$$

Theorem 2.12.2 Let N be a normal subgroup of a group G, and let $\overline{G}$ denote the set of cosets of N in G. There is a law of composition on $\overline{G}$ that makes this set into a group, such that the map $\pi: G \to \overline{G}$ defined by $\pi(a) = \bar{a}$ is a surjective homomorphism whose kernel is N.

• The map π is often referred to as the *canonical map* from G to $\overline{G}$. The word "canonical" indicates that this is the only map that we might reasonably be talking about.

The next corollary is very simple, but it is important enough to single out:

Corollary 2.12.3 Let N be a normal subgroup of a group G, and let $\overline{G}$ denote the set of cosets of N in G. Let $\pi: G \to \overline{G}$ be the canonical homomorphism. Let $a_1, \ldots, a_k$ be elements of G such that the product $a_1 \cdots a_k$ is in N. Then $\bar{a}_1 \cdots \bar{a}_k = \bar{1}$.

Proof. Let $p = a_1 \cdots a_k$. Then p is in N, so $\pi(p) = \bar{p} = \bar{1}$. Since π is a homomorphism, $\bar{a}_1 \cdots \bar{a}_k = \bar{p}$. □

Proof of Theorem 2.12.2. There are several things to be done. We must

- define a law of composition on $\overline{G}$,
- prove that the law makes $\overline{G}$ into a group,
- prove that π is a surjective homomorphism, and
- prove that the kernel of π is N.

We use the following notation: If A and B are subsets of a group G, then AB denotes the set of products ab:

$$AB = \{x \in G \mid x = ab \text{ for some } a \in A \text{ and } b \in B\}. \tag{2.12.4}$$

We will call this a *product set*, though in some other contexts the phrase "product set" refers to the set $A \times B$ of pairs of elements.

Lemma 2.12.5 Let N be a normal subgroup of a group G, and let aN and bN be cosets of N. The product set $(aN)(bN)$ is also a coset. It is equal to the coset abN.

We note that the set $(aN)(bN)$ consists of all elements of G that can be written in the form $anbn'$, with n and n' in N.

Proof. Since N is a subgroup, $NN = N$. Since N is normal, left and right cosets are equal: $Nb = bN$ (2.8.17). The lemma is proved by the following formal manipulation:

$$(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN. \qquad \square$$

This lemma allows us to define multiplication on the set $\overline{G} = G/N$. Using the bracket notation (2.7.8), the definition is this: If C_1 and C_2 are cosets, then $[C_1][C_2] = [C_1C_2]$, Where C_1C_2 is the product set. The lemma shows that this product set is another coset. To compute the product $[C_1][C_2]$, take any elements a in C_1 and b in C_2. Then $C_1 = aN$, $C_2 = bN$, and C_1C_2 is the coset abN that contains ab. So we have the very natural formula

$$[aN][bN] = [abN] \quad \text{or} \quad \overline{a}\overline{b} = \overline{ab}. \tag{2.12.6}$$

Then by definition of the map π in (2.12.2),

$$\pi(a)\pi(b) = \overline{a}\overline{b} = \overline{ab} = \pi(ab). \tag{2.12.7}$$

The fact that π is a homomorphism will follow from (2.12.7), once we show that $\overline{G}$ is a group. Since the canonical map π is surjective (2.7.8), the next lemma proves this.

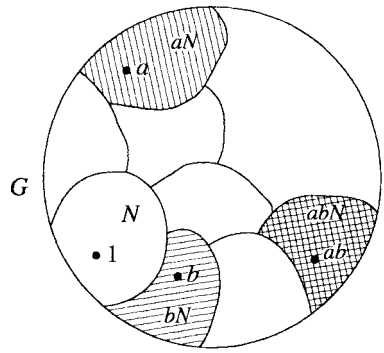
Lemma 2.12.8 Let G be a group, and let Y be a set with a law of composition, both laws written with multiplicative notation. Let $\varphi : G \to Y$ be a surjective map with the homomorphism property, that $\varphi(ab) = \varphi(a)\varphi(b)$ for all a and b in G. Then Y is a group and φ is a homomorphism.

Proof. The group axioms that are true in G are carried over to Y by the surjective map φ. Here is the proof of the associative law: Let y_1, y_2, y_3 be elements of Y. Since φ is surjective, $y_i = \varphi(x_i)$ for some x_i in G. Then

$$(y_1y_2)y_3 = (\varphi(x_1)\varphi(x_2))\varphi(x_3) = \varphi(x_1x_2)\varphi(x_3) = \varphi((x_1x_2)x_3)$$
$$\stackrel{*}{=} \varphi(x_1(x_2x_3)) = \varphi(x_1)\varphi(x_2x_3) = \varphi(x_1)(\varphi(x_2)\varphi(x_3)) = y_1(y_2y_3).$$

The equality marked with an asterisk is the associative law in G. The other equalities follow from the homomorphism property of φ. The verifications of the other group axioms are similar. □

The only thing remaining to be verified is that the kernel of the homomorphism π is the subgroup N. Well, $\pi(a) = \pi(1)$ if and only if $\bar{a} = \bar{1}$, or $[aN] = [1N]$, and this is true if and only if a is an element of N. □

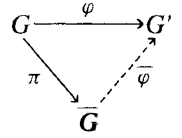


(2.12.9) A Schematic Diagram of Coset Multiplication.

Note: Our assumption that N be a *normal* subgroup of G is crucial to Lemma 2.12.5. If H is not normal, there will be left cosets C_1 and C_2 of H in G such that the product set C_1C_2 does not lie in a single left coset. Going back once more to the subgroup $H = \langle y \rangle$ of S_3, the product set $(1H)(xH)$ contains four elements: $\{1, y\}\{x, xy\} = \{x, xy, x^2y, x^2\}$. It is not a coset. The subgroup H is not normal. □

The next theorem relates the quotient group construction to a general group homomorphism, and it provides a fundamental method of identifying quotient groups.

Theorem 2.12.10 First Isomorphism Theorem. Let $\varphi : G \to G'$ be a surjective group homomorphism with kernel N. The quotient group $\bar{G} = G/N$ is isomorphic to the image G'. To be precise, let $\pi : G \to \bar{G}$ be the canonical map. There is a unique isomorphism $\bar{\varphi} : \bar{G} \to G'$ such that $\varphi = \bar{\varphi} \circ \pi$.



Proof. The elements of $\overline{G}$ are the cosets of N, and they are also the fibres of the map φ (2.7.15). The map $\overline{\varphi}$ referred to in the theorem is the one that sends a nonempty fibre to its image: $\overline{\varphi}(\overline{x}) = \varphi(x)$. For any surjective map of sets $\varphi: G \to G'$, one can form the set $\overline{G}$ of fibres, and then one obtains a diagram as above, in which $\overline{\varphi}$ is the bijective map that sends a fibre to its image. When φ is a group homomorphism, $\overline{\varphi}$ is an isomorphism because $\overline{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. □

Corollary 2.12.11 Let $\varphi: G \to G'$ be a group homomorphism with kernel N and image H'. The quotient group $\overline{G} = G/N$ is isomorphic to the image H'. □

Two quick examples: The image of the absolute value map $\mathbb{C}^\times \to \mathbb{R}^\times$ is the group of positive real numbers, and its kernel is the unit circle U. The theorem asserts that the quotient group $\mathbb{C}^\times/U$ is isomorphic to the multiplicative group of positive real numbers. The determinant is a surjective homomorphism $GL_n(\mathbb{R}) \to \mathbb{R}^\times$, whose kernel is the special linear group $SL_n(\mathbb{R})$. So the quotient $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ is isomorphic to $\mathbb{R}^\times$.

There are also theorems called the Second and the Third Isomorphism Theorems, though they are less important.

Es giebt alſo ſehr viel verſchiedene Arten von Größen,
welche ſich nicht wohl herzehlen laßen;
und daher entſtehen die verſchiedene Theile der Mathematic,
deren eine jegliche mit einer beſondern Art von Größen beſchäftiget iſt.

—Leonhard Euler

EXERCISES

Section 1 Laws of Composition

1.1. Let S be a set. Prove that the law of composition defined by $ab = a$ for all a and b in S is associative. For which sets does this law have an identity?

1.2. Prove the properties of inverses that are listed near the end of the section.

1.3. Let $\mathbb{N}$ denote the set $\{1, 2, 3, \ldots, \}$ of natural numbers, and let $s: \mathbb{N} \to \mathbb{N}$ be the *shift* map, defined by $s(n) = n + 1$. Prove that s has no right inverse, but that it has infinitely many left inverses.

Section 2 Groups and Subgroups

2.1. Make a multiplication table for the symmetric group S_3.

2.2. Let S be a set with an associative law of composition and with an identity element. Prove that the subset consisting of the invertible elements in S is a group.

2.3. Let x, y, z, and w be elements of a group G.

(a) Solve for y, given that $xyz^{-1}w = 1$.

(b) Suppose that $xyz = 1$. Does it follow that $yzx = 1$? Does it follow that $yxz = 1$?

2.4. In which of the following cases is H a subgroup of G?

(a) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$.

(b) $G = \mathbb{R}^\times$ and $H = \{1, -1\}$.

(c) $G = \mathbb{Z}^+$ and H is the set of positive integers.

(d) $G = \mathbb{R}^\times$ and H is the set of positive reals.

(e) $G = GL_2(\mathbb{R})$ and H is the set of matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$.

2.5. In the definition of a subgroup, the identity element in H is required to be the identity of G. One might require only that H have an identity element, not that it need be the same as the identity in G. Show that if H has an identity at all, then it is the identity in G. Show that the analogous statement is true for inverses.

2.6. Let G be a group. Define an *opposite group* G° with law of composition $a * b$ as follows: The underlying set is the same as G, but the law of composition is $a * b = ba$. Prove that G° is a group.

Section 3 Subgroups of the Additive Group of Integers

3.1. Let $a = 123$ and $b = 321$. Compute $d = \gcd(a, b)$, and express d as an integer combination $ra + bs$.

3.2. Prove that if a and b are positive integers whose sum is a prime p, their greatest common divisor is 1.

3.3. **(a)** Define the greatest common divisor of a set $\{a_1, \ldots, a_n\}$ of n integers. Prove that it exists, and that it is an integer combination of $a_1, \ldots, a_n$.

(b) Prove that if the greatest common divisor of $\{a_1, \ldots, a_n\}$ is d, then the greatest common divisor of $\{a_1/d, \ldots, a_n/d\}$ is 1.

Section 4 Cyclic Groups

4.1. Let a and b be elements of a group G. Assume that a has order 7 and that $a^3b = ba^3$. Prove that $ab = ba$.

4.2. An nth root of unity is a complex number z such that $z^n = 1$.

(a) Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.

(b) Determine the product of all the nth roots of unity.

4.3. Let a and b be elements of a group G. Prove that ab and ba have the same order.

4.4. Describe all groups G that contain no proper subgroup.

4.5. Prove that every subgroup of a cyclic group is cyclic. Do this by working with exponents, and use the description of the subgroups of $\mathbb{Z}^+$.

4.6. **(a)** Let G be a cyclic group of order 6. How many of its elements generate G? Answer the same question for cyclic groups of orders 5 and 8.

(b) Describe the number of elements that generate a cyclic group of arbitrary order n.

4.7. Let x and y be elements of a group G. Assume that each of the elements x, y, and xy has order 2. Prove that the set $H = \{1, x, y, xy\}$ is a subgroup of G, and that it has order 4.

4.8. **(a)** Prove that the elementary matrices of the first and third types (1.2.4) generate $GL_n(\mathbb{R})$.

(b) Prove that the elementary matrices of the first type generate $SL_n(\mathbb{R})$. Do the 2×2 case first.

4.9. How many elements of order 2 does the symmetric group S_4 contain?

4.10. Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian?

4.11. **(a)** Adapt the method of row reduction to prove that the transpositions generate the symmetric group S_n.

(b) Prove that, for $n \geq 3$, the three-cycles generate the alternating group A_n.

Section 5 Homomorphisms

5.1. Let $\varphi: G \to G'$ be a surjective homomorphism. Prove that if G is cyclic, then G' is cyclic, and if G is abelian, then G' is abelian.

5.2. Prove that the intersection $K \cap H$ of subgroups of a group G is a subgroup of H, and that if K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H.

5.3. Let U denote the group of invertible upper triangular 2×2 matrices $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, and let $\varphi: U \to \mathbb{R}^\times$ be the map that sends $A \rightsquigarrow a^2$. Prove that φ is a homomorphism, and determine its kernel and image.

5.4. Let $f: \mathbb{R}^+ \to \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism, and determine its kernel and image.

5.5. Prove that the $n \times n$ matrices that have the block form $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$, with A in $GL_r(\mathbb{R})$ and D in $GL_{n-r}(\mathbb{R})$, form a subgroup H of $GL_n(\mathbb{R})$, and that the map $H \to GL_r(\mathbb{R})$ that sends $M \rightsquigarrow A$ is a homomorphism. What is its kernel?

5.6. Determine the center of $GL_n(\mathbb{R})$.

Hint: You are asked to determine the invertible matrices A that commute with every invertible matrix B. Do not test with a general matrix B. Test with elementary matrices.

Section 6 Isomorphisms

6.1. Let G' be the group of real matrices of the form $\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}$. Is the map $\mathbb{R}^+ \to G'$ that sends x to this matrix an isomorphism?

6.2. Describe all homomorphisms $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$. Determine which are injective, which are surjective, and which are isomorphisms.

6.3. Show that the functions $f = 1/x$, $g = (x-1)/x$ generate a group of functions, the law of composition being composition of functions, that is isomorphic to the symmetric group S_3.

6.4. Prove that in a group, the products ab and ba are conjugate elements.

6.5. Decide whether or not the two matrices $A = \begin{bmatrix} 3 & \\ & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix}$ are conjugate elements of the general linear group $GL_2(\mathbb{R})$.

6.6. Are the matrices $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$ conjugate elements of the group $GL_2(\mathbb{R})$? Are they conjugate elements of $SL_2(\mathbb{R})$?

6.7. Let H be a subgroup of G, and let g be a fixed element of G. The *conjugate subgroup* gHg^{-1} is defined to be the set of all conjugates ghg^{-1}, with h in H. Prove that gHg^{-1} is a subgroup of G.

6.8. Prove that the map $A \rightsquigarrow (A^t)^{-1}$ is an automorphism of $GL_n(\mathbb{R})$.

6.9. Prove that a group G and its opposite group G° (Exercise 2.6) are isomorphic.

6.10. Find all automorphisms of
(a) a cyclic group of order 10, **(b)** the symmetric group S_3.

6.11. Let a be an element of a group G. Prove that if the set $\{1, a\}$ is a normal subgroup of G, then a is in the center of G.

Section 7 Equivalence Relations and Partitions

7.1. Let G be a group. Prove that the relation $a \sim b$ if $b = gag^{-1}$ for some g in G is an equivalence relation on G.

7.2. An equivalence relation on S is determined by the subset R of the set $S \times S$ consisting of those pairs (a, b) such that $a \sim b$. Write the axioms for an equivalence relation in terms of the subset R.

7.3. With the notation of Exercise 7.2, is the intersection $R \cap R'$ of two equivalence relations R and R' an equivalence relation? Is the union?

7.4. A relation R on the set of real numbers can be thought of as a subset of the (x, y)-plane. With the notation of Exercise 7.2, explain the geometric meaning of the reflexive and symmetric properties.

7.5. With the notation of Exercise 7.2, each of the following subsets R of the (x, y)-plane defines a relation on the set $\mathbb{R}$ of real numbers. Determine which of the axioms (2.7.3) are satisfied: **(a)** the set $\{(s, s) \mid s \in \mathbb{R}\}$, **(b)** the empty set, **(c)** the locus $\{xy + 1 = 0\}$, **(d)** the locus $\{x^2y - xy^2 - x + y = 0\}$.

7.6. How many different equivalence relations can be defined on a set of five elements?

Section 8 Cosets

8.1. Let H be the cyclic subgroup of the alternating group A_4 generated by the permutation **(123)**. Exhibit the left and the right cosets of H explicitly.

8.2. In the additive group $\mathbb{R}^m$ of vectors, let W be the set of solutions of a system of homogeneous linear equations $AX = 0$. Show that the set of solutions of an inhomogeneous system $AX = B$ is either empty, or else it is an (additive) coset of W.

8.3. Does every group whose order is a power of a prime p contain an element of order p?

8.4. Does a group of order 35 contain an element of order 5? of order 7?

8.5. A finite group contains an element x of order 10 and also an element y of order 6. What can be said about the order of G?

8.6. Let $\varphi: G \to G'$ be a group homomorphism. Suppose that $|G| = 18$, $|G'| = 15$, and that φ is not the trivial homomorphism. What is the order of the kernel?

8.7. A group G of order 22 contains elements x and y, where $x \neq 1$ and y is not a power of x. Prove that the subgroup generated by these elements is the whole group G.

8.8. Let G be a group of order 25. Prove that G has at least one subgroup of order 5, and that if it contains only one subgroup of order 5, then it is a cyclic group.

8.9. Let G be a finite group. Under what circumstances is the map $\varphi: G \to G$ defined by $\varphi(x) = x^2$ an automorphism of G?

8.10. Prove that every subgroup of index 2 is a normal subgroup, and show by example that a subgroup of index 3 need not be normal.

8.11. Let G and H be the following subgroups of $GL_2(\mathbb{R})$:

$$G = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \right\}, \quad H = \left\{ \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \right\},$$

with x and y real and $x > 0$. An element of G can be represented by a point in the right half plane. Make sketches showing the partitions of the half plane into left cosets and into right cosets of H.

8.12. Let S be a subset of a group G that contains the identity element 1, and such that the left cosets aS, with a in G, partition G. Prove that S is a subgroup of G.

8.13. Let S be a set with a law of composition. A partition $\Pi_1 \cup \Pi_2 \cup \cdots$ of S is *compatible* with the law of composition if for all i and j, the product set

$$\Pi_i \Pi_j = \{xy \mid x \in \Pi_i, y \in \Pi_j\}$$

is contained in a single subset Π_k of the partition.

(a) The set $\mathbb{Z}$ of integers can be partitioned into the three sets [Pos], [Neg], [{0}]. Discuss the extent to which the laws of composition $+$ and $\times$ are compatible with this partition.

(b) Describe all partitions of the integers that are compatible with the operation $+$.

Section 9 Modular Arithmetic

9.1. For which integers n does 2 have a multiplicative inverse in $\mathbb{Z}/\mathbb{Z}n$?

9.2. What are the possible values of a^2 modulo 4? modulo 8?

9.3. Prove that every integer a is congruent to the sum of its decimal digits modulo 9.

9.4. Solve the congruence $2x \equiv 5$ modulo 9 and modulo 6.

9.5. Determine the integers n for which the pair of congruences $2x - y \equiv 1$ and $4x + 3y \equiv 2$ modulo n has a solution.

9.6. Prove the *Chinese Remainder Theorem*: Let a, b, u, v be integers, and assume that the greatest common divisor of a and b is 1. Then there is an integer x such that $x \equiv u$ modulo a and $x \equiv v$ modulo b.

Hint: Do the case $u = 0$ and $v = 1$ first.

9.7. Determine the order of each of the matrices $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ when the matrix entries are interpreted modulo 3.

Section 10 The Correspondence Theorem

10.1. Describe how to tell from the cycle decomposition whether a permutation is odd or even.

10.2. Let H and K be subgroups of a group G.

(a) Prove that the intersection $xH \cap yK$ of two cosets of H and K is either empty or else is a coset of the subgroup $H \cap K$.

(b) Prove that if H and K have finite index in G then $H \cap K$ also has finite index in G.

10.3. Let G and G' be cyclic groups of orders 12 and 6, generated by elements x and y, respectively, and let $\varphi : G \to G'$ be the map defined by $\varphi(x^i) = y^i$. Exhibit the correspondence referred to in the Correspondence Theorem explicitly.

10.4. With the notation of the Correspondence Theorem, let H and H' be corresponding subgroups. Prove that $[G:H] = [G':H']$.

10.5. With reference to the homomorphism $S_4 \to S_3$ described in Example 2.5.13, determine the six subgroups of S_4 that contain K.

Section 11 Product Groups

11.1. Let x be an element of order r of a group G, and let y be an element of G' of order s. What is the order of (x, y) in the product group $G \times G'$?

11.2. What does Proposition 2.11.4 tell us when, with the usual notation for the symmetric group S_3, K and H are the subgroups $\langle y \rangle$ and $\langle x \rangle$?

11.3. Prove that the product of two infinite cyclic groups is not infinite cyclic.

11.4. In each of the following cases, determine whether or not G is isomorphic to the product group $H \times K$.

(a) $G = \mathbb{R}^\times$, $H = \{\pm 1\}$, $K = \{\text{positive real numbers}\}$.

(b) $G = \{\text{invertible upper triangular } 2 \times 2 \text{ matrices}\}$, $H = \{\text{invertible diagonal matrices}\}$, $K = \{\text{upper triangular matrices with diagonal entries } 1\}$.

(c) $G = \mathbb{C}^\times$, $H = \{\text{unit circle}\}$, $K = \{\text{positive real numbers}\}$.

11.5. Let G_1 and G_2 be groups, and let Z_i be the center of G_i. Prove that the center of the product group $G_1 \times G_2$ is $Z_1 \times Z_2$.

11.6. Let G be a group that contains normal subgroups of orders 3 and 5, respectively. Prove that G contains an element of order 15.

11.7. Let H be a subgroup of a group G, let $\varphi: G \to H$ be a homomorphism whose restriction to H is the identity map, and let N be its kernel. What can one say about the product map $H \times N \to G$?

11.8. Let G, G', and H be groups. Establish a bijective correspondence between homomorphisms $\Phi: H \to G \times G'$ from H to the product group and pairs (φ, φ') consisting of a homomorphism $\varphi: H \to G$ and a homomorphism $\varphi': H \to G'$.

11.9. Let H and K be subgroups of a group G. Prove that the product set HK is a subgroup of G if and only if $HK = KH$.

Section 12 Quotient Groups

12.1. Show that if a subgroup H of a group G is not normal, there are left cosets aH and bH whose product is not a coset.

12.2. In the general linear group $GL_3(\mathbb{R})$, consider the subsets

$$H = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}, \text{ and } K = \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where $*$ represents an arbitrary real number. Show that H is a subgroup of GL_3, that K is a normal subgroup of H, and identify the quotient group H/K. Determine the center of H.

12.3. Let P be a partition of a group G with the property that for any pair of elements A, B of the partition, the product set AB is contained entirely within another element C of the partition. Let N be the element of P that contains 1. Prove that N is a normal subgroup of G and that P is the set of its cosets.

12.4. Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = \mathbb{C}^\times$ of fourth roots of unity. Describe the cosets of H in G explicitly. Is G/H isomorphic to G?

12.5. Let G be the group of upper triangular real matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, with a and d different from zero. For each of the following subsets, determine whether or not S is a subgroup, and whether or not S is a normal subgroup. If S is a normal subgroup, identify the quotient group G/S.

(i) S is the subset defined by $b = 0$.

(ii) S is the subset defined by $d = 1$.

(iii) S is the subset defined by $a = d$.

Miscellaneous Problems

M.1. Describe the column vectors $(a, c)^t$ that occur as the first column of an integer matrix A whose inverse is also an integer matrix.

M.2. **(a)** Prove that every group of even order contains an element of order 2.

(b) Prove that every group of order 21 contains an element of order 3.

M.3. Classify groups of order 6 by analyzing the following three cases:

(i) G contains an element of order 6.

(ii) G contains an element of order 3 but none of order 6.

(iii) All elements of G have order 1 or 2.

M.4. A *semigroup* S is a set with an associative law of composition and with an identity. Elements are not required to have inverses, and the Cancellation Law need not hold. A semigroup S is said to be generated by an element s if the set $\{1, s, s^2, \ldots\}$ of nonnegative powers of s is equal to S. Classify semigroups that are generated by one element.

M.5. Let S be a finite semigroup (see Exercise M.4) in which the Cancellation Law 2.2.3 holds. Prove that S is a group.

***M.6.** Let $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$ be points in k-dimensional space $\mathbb{R}^k$. A *path* from a to b is a continuous function on the unit interval $[0, 1]$ with values in $\mathbb{R}^k$, a function $X : [0, 1] \to \mathbb{R}^k$, sending $t \rightsquigarrow X(t) = (x_1(t), \ldots, x_k(t))$, such that $X(0) = a$ and $X(1) = b$. If S is a subset of $\mathbb{R}^k$ and if a and b are in S, define $a \sim b$ if a and b can be joined by a path lying entirely in S.

(a) Show that $\sim$ is an equivalence relation on S. Be careful to check that any paths you construct stay within the set S.

(b) A subset S is *path connected* if $a \sim b$ for any two points a and b in S. Show that every subset S is partitioned into path-connected subsets with the property that two points in different subsets cannot be connected by a path in S.

(c) Which of the following loci in $\mathbb{R}^2$ are path-connected: $\{x^2 + y^2 = 1\}$, $\{xy = 0\}$, $\{xy = 1\}$?

***M.7.** The set of $n \times n$ matrices can be identified with the space $\mathbb{R}^{n \times n}$. Let G be a subgroup of $GL_n(\mathbb{R})$. With the notation of Exercise M.6, prove:

(a) If A, B, C, D are in G, and if there are paths in G from A to B and from C to D, then there is a path in G from AC to BD.

(b) The set of matrices that can be joined to the identity I forms a normal subgroup of G. (It is called the *connected component* of G.)

***M.8.** **(a)** The group $SL_n(\mathbb{R})$ is generated by elementary matrices of the first type (see Exercise 4.8). Use this fact to prove that $SL_n(\mathbb{R})$ is path-connected.

(b) Show that $GL_n(\mathbb{R})$ is a union of two path-connected subsets, and describe them.

M.9. (*double cosets*) Let H and K be subgroups of a group G, and let g be an element of G. The set $HgK = \{x \in G \mid x = hgk \text{ for some } h \in H, k \in K\}$ is called a *double coset*. Do the double cosets partition G?

M.10. Let H be a subgroup of a group G. Show that the double cosets (see Exercise M.9)

$$HgH = \{h_1 g h_2 | h_1, h_2 \in H\}$$

are the left cosets gH if and only if H is normal.

***M.11.** Most invertible matrices can be written as a product $A = LU$ of a lower triangular matrix L and an upper triangular matrix U, where in addition all diagonal entries of U are 1.

(a) Explain how to compute L and U when the matrix A is given.

(b) Prove uniqueness, that there is at most one way to write A as such a product.

(c) Show that every invertible matrix can be written as a product LPU, where L, U are as above and P is a permutation matrix.

(d) Describe the double cosets LgU (see Exercise M.9).

M.12. (*postage stamp problem*) Let a and b be positive, relatively prime integers.

(a) Prove that every sufficiently large positive integer n can be obtained as $ra + sb$, where r and s are positive integers.

(b) Determine the largest integer that is not of this form.

M.13. (*a game*) The starting position is the point $(1, 1)$, and a permissible "move" replaces a point (a, b) by one of the points $(a + b, b)$ or $(a, a + b)$. So the position after the first move will be either $(2, 1)$ or $(1, 2)$. Determine the points that can be reached.

M.14. (*generating $SL_2(\mathbb{Z})$*) Prove that the two matrices

$$E = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad E' = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

generate the group $SL_2(\mathbb{Z})$ of all *integer* matrices with determinant 1. Remember that the subgroup they generate consists of all elements that can be expressed as products using the four elements E, E', E^{-1}, E'^{-1}.

Hint: Do not try to write a matrix directly as a product of the generators. Use row reduction.

M.15. (*the semigroup generated by elementary matrices*) Determine the semigroup S (see Exercise M.4) of matrices A that can be written as a product, of arbitrary length, each of whose terms is one of the two matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \text{or} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Show that every element of S can be expressed as such a product in exactly one way.

M.16. [1](*the homophonic group: a mathematical diversion*) By definition, English words have the same pronunciation if their phonetic spellings in the dictionary are the same. The homophonic group $\mathcal{H}$ is generated by the letters of the alphabet, subject to the following relations: English words with the same pronunciation represent equal elements of the group. Thus $be = bee$, and since $\mathcal{H}$ is a group, we can cancel be to conclude that $e = 1$. Try to determine the group $\mathcal{H}$.

[1] I learned this problem from a paper by Mesirov, Mesirov, Selcuk, Washington and Zagier.