Chapter 2

Groups

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

1. THE DEFINITION OF A GROUP

In this chapter we study one of the most important algebraic concepts, that of a *group*. A group is a set on which a law of composition is defined, such that all elements have inverses. The precise definition is given below in (1.10). For example, the set of nonzero real numbers forms a group $\mathbb{R}^{\times}$ under multiplication, and the set of all real numbers forms a group $\mathbb{R}^{+}$ under addition. The set of invertible $n \times n$ matrices, called the general linear group, is a very important example in which the law of composition is matrix multiplication. We will see many more examples as we go along.

By a *law of composition* on a set S, we mean a rule for combining pairs a, b of elements S to get another element, say p, of S. The original models for this notion are addition and multiplication of real numbers. Formally, a law of composition is a function of two variables on S, with values in S, or it is a map

$$\begin{aligned} S \times S &\longrightarrow S \\ a, b &\rightsquigarrow p. \end{aligned}$$

Here, $S \times S$ denotes, as always, the product set of pairs (a, b) of elements of S.

Functional notation $p = f(a, b)$ isn't very convenient for laws of composition. Instead, the element obtained by applying the law to a pair (a, b) is usually denoted using a notation resembling those used for multiplication or addition:

$$p = ab,\ a \times b,\ a \circ b,\ a + b, \text{ and so on,}$$

a choice being made for the particular law in question. We call the element p the *product* or *sum* of a and b, depending on the notation chosen.

Our first example of a law of composition, and one of the two main examples, is matrix multiplication on the set S of $n \times n$ matrices.

We will use the product notation ab most frequently. Anything we prove with product notation can be rewritten using another notation, such as addition. It will continue to be valid, because the rewriting is just a change of notation.

It is important to note that the symbol ab is a notation for a certain element of S. Namely, it is the element obtained by applying the given law of composition to the elements called a and b. Thus if the law is multiplication of matrices 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 can not be recovered from it.

Let us consider a law of composition written multiplicatively as ab. It will be called *associative* if the rule

$$(1.1) \qquad (ab)c = a(bc) \quad (\textit{associative law})$$

holds for all a, b, c in S, and *commutative* if

$$(1.2) \qquad ab = ba \quad (\textit{commutative law})$$

holds for all a, b in S. Our example of matrix multiplication is associative but not commutative.

When discussing groups in general, we will use multiplicative notation. It is customary to reserve additive notation $a + b$ for commutative laws of composition, that is, when $a + b = b + a$ for all a, b. Multiplicative notation carries no implication either way concerning commutativity.

In additive notation the associative law is $(a + b) + c = a + (b + c)$, and in functional notation it is

$$f(f(a,b),c) = f(a, f(b,c)).$$

This ugly formula illustrates the fact that functional notation isn't convenient for algebraic manipulation.

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

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

is a law of composition on the set $S = \text{Maps}(T, T)$ of all maps $T \longrightarrow T$.

As is true for matrix multiplication, composition of functions is an associative law. For if f, g, h are three maps from T to itself, then $(h \circ g) \circ f = h \circ (g \circ f)$:

$$\begin{tikzcd} T \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & T \arrow[r, "g"] \arrow[rr, bend left, "h \circ g"] & T \arrow[r, "h"] & T. \end{tikzcd}$$

This is clear, since both of the composed maps send $t \rightsquigarrow h(g(f(t)))$.

The simplest example is that T is a set of two elements $\{a, b\}$. Then there are four maps $T \longrightarrow T$:

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 S can be exhibited in a *multiplication table* as follows:

(1.3)
$$\begin{array}{c|cccc} & i & \tau & \alpha & \beta \\ \hline i & i & \tau & \alpha & \beta \\ \tau & \tau & i & \beta & \alpha \\ \alpha & \alpha & \alpha & \alpha & \alpha \\ \beta & \beta & \beta & \beta & \beta \end{array}$$

which is to be read in this way:

$$\begin{array}{c|c} & \cdots\cdot\ v\ \cdot\cdot \\ \hline \vdots & \vdots \\ u & \cdots\cdot\ u \circ v \\ \vdots & \end{array}$$

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

Going back to a general law of composition, suppose we want to define the product of a string of n elements of a set:

$$a_1 a_2 \cdots a_n = ?$$

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 $a_1 a_2$, then multiply this element by a_3, and so on:

$$((a_1 a_2) a_3) a_4 \cdots .$$

When $n = 4$, there are four other ways to combine the same elements; $(a_1 a_2)(a_3 a_4)$ is one of them. It can be proved by induction that if the law is *associative*, then all such products are equal. This allows us to speak of the product of an arbitrary string of elements.

(1.4) **Proposition.** Suppose an associative law of composition is 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 (we denote it 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 between 1 and n, $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$.

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

Proof. We use induction on n. The product is defined by (i) and (ii) for $n \le 2$, and it does satisfy (iii) when $n = 2$. Suppose that we know how to define the product of r elements when $r \le n - 1$, and that this product 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 it exists, the product is unique. We must now check (iii) for $i < n - 1$:

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

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 having the property that

(1.5) $$ea = a \quad \text{and} \quad ae = a, \text{ for all } a \in S.$$

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

Both of our examples, matrix multiplication and composition of functions, have an identity. For $n \times n$ matrices it is the identity matrix I, and for Maps(T, T) it is the identity map, which carries each element of T to itself.

Often the identity is denoted by 1 if the law of composition is written multiplicatively, or by 0 if it 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 our law of composition has an identity, and let us use the symbol 1 for it. An element $a \in S$ is called *invertible* if there is another element b such that

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

As with matrix multiplication [Chapter 1 (1.17)], it follows from the associative law that the inverse is unique if it exists. It is denoted by a^{-1} :

$$aa^{-1} = a^{-1}a = 1.$$

Inverses multiply in the opposite order:

(1.6) $$(ab)^{-1} = b^{-1}a^{-1}.$$

The proof is the same as for matrices [Chapter 1 (1.18)].

Power notation may be used for an associative law of composition:

(1.7)
$$\begin{aligned} a^n &= \underbrace{a \cdots a}_{n \text{ times}} && (n \geq 1) \\ a^0 &= 1 && \text{provided the identity exists} \\ a^{-n} &= a^{-1} \cdots a^{-1} && \text{provided } a \text{ is invertible.} \end{aligned}$$

The usual rules for manipulation of powers hold:

(1.8) $$a^{r+s} = a^r a^s \quad \text{and} \quad (a^r)^s = a^{rs}.$$

It isn't advisable to introduce fraction notation

(1.9) $$\frac{b}{a}$$

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

When additive notation is used for the law of composition, the inverse is denoted by $-a$, and the power notation a^n is replaced by the notation $na = a + \cdots + a$, as with addition of real numbers.

(1.10) **Definition.** A *group* is a set G together with a law of composition which is associative and has an identity element, and such that every element of G has an inverse.

It is customary to denote the group and the set of its elements by the same symbol.

An *abelian group* is a group whose law of composition is commutative. Additive notation is often used for abelian groups. Here are some simple examples of abelian groups:

(1.11)
$\mathbb{Z}^+$: the integers, with addition;
$\mathbb{R}^+$: the real numbers, with addition;
$\mathbb{R}^\times$: the nonzero real numbers, with multiplication;
$\mathbb{C}^+$, $\mathbb{C}^\times$: the analogous groups, where the set $\mathbb{C}$ of complex numbers replaces the real numbers $\mathbb{R}$.

Here is an important property of groups:

(1.12) **Proposition.** *Cancellation Law:* Let a, b, c be elements of a group G. If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.

Proof. Multiply both sides of $ab = ac$ by a^{-1} on the left: $b = a^{-1}ab = a^{-1}ac = c$. □

Multiplication by a^{-1} in this proof is not a trick; it is essential. If an element a is not invertible, the cancellation law need not hold. For instance, $0 \cdot 1 = 0 \cdot 2$, or

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

The two most basic examples of groups are obtained from the examples of laws of composition that we have considered—multiplication of matrices and composition of functions—by leaving out the elements which are not invertible. As we remarked in Chapter 1, the $n \times n$ *general linear group* is the group of all invertible $n \times n$ matrices. It is denoted by

$$(1.13) \qquad GL_n = \{n \times n \text{ matrices } A \text{ with } \det A \neq 0\}.$$

If we want to indicate that we are working with real or complex matrices, we write

$$GL_n(\mathbb{R}) \quad \text{or} \quad GL_n(\mathbb{C}),$$

according to the case.

In the set $S = \text{Maps}(T, T)$ of functions, a map $f: T \longrightarrow T$ has an inverse function if and only if it is bijective. Such a map is also called a *permutation* of T. The set of permutations forms a group. In Example (1.3), the invertible elements are i and τ, and they form a group with two elements. These two elements are the permutations of the set $\{a, b\}$.

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

$$(1.14) \qquad S_n = \text{group of permutations of } \{\mathbf{1}, \ldots, \mathbf{n}\}.$$

Because there are $n!$ permutations of a set of n elements, this group contains $n!$ elements. (We say that the *order* of the group is $n!$.) The symmetric group S_2 consists of the two elements i and τ, where i denotes the identity permutation and τ denotes the transposition which interchanges $\mathbf{1}, \mathbf{2}$ as in (1.3). The group law, composition of functions, is described by the fact that i is the identity element and by the relation $\tau\tau = \tau^2 = i$.

The structure of S_n becomes complicated very rapidly as n increases, but we can work out the case $n = 3$ fairly easily. The symmetric group S_3 contains six elements. It will be an important example for us because it is the smallest group whose law of composition is not commutative. To describe this group, we pick two particular permutations x, y in terms of which we can write all others. Let us take for x the cyclic permutation of the indices. It is represented by matrix (4.3) from Chapter 1:

$$(1.15) \qquad x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

For y, we take the transposition which interchanges **1**, **2**, fixing **3**:

$$y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{1.16}$$

The six permutations of $\{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$ are

$$\{1, x, x^2, y, xy, x^2y\} = \{x^iy^j \mid 0 \le i \le 2, 0 \le j \le 1\}, \tag{1.17}$$

where 1 denotes the identity permutation. This can be verified by computing the products.

The rules

$$x^3 = 1, y^2 = 1, yx = x^2y \tag{1.18}$$

can also be verified directly. They suffice for computation in the group S_3. Any product of the elements x,y and of their inverses, such as $x^{-1}y^3x^2y$ for instance, can be brought into the form x^iy^j with $0 \le i \le 2$ and $0 \le j \le 1$ by applying the above rules repeatedly. To do so, we move all occurrences of y to the right side using the last relation and bring the exponents into the indicated ranges using the first two relations:

$$x^{-1}y^3x^2y = x^2yx^2y = x^2(yx)xy = x^2x^2yxy = \cdots = x^6y^2 = 1.$$

Therefore one can write out a complete multiplication table for S_3 with the aid of these rules. Because of this, the rules are called *defining relations* for the group, a concept which we will study formally in Chapter 6.

Note that the commutative law does not hold in S_3, because $yx \neq xy$.

2. SUBGROUPS

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

(2.1) (a) *Closure:* If $a \in H$ and $b \in H$, then $ab \in H$.

(b) *Identity:* $1 \in H$.

(c) *Inverses:* If $a \in H$, then $a^{-1} \in H$.

These conditions are explained as follows: The first condition (a) tells us that the law of composition on the group G can be used to define a law on H, called the *induced law of composition*. The second and third conditions (b, c) say that H is a group with respect to this induced law. Notice that (2.1) mentions all parts of the definition of a group except for the associative law. We do not need to mention associativity. It carries over automatically from G to H.

Every group has two obvious subgroups: the whole group and the subgroup $\{1\}$ consisting of the identity element alone. A subgroup is said to be a *proper subgroup* if it is not one of these two.

Here are two examples of subgroups:

(2.2) **Examples.**

(a) The set T of invertible upper triangular 2×2 matrices

$$\begin{bmatrix} a & b \\ & d \end{bmatrix} \qquad (a, d \neq 0)$$

is a subgroup of the general linear group $GL_2(\mathbb{R})$.

(b) 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 $\mathbb{C}^\times$.

As a further example, we will determine the subgroups of the additive group $\mathbb{Z}^+$ of integers. Let us denote the subset of $\mathbb{Z}$ consisting of all multiples of a given integer b by $b\mathbb{Z}$:

$$b\mathbb{Z} = \{n \in \mathbb{Z} \mid n = bk \text{ for some } k \in \mathbb{Z}\}. \tag{2.3}$$

(2.4) **Proposition.** For any integer b, the subset $b\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$. Moreover, every subgroup H of $\mathbb{Z}^+$ is of the type $H = b\mathbb{Z}$ for some integer b.

Proof. We leave the verification that $b\mathbb{Z}$ is a subgroup as an exercise and proceed to show that every subgroup has this form. Let H be a subgroup of $\mathbb{Z}^+$. Remember that the law of composition on $\mathbb{Z}^+$ is addition, the identity element is 0, and the inverse of a is $-a$. So the axioms for a subgroup read

(i) if $a \in H$ and $b \in H$, then $a + b \in H$;

(ii) $0 \in H$;

(iii) if $a \in H$, then $-a \in H$.

By axiom (ii), $0 \in H$. If 0 is the only element of H, then $H = 0\mathbb{Z}$, so that case is settled. If not, there is a positive integer in H. For let $a \in H$ be any nonzero element. If a is negative, then $-a$ is positive, and axiom (iii) tells us that $-a$ is in H. We choose for b the smallest positive integer in H, and we claim that $H = b\mathbb{Z}$. We first show that $b\mathbb{Z} \subset H$, in other words, that $bk \in H$ for every integer k. If k is a positive integer, then $bk = b + b + \cdots + b$ (k terms). This element is in H by axiom (i) and induction. So is $b(-k) = -bk$, by axiom (iii). Finally, axiom (ii) tells us that $b0 = 0 \in H$.

Next we show that $H \subset b\mathbb{Z}$, that is, that every element $n \in H$ is an integer multiple of b. We use division with remainder to write $n = bq + r$, where q, r are integers and where the remainder r is in the range $0 \leq r < b$. Then n and bq are both in H, and axioms (iii) and (i) show that $r = n - bq$ is in H too. Now by our choice, b is the smallest positive integer in H, while $0 \le r < b$. Therefore $r = 0$, and $n = bq \in b\mathbb{Z}$, as required. □

The elements of the subgroup $b\mathbb{Z}$ can be described as the integers which are divisible by b. This description leads to a striking application of proposition (2.3) to subgroups which are generated by *two* integers a, b. Let us assume that a and b are not both zero. The set

(2.5) $$a\mathbb{Z} + b\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ar + bs \text{ for some integers } r, s\}$$

is a subgroup of $\mathbb{Z}^+$. It is called the subgroup *generated* by a and b, because it is the smallest subgroup which contains both of these elements. Proposition (2.3) tells us that this subgroup has the form $d\mathbb{Z}$ for some integer d, so it is the set of integers which are divisible by d. The generator d is called the *greatest common divisor* of a and b, for reasons which are explained in the following proposition:

(2.6) **Proposition.** Let a, b be integers, not both zero, and let d be the positive integer which generates the subgroup $a\mathbb{Z} + b\mathbb{Z}$. Then

(a) d can be written in the form $d = ar + bs$ for some integers r and s.
(b) d divides a and b.
(c) If an integer e divides a and b, it also divides d.

Proof. The first assertion (a) just restates the fact that d is contained in $a\mathbb{Z} + b\mathbb{Z}$. Next, notice that a and b are in the subgroup $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Therefore d divides a and b. Finally, if e is an integer which divides a and b, then a and b are in $e\mathbb{Z}$. This being so, any integer $n = ar + bs$ is also in $e\mathbb{Z}$. By assumption, d has this form, so e divides d. □

If two integers a, b are given, one way to find their greatest common divisor is to factor each of them into prime integers and then collect the common ones. Thus the greatest common divisor of $36 = 2 \cdot 2 \cdot 3 \cdot 3$ and $60 = 2 \cdot 2 \cdot 3 \cdot 5$ is $12 = 2 \cdot 2 \cdot 3$. Properties (2.6ii, iii) are easy to verify. But without proposition (2.4), the fact that the integer determined by this method has the form $ar + bs$ would not be clear at all. (In our example, $12 = 36 \cdot 2 - 60 \cdot 1$.) We will discuss the applications of this fact to arithmetic in Chapter 11.

We now come 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 powers of x:

(2.7) $$H = \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, \ldots\}.$$

It is a subgroup of G—the smallest subgroup which contains x. But to interpret (2.7) correctly, we must remember that x^n is a notation for a certain element of G. It may happen that there are repetitions in the list. For example, if $x = 1$, then all elements in the list are equal to 1. We may distinguish two possibilities: Either the powers of

x are all distinct elements, or they are not. In the first case, the group H is called *infinite cyclic*.

Suppose we have the second case, so that two powers are equal, say $x^n = x^m$, where $n > m$. Then $x^{n-m} = 1$ [Cancellation Law (1.12)], and so there is a nonzero power of x which is equal to 1.

(2.8) **Lemma.** The set S of integers n such that $x^n = 1$ is a subgroup of $\mathbb{Z}^+$.

Proof. If $x^m = 1$ and $x^n = 1$, then $x^{m+n} = x^m x^n = 1$ too. This shows that $m + n \in S$ if $m, n \in S$. So axiom (i) for a subgroup is verified. Also, axiom (ii) holds because $x^0 = 1$. Finally, if $x^n = 1$, then $x^{-n} = x^n x^{-n} = x^0 = 1$. Thus $-n \in S$ if $n \in S$. □

It follows from Lemma (2.8) and Proposition (2.4) that $S = m\mathbb{Z}$, where m is the smallest positive integer such that $x^m = 1$. The m elements $1, x, \ldots, x^{m-1}$ are all different. (If $x^i = x^j$ with $0 \le i < j < m$, then $x^{j-i} = 1$. But $j - i < m$, so this is impossible.) Moreover, any power x^n is equal to one of them: By division with remainder, we may write $n = mq + r$ with remainder r less than m. Then $x^n = (x^m)^q x^r = x^r$. Thus H consists of the following m elements:

(2.9) $$H = \{1, x, \ldots, x^{m-1}\}, \textit{ these powers are distinct, and } x^m = 1.$$

Such a group is called a *cyclic group of order m*.

The *order* of any group G is the number of its elements. We will often denote the order by

(2.10) $$|G| = \textit{number of elements of } G.$$

Of course, the order may be infinite.

An element of a group is said to have *order m* (possibly infinity) if the cyclic subgroup it generates has order m. This means that m is the smallest positive integer with the property $x^m = 1$ or, if the order is infinite, that $x^m \neq 1$ for all $m \neq 0$.

For example, the matrix $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ is an element of order 6 in $GL_2(\mathbb{R})$, so the cyclic subgroup it generates has order 6. On the other hand, the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order, because

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

We may also speak of the subgroup of a group G *generated by a subset U*. This is the smallest subgroup of G containing U, and it consists of all elements of G which can be expressed as a product of a string of elements of U and of their inverses. In particular, a subset U of G is said to *generate* G if every element of G is such a product. For example, we saw in (1.17) that the set $U = \{x, y\}$ generates the symmetric group S_3. Proposition (2.18) of Chapter 1 shows that the elementary matrices generate GL_n.

The *Klein four group* V is the simplest group which is not cyclic. It will appear in many forms. For instance, it can be realized as the group consisting of the four matrices

$$\begin{bmatrix} \pm 1 & \\ & \pm 1 \end{bmatrix}. \tag{2.11}$$

Any two elements different from the identity generate V.

The *quaternion group* H is another example of a small subgroup of $GL_2(\mathbb{C})$ which is not cyclic. It consists of the eight matrices

$$H = \{\pm \mathbf{1}, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}, \tag{2.12}$$

where

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

The two elements $\mathbf{i}, \mathbf{j}$ generate H, and computation leads to the formulas

$$\mathbf{i}^4 = 1, \quad \mathbf{i}^2 = \mathbf{j}^2, \mathbf{ji} = \mathbf{i}^3\mathbf{j}. \tag{2.13}$$

These products determine the multiplication table of H.

3. ISOMORPHISMS

Let G and G' be two groups. We want to say that they are *isomorphic* if all properties of the group structure of G hold for G' as well, and conversely. For example, let G be the set of real matrices of the form

$$\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}.$$

This is a subgroup of $GL_2(\mathbb{R})$, and the product of two such matrices is

$$\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}\begin{bmatrix} 1 & y \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ & 1 \end{bmatrix}.$$

The upper right entries of the matrices add when the matrices are multiplied, the rest of the matrix being fixed. So when computing with such matrices, we need to keep track of only the upper right entry. This fact is expressed formally by saying that the group G is isomorphic to the additive group of real numbers.

How to make the concept of isomorphism precise will not be immediately clear, but it turns out that the right way is to relate two groups by a *bijective correspondence* between their elements, *compatible with the laws of composition,* that is, a correspondence

$$G \longleftrightarrow G' \tag{3.1}$$

having this property: If $a, b \in G$ correspond to $a', b' \in G'$, then the product ab in G corresponds to the product $a'b'$ in G'. When this happens, all properties of the group structure carry over from one group to the other.

For example, the identity elements in isomorphic groups G and G' correspond. To see this, say that the identity element 1 of G corresponds to an element ϵ' in G'. Let a' be an arbitrary element of G', and let a be the corresponding element of G. By assumption, products correspond to products. Since $1a = a$ in G, it follows that $\epsilon'a' = a'$ in G'. In this way, one shows that $\epsilon' = 1'$. Another example: The orders of corresponding elements are equal. If a corresponds to a' in G', then, since the correspondence is compatible with multiplication, $a^r = 1$ if and only if $a'^r = 1'$.

Since two isomorphic groups have the same properties, it is often convenient to identify them with each other when speaking informally. For example, the symmetric group S_n of permutations of $\{\mathbf{1},\ldots,\mathbf{n}\}$ is isomorphic to the group of permutation matrices, a subgroup of $GL_n(\mathbb{R})$, and we often blur the distinction between these two groups.

We usually write the correspondence (3.1) asymmetrically as a function, or map $\varphi: G \longrightarrow G'$. Thus an *isomorphism* φ *from* G *to* G' is a bijective map which is compatible with the laws of composition. If we write out what this compatibility means using function notation for φ, we get the condition

$$(3.2) \qquad \varphi(ab) = \varphi(a)\varphi(b), \text{ for all } a, b \in G.$$

The left side of this equality means to multiply a and b in G and then apply φ, while on the right the elements $\varphi(a)$ and $\varphi(b)$, which we denoted by a', b' before, are multiplied in G'. We could also write this condition as

$$(ab)' = a'b'.$$

Of course, the choice of G as domain for this isomorphism is arbitrary. The inverse function $\varphi^{-1}: G' \longrightarrow G$ would serve just as well.

Two groups G and G' are called *isomorphic* if there exists an isomorphism $\varphi: G \longrightarrow G'$. We will sometimes indicate that two groups are isomorphic by the symbol $\approx$:

$$(3.3) \qquad G \approx G' \textit{ means } G \textit{ is isomorphic to } G'.$$

For example, let $C = \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$ be an infinite cyclic group. Then the map

$$\varphi: \mathbb{Z}^+ \longrightarrow C$$

defined by $\varphi(n) = a^n$ is an isomorphism. Since the notation is additive in the domain and multiplicative in the range, condition (3.2) translates in this case to $\varphi(m + n) = \varphi(m)\varphi(n)$, or

$$a^{m+n} = a^m a^n.$$

One more simple example:
Let $G = \{1, x, x^2, \ldots, x^{n-1}\}$ and $G' = \{1, y, y^2, \ldots, y^{n-1}\}$ be two cyclic groups, generated by elements x, y of the same order. Then the map which sends x^i to y^i is an isomorphism: Two cyclic groups of the same order are isomorphic.

Recapitulating, two groups G and G' are isomorphic if there exists an isomorphism $\varphi: G \longrightarrow G'$, a bijective map compatible with the laws of composition. The groups isomorphic to a given group G form what is called the *isomorphism class* of G, and any two groups in an isomorphism class are isomorphic. When one speaks of *classifying* groups, what is meant is to describe the isomorphism classes. This is too hard to do for all groups, but we will see later that there is, for example, one isomorphism class of groups of order 3 [see (6.13)], and that there are two classes of groups of order 4 and five classes of groups of order 12 [Chapter 6 (5.1)].

A confusing point about isomorphisms is that there exist isomorphisms from a group G to itself:

$$\varphi: G \longrightarrow G.$$

Such an isomorphism is called an *automorphism* of G. The identity map is an automorphism, of course, but there are nearly always other automorphisms as well. For example, let $G = \{1, x, x^2\}$ be a cyclic group of order 3, so that $x^3 = 1$. The transposition which interchanges x and x^2 is an automorphism of G:

$$\begin{aligned} 1 &\rightsquigarrow 1 \\ x &\rightsquigarrow x^2 \\ x^2 &\rightsquigarrow x. \end{aligned}$$

This is because x^2 is another element of order 3 in the group. If we call this element y, the cyclic subgroup $\{1, y, y^2\}$ generated by y is the whole group G, because $y^2 = x$. The automorphism compares the two realizations of G as a cyclic group.

The most important example of automorphism is conjugation: Let $b \in G$ be a fixed element. Then *conjugation by b* is the map φ from G to itself defined by

(3.4)
$$\varphi(x) = bxb^{-1}.$$

This is an automorphism because, first of all, it is compatible with multiplication in the group:

$$\varphi(xy) = bxyb^{-1} = bxb^{-1}byb^{-1} = \varphi(x)\varphi(y),$$

and, secondly, it is a bijective map since it has an inverse function, namely conjugation by b^{-1}. If the group is abelian, then conjugation is the identity map: $bab^{-1} = abb^{-1} = a$. But any noncommutative group has some nontrivial conjugations, and so it has nontrivial automorphisms.

The element bab^{-1} is called the *conjugate* of a by b and will appear often. Two elements a, a' of a group G are called *conjugate* if $a' = bab^{-1}$ for some $b \in G$. The conjugate behaves in much the same way as the element a itself; for example, it has the same order in the group. This follows from the fact that it is the image of a by an automorphism.

The conjugate has a useful, though trivial, interpretation. Namely, if we denote bab^{-1} by a', then

(3.5) $$ba = a'b.$$

So we can think of conjugation by b as the change in a which results when one moves b from one side to the other.

4. HOMOMORPHISMS

Let G, G' be groups. A *homomorphism* $\varphi: G \longrightarrow G'$ is any map satisfying the rule

(4.1) $$\varphi(ab) = \varphi(a)\varphi(b),$$

for all $a, b \in G$. This is the same requirement as for an isomorphism [see (3.2)]. The difference is that φ is not assumed to be bijective here.

(4.2) **Examples.** The following maps are homomorphisms:

(a) the determinant function det: $GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$;
(b) the sign of a permutation sign: $S_n \longrightarrow \{\pm 1\}$ [see Chapter 1 (4.9)];
(c) the map φ: $\mathbb{Z}^+ \longrightarrow G$ defined by $\varphi(n) = a^n$, where a is a fixed element of G;
(d) the *inclusion map* i: $H \longrightarrow G$ of a subgroup H into a group G, defined by $i(x) = x$.

(4.3) **Proposition.** A group homomorphism $\varphi: G \longrightarrow G'$ carries the identity to the identity, and inverses to inverses. In other words, $\varphi(1_G) = 1_{G'}$, and $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof. Since $1 = 1 \cdot 1$ and since φ is a homomorphism, $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$. Cancel $\varphi(1)$ from both sides by (1.12): $1 = \varphi(1)$. Next, $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1) = 1$, and similarly $\varphi(a)\varphi(a^{-1}) = 1$. Hence $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Every group homomorphism φ determines two important subgroups: its image and its kernel. The *image* of a homomorphism $\varphi: G \longrightarrow G'$ is easy to understand. It is the image of the map

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

and it is a subgroup of G'. Another notation for the image is $\varphi(G)$. In Examples (4.2a,b), the image is equal to the range of the map, but in example (4.2c) it is the cyclic subgroup of G generated by a, and in Example (4.2d) it is the subgroup H.

The *kernel* of φ is more subtle. It is the set of elements of G which are mapped to the identity in G':

(4.5) $$\ker \varphi = \{a \in G \mid \varphi(a) = 1\},$$

which can also be described as the inverse image $\varphi^{-1}(1)$ of the identity element [see Appendix (1.5)]. The kernel is a subgroup of G, because if a and b are in ker φ, then $\varphi(ab) = \varphi(a)\varphi(b) = 1 \cdot 1 = 1$, hence $ab \in \ker \varphi$, and so on.

The kernel of the determinant homomorphism is the subgroup of matrices whose determinant is 1. This subgroup is called the *special linear group* and is denoted by $SL_n(\mathbb{R})$:

$$SL_n(\mathbb{R}) = \{\text{real } n \times n \text{ matrices } A \mid \det A = 1\}, \tag{4.6}$$

a subgroup of $GL_n(\mathbb{R})$. The kernel of the sign homomorphism in Example (4.2b) above is called the *alternating group* and is denoted by A_n:

$$A_n = \{\text{even permutations}\}, \tag{4.7}$$

a subgroup of S_n. The kernel of the homomorphism (4.2d) is the set of integers n such that $a^n = 1$. That this is a subgroup of $\mathbb{Z}^+$ was proved before, in (2.8).

In addition to being a subgroup, the kernel of a homomorphism has an extra property which is subtle but very important. Namely, if a is in ker φ and b is any element of the group G, then the conjugate bab^{-1} is in ker φ. For to say $a \in \ker \varphi$ means $\varphi(a) = 1$. Then

$$\varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b^{-1}) = \varphi(b)1\varphi(b)^{-1} = 1,$$

so $bab^{-1} \in \ker \varphi$ too.

(4.8) **Definition.** A subgroup N of a group G is called a *normal subgroup* if it has the following property: For every $a \in N$ and every $b \in G$, the conjugate bab^{-1} is in N.

As we have just seen,

(4.9) *The kernel of a homomorphism is a normal subgroup.*

Thus $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$, and A_n is a normal subgroup of S_n.

Any subgroup of an abelian group G is normal, because when G is abelian, $bab^{-1} = a$. But subgroups need not be normal in nonabelian groups. For example, group T of invertible upper triangular matrices is not a normal subgroup of $GL_2(\mathbb{R})$. For let $A = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ and $B = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$. Then $BAB^{-1} = \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$. Here $A \in T$ and $B \in GL_2(\mathbb{R})$, but $BAB^{-1} \not\in T$.

The *center* of a group G, sometimes denoted by Z or by $Z(G)$, is the set of elements which commute with every element of G:

$$Z = \{z \in G \mid zx = xz \text{ for all } x \in G\}. \tag{4.10}$$

The center of any group is a normal subgroup of the group. For example, it can be shown that the center of $GL_n(\mathbb{R})$ is the group of *scalar matrices*, that is, those of the form cI.

5. EQUIVALENCE RELATIONS AND PARTITIONS

A fundamental mathematical construction is to start with a set S and to form a new set by equating certain elements of S according to a given rule. For instance, we may divide the set of integers into two classes, the even integers and the odd integers. Or we may wish to view congruent triangles in the plane as equivalent geometric objects. This very general procedure arises in several ways, which we will discuss here.

Let S be a set. By a *partition* P of S, we mean a subdivision of S into nonoverlapping subsets:

$$S = \text{union of disjoint, nonempty subsets.} \tag{5.1}$$

For example, the sets

$$\{1,3\}, \{2,5\}, \{4\}$$

form a partition of the set $\{1,2,3,4,5\}$. The two sets, of even integers and of odd integers, form a partition of the set $\mathbb{Z}$ of all integers.

An *equivalence relation* on S is a relation which holds between certain elements of S. We often write it as $a \sim b$ and speak of it as *equivalence* of a and b.

(5.2) An equivalence relation is required to be:

(i) *transitive:* If $a \sim b$ and $b \sim c$, then $a \sim c$;

(ii) *symmetric:* If $a \sim b$, then $b \sim a$;

(iii) *reflexive:* $a \sim a$ for all $a \in S$.

Congruence of triangles is an example of an equivalence relation on the set S of triangles in the plane.

Formally, a relation on S is the same thing as a subset R of the set $S \times S$ of pairs of elements; namely, the subset R consists of pairs (a,b) such that $a \sim b$. In terms of this subset, we can write the axioms for an equivalence relation as follows: (i) if $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$; (ii) if $(a,b) \in R$, then $(b,a) \in R$; and (iii) $(a,a) \in R$ for all a.

The notions of a partition of S and an equivalence relation on S are logically equivalent, though in practice one is often presented with just one of the two. Given a partition P on S, we can define an equivalence relation R by the rule $a \sim b$ if a and b lie in the same subset of the partition. Axioms (5.2) are obviously satisfied. Conversely, given an equivalence relation R, we can define a partition P this way: The subset containing a is the set of all elements b such that $a \sim b$. This subset is called the *equivalence class* of a, and S is partitioned into equivalence classes.

Let us check that the equivalence classes partition the set S. Call C_a the equivalence class of an element $a \in S$. So C_a consists of the elements b such that $a \sim b$:

$$C_a = \{b \in S \mid a \sim b\}. \tag{5.3}$$

The reflexive axiom tells us that $a \in C_a$. Therefore the classes C_a are nonempty, and since a can be any element, the classes cover S. The remaining property of a partition which must be verified is that equivalence classes do not overlap. It is easy to become confused here, because if $a \sim b$ then by definition $b \in C_a$. But $b \in C_b$ too. Doesn't this show that C_a and C_b overlap? We must remember that the symbol C_a is our notation for a subset of S defined in a certain way. The partition consists of the subsets, not of the notations. It is true that C_a and C_b have the element b in common, but that is all right because these are two notations for the same set. We will show the following:

(5.4) *Suppose that C_a and C_b have an element d in common. Then $C_a = C_b$.*

Let us first show that if $a \sim b$ then $C_a = C_b$. To do so, let x be an arbitrary element of C_b. Then $b \sim x$. Since $a \sim b$, transitivity shows that $a \sim x$, hence that $x \in C_a$. Therefore $C_b \subset C_a$. The opposite inclusion follows from interchanging the roles of a and b. To prove (5.4), suppose that d is in C_a and in C_b; then $a \sim d$ and $b \sim d$. Then by what has been shown, $C_a = C_d = C_b$, as required. □

Suppose that an equivalence relation or a partition is given on a set S. Then we may construct a new set $\overline{S}$ whose elements are the equivalence classes or the subsets making up the partition. To simplify notation, the equivalence class of a, or the subset of the partition containing a, is often denoted by $\overline{a}$. Thus $\overline{a}$ is an element of $\overline{S}$.

Notice that there is a natural surjective map

(5.5)
$$S \longrightarrow \overline{S}, \text{ which sends}$$
$$a \rightsquigarrow \overline{a}.$$

In our original example of the partition of $S = \mathbb{Z}$, the set $\overline{S}$ contains the two elements (*Even*), (*Odd*), where the symbol (*Even*) represents the set of even integers and (*Odd*) the set of odd integers. And $\overline{0} = \overline{2} = \overline{4}$ and so on. So we can denote the set (*Even*) by any one of these symbols. The map

(5.6)
$$\mathbb{Z} \longrightarrow \{(Even), (Odd)\}$$

is the obvious one.

There are two ways to think of this construction. We can imagine putting the elements of S into separate piles, one for each subset of the partition, and then regarding the piles as the elements of a new set $\overline{S}$. The map $S \longrightarrow \overline{S}$ associates each element with its pile. Or we can think of changing what we mean by equality among elements of S, interpreting $a \sim b$ to mean $a = b$ in $\overline{S}$. With this way of looking at it, the elements in the two sets S and $\overline{S}$ correspond, but in $\overline{S}$ more of them are equal to each other. It seems to me that this is the way we treat congruent triangles in school. The bar notation (5.5) is well suited to this intuitive picture. We can work with the same symbols as in S, but with bars over them to remind us of the new rule:

(5.7)
$$\overline{a} = \overline{b} \textit{ means } a \sim b.$$

This notation is often very convenient.

A disadvantage of the bar notation is that many symbols represent the same element of $\overline{S}$. Sometimes this disadvantage can be overcome by choosing once and for all a particular element, or a *representative,* in each equivalence class. For example, it is customary to represent $(Even)$ by $\overline{0}$ and (Odd) by $\overline{1}$:

(5.8) $$\{(Even), (Odd)\} = \{\overline{0},\overline{1}\}.$$

Though the pile picture is more immediate, the second way of viewing $\overline{S}$ is often the better one, because operations on the piles are clumsy to visualize, whereas the bar notation is well suited to algebraic manipulation.

Any map of sets $\varphi: S \longrightarrow T$ defines an equivalence relation on the domain S, namely the relation given by the rule $a \sim b$ if $\varphi(a) = \varphi(b)$. We will refer to this as *the equivalence relation determined by the map.* The corresponding partition is made up of the nonempty inverse images of the elements of T. By definition, the *inverse image* of an element $t \in T$ is the subset of S consisting of all elements s such that $\varphi(s) = t$. It is denoted symbolically as

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

Thus $\varphi^{-1}(t)$ is a subset of the domain S, determined by the element $t \in T$. (This is symbolic notation. Please remember that φ^{-1} is usually not a function.) The inverse images may also be called the *fibres* of the map φ. The fibres $\varphi^{-1}(t)$ which are *nonempty,* which means t is in the image of φ, form a partition of S. Here the set $\overline{S}$ of equivalence classes, which is the set of nonempty fibres, has another incarnation, as the image im φ of the map. Namely, there is a bijective map

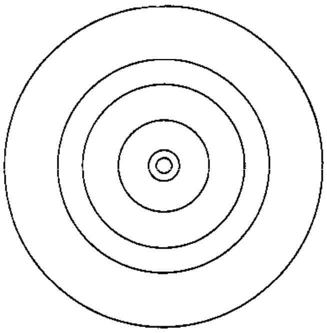
(5.10) $$\overline{\varphi}: \overline{S} \longrightarrow \operatorname{im} \varphi,$$

the map which sends an element $\overline{s}$ of $\overline{S}$ to $\varphi(s)$.

We now go back to group homomorphisms. Let $\varphi: G \longrightarrow G'$ be a homomorphism, and let us analyze the equivalence relation on G which is associated to the map φ or, equivalently, the fibres of the homomorphism. This relation is usually denoted by $\equiv$, rather than by $\sim$, and is referred to as *congruence:*

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

For example, let $\varphi: \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$ be the absolute value homomorphism defined by $\varphi(a) = |a|$. The induced equivalence relation is $a \equiv b$ if $|a| = |b|$. The fibres of this map are the concentric circles about 0. They are in bijective correspondence with elements of im φ, the set of positive reals.



(5.12) **Figure.** Fibres of the absolute value map $\mathbb{C}^\times \longrightarrow \mathbb{R}^\times$.

The relation (5.11) can be rewritten in a number of ways, of which the following will be the most important for us:

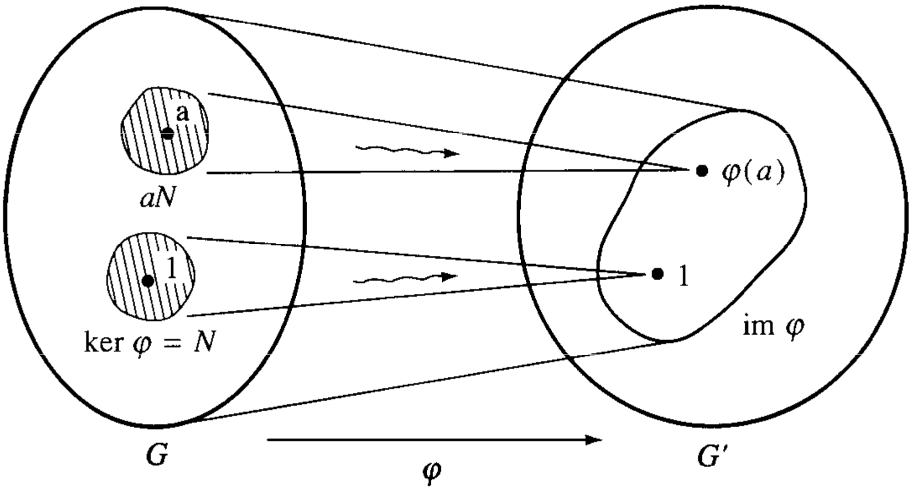
(5.13) **Proposition.** Let φ: $G \longrightarrow G'$ be a group homomorphism with kernel N, and let a, b be elements of G. Then $\varphi(a) = \varphi(b)$ if and only if $b = an$ for some element $n \in N$, or equivalently, if $a^{-1}b \in N$.

Proof. Suppose that $\varphi(a) = \varphi(b)$. Then $\varphi(a)^{-1}\varphi(b) = 1$, and since φ is a homomorphism we can use (4.1) and (4.3) to rewrite this equality as $\varphi(a^{-1}b) = 1$. Now by definition, the kernel N is the set of all elements $x \in G$ such that $\varphi(x) = 1$. Thus $a^{-1}b \in N$, or $a^{-1}b = n$ for some $n \in N$. Hence $b = an$, as required. Conversely, if $b = an$ and $n \in N$, then $\varphi(b) = \varphi(a)\varphi(n) = \varphi(a)1 = \varphi(a)$. □

The set of elements of the form an is denoted by aN and is called a *coset* of N in G:

(5.14) $$aN = \{g \in G \mid g = an \text{ for some } n \in N\}.$$

So the coset aN is the set of all group elements b which are congruent to a. The congruence relation $a \equiv b$ partitions the group G into *congruence classes*, the cosets aN. They are the fibres of the map φ. In particular, the circles about the origin depicted in (5.12) are cosets of the absolute value homomorphism.



(5.15) **Figure.** A schematic diagram of a group homomorphism.

An important case to look at is when the kernel is the trivial subgroup. In that case (5.13) reads as follows:

(5.16) **Corollary.** A group homomorphism φ: $G \longrightarrow G'$ is injective if and only if its kernel is the trivial subgroup $\{1\}$. □

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

6. COSETS

One can define cosets for any subgroup H of a group G, not only for the kernel of a homomorphism. A *left coset* is a subset of the form

$$aH = \{ah \mid h \in H\}. \tag{6.1}$$

Note that the subgroup H is itself a coset, because $H = 1H$.

The cosets are equivalence classes for the *congruence* relation

$$a \equiv b \text{ if } b = ah, \text{ for some } h \in H. \tag{6.2}$$

Let us 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 $h,h' \in H$. Therefore $c = ahh'$. Since H is a subgroup, $hh' \in H$. Thus $a \equiv c$. *Symmetry:* Suppose $a \equiv b$, so that $b = ah$. Then $a = bh^{-1}$ and $h^{-1} \in H$, and so $b \equiv a$. *Reflexivity:* $a = a1$ and $1 \in H$, so $a \equiv a$. Note that we have made use of all the defining properties of a subgroup.

Since equivalence classes form a partition, we find the following:

(6.3) **Corollary.** The left cosets of a subgroup partition the group. □

(6.4) **Note.** The notation aH defines a certain subset of G. As with any equivalence relation, different notations may represent the same subset. In fact, we know that aH is the unique coset containing a, and so

$$aH = bH \textit{ if and only if } a \equiv b. \tag{6.5}$$

The corollary just restates (5.4):

(6.6) *If aH and bH have an element in common, then they are equal.*

For example, let G be the symmetric group S_3, with the presentation given in (1.18): $G = \{1, x, x^2, y, xy, x^2y\}$. The element xy has order 2, and so it generates a cyclic subgroup $H = \{1, xy\}$ of order 2. The left cosets of H in G are the three sets

$$\{1, xy\} = H = xyH, \quad \{x, x^2y\} = xH = x^2yH, \quad \{x^2y\} = x^2H = yH. \tag{6.7}$$

Notice that they do partition the group.

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

$$[G : H]. \tag{6.8}$$

Thus in our example the index is 3. Of course if G contains infinitely many elements, the index may be infinite too.

Note that there is a bijective map from the subgroup H to the coset aH, sending $h \rightsquigarrow ah$. (Why is this a bijective map?) Thus

(6.9) *Each coset aH has the same number of elements as H does.*

Since G is the union of the cosets of H and since these cosets do not overlap, we obtain the important *Counting Formula*

(6.10) $$|G| = |H|[G : H],$$

where $|G|$ denotes the order of the group, as in (2.10), and where the equality has the obvious meaning if some terms are infinite. In our example (6.7), this formula reads $6 = 2 \cdot 3$.

The fact that the two terms on the right side of equation (6.10) must divide the left side is very important. Here is one of these conclusions, stated formally:

(6.11) **Corollary.** *Lagrange's Theorem:* Let G be a finite group, and let H be a subgroup of G. The order of H divides the order of G. □

In Section 2 we defined the order of an element $a \in G$ to be the order of the cyclic subgroup generated by a. Hence Lagrange's Theorem implies the following:

(6.12) *The order of an element divides the order of the group.*

This fact has a remarkable consequence:

(6.13) **Corollary.** Suppose that a group G has p elements and that p is a prime integer. Let $a \in G$ be any element, not the identity. Then G is the cyclic group $\{1, a, \dots, a^{p-1}\}$ generated by a.

For, since $a \neq 1$, the order of a is greater than 1, and it divides $|G| = p$. Hence it is equal to p. Since G has order p, $\{1, a, \dots, a^{p-1}\}$ is the whole group. □

Thus we have classified all groups of prime order p. They form one isomorphism class, the class of a cyclic group of order p.

The Counting Formula can also be applied when a homomorphism is given. Let $\varphi: G \longrightarrow G'$ be a homomorphism. As we saw in (5.13), the left cosets of $\ker \varphi$ are the fibres of the map φ. They are in bijective correspondence with the elements in the image.

(6.14) $$[G : \ker \varphi] = |\operatorname{im} \varphi|.$$

Thus (6.10) implies the following:

(6.15) **Corollary.** Let $\varphi: G \longrightarrow G'$ be a homomorphism of finite groups. Then

$$|G| = |\ker \varphi| \cdot |\operatorname{im} \varphi|.$$

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

Proof. The formula is obtained by combining (6.10) and (6.14), and it implies that $|\ker \varphi|$ and $|\operatorname{im} \varphi|$ divide $|G|$. Since $\operatorname{im} \varphi$ is a subgroup of G', $|\operatorname{im} \varphi|$ divides $|G'|$ as well. □

Let us go back for a moment 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 are the sets

$$Ha = \{ha \mid h \in H\}, \tag{6.16}$$

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

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

Right cosets need not be the same as left cosets. For instance, the right cosets of the subgroup $\{1, xy\}$ of S_3 are

$$\{1, xy\} = H = Hxy, \quad \{x, y\} = Hx = Hy, \quad \{x^2, x^2y\} = Hx^2 = Hx^2y. \tag{6.17}$$

This partition of S_3 is not the same as the partition (6.7) into left cosets.

However, if N is a normal subgroup, then right and left cosets agree.

(6.18) **Proposition.** A subgroup H of a group G is normal if and only if every left coset is also a right coset. If H is normal, then $aH = Ha$ for every $a \in G$.

Proof. Suppose that H is normal. For any $h \in H$ and any $a \in G$,

$$ah = (aha^{-1})a.$$

Since H is a normal subgroup, the conjugate element $k = aha^{-1}$ is in H. Thus the element $ah = ka$ is in aH and also in Ha. This shows that $aH \subset Ha$. Similarly, $aH \supset Ha$, and so these two cosets are equal. Conversely, suppose that H is not normal. Then there are elements $h \in H$ and $a \in G$ so that aha^{-1} is not in H. Then ah is in the left coset aH but not in the right coset Ha. If it were, say $ah = h'a$ for some $h' \in H$, then we would have $aha^{-1} = h' \in H$, contrary to our hypothesis. On the other hand, aH and Ha do have an element in common, namely the element a. So aH can't be in some other right coset. This shows that the partition into left cosets is not the same as the partition into right cosets. □

7. *RESTRICTION OF A HOMOMORPHISM TO A SUBGROUP*

The usual way to get an understanding of a complicated group is to study some less complicated subgroups. If it made sense to single out one method in group theory as the most important, this would be it. For example, the general linear group GL_2 is much more complicated than the group of invertible upper triangular matrices. We expect to answer any question about upper triangular matrices which comes up. And by taking products of upper and lower triangular matrices, we can cover most of the group GL_2. Of course, the trick is to get back information about a group from an understanding of its subgroups. We don't have general rules about how this should be done. But whenever a new construction with groups is made, we should study its effect on subgroups. This is what is meant by *restriction to a subgroup*. We will do this for subgroups and homomorphisms in this section.

Let H be a subgroup of a group G. Let us first consider the case that a second subgroup K is given. The restriction of K to H is the intersection $K \cap H$. The following proposition is a simple exercise.

(7.1) **Proposition.** The intersection $K \cap H$ of two subgroups is a subgroup of H. If K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H. □

There is not very much more to be said here, but if G is a finite group, we may be able to apply the Counting Formula (6.10), especially Lagrange's Theorem, to get information about the intersection. Namely, $K \cap H$ is a subgroup of H and also a subgroup of K. So its order divides both of the orders $|H|$ and $|K|$. If $|H|$ and $|K|$ have no common factor, we can conclude that $K \cap H = \{1\}$.

Now suppose that a homomorphism $\varphi: G \longrightarrow G'$ is given and that H is a subgroup of G as before. Then we may *restrict* φ *to* H, obtaining a homomorphism

$$\varphi|_H: H \longrightarrow G'. \tag{7.2}$$

This means that we take the same map φ but restrict its domain to H. In other words, $\varphi|_H(h) = \varphi(h)$ for all $h \in H$. The restriction is a homomorphism because φ is one.

The kernel of $\varphi|_H$ is the intersection of ker φ with H :

$$\ker \varphi|_H = (\ker \varphi) \cap H. \tag{7.3}$$

This is clear from the definition of kernel: $\varphi(h) = 1$ if and only if $h \in \ker \varphi$.

Again, the Counting Formula may help to describe this restriction. For, the image of $\varphi|_H$ is $\varphi(H)$. According to Corollary (6.15), $|\varphi(H)|$ divides both $|H|$ and $|G'|$. So if $|H|$ and $|G'|$ have no common factor, $\varphi(H) = \{1\}$. Then we can conclude that $H \subset \ker \varphi$.

For example, the sign of a permutation is described by a homomorphism (4.2b), $S_n \longrightarrow \{\pm 1\}$. The range of this homomorphism has order 2, and its kernel is the alternating group. If a subgroup H of S_n has odd order, then the restriction of this homomorphism to H is trivial, which means that H is contained in the alternating group, that is, H consists of even permutations. This will be so when H is the cyclic subgroup generated by a permutation p whose order in the group is odd. It follows that every permutation of odd order is an even permutation. On the other hand, we can not make any conclusion about permutations of even order. They may be odd or even.

When a homomorphism $\varphi: G \longrightarrow G'$ and a subgroup H' of G' are given, we may also restrict φ to H'. Here we must cut down the domain G of φ suitably, in order to get a map to H'. The natural thing to do is to cut down the domain as little as possible by taking the entire inverse image of H':

(7.4) **Proposition.** Let $\varphi: G \longrightarrow G'$ be a homomorphism, and let H' be a subgroup of G'. Denote the inverse image $\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}$ by $\tilde{H}$. Then

(a) $\tilde{H}$ is a subgroup of G.
(b) If H' is a normal subgroup of G', then $\tilde{H}$ is a normal subgroup of G.
(c) $\tilde{H}$ contains ker φ.
(d) The restriction of φ to $\tilde{H}$ defines a homomorphism $\tilde{H} \longrightarrow H'$, whose kernel is ker φ.

For example, consider the determinant homomorphism det: $GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^{\times}$. The set P of positive real numbers is a subgroup of $\mathbb{R}^{\times}$, and its inverse image is the set of invertible $n \times n$ matrices with positive determinant, which is a normal subgroup of $GL_n(\mathbb{R})$.

Proof of Proposition (7.4). This proof is also a simple exercise, but we must keep in mind that φ^{-1} is not a map. By definition, $\tilde{H}$ is the set of elements $x \in G$ such that $\varphi(x) \in H'$. We verify the conditions for a subgroup. *Identity:* $1 \in \tilde{H}$ because $\varphi(1) = 1 \in H'$. *Closure:* Suppose that $x, y \in \tilde{H}$. This means that $\varphi(x)$ and $\varphi(y)$ are in H'. Since H' is a subgroup, $\varphi(x)\varphi(y) \in H'$. Since φ is a homomorphism, $\varphi(x)\varphi(y) = \varphi(xy) \in H'$. Therefore $xy \in \tilde{H}$. *Inverses:* Suppose $x \in \tilde{H}$, so that $\varphi(x) \in H'$; then $\varphi(x)^{-1} \in H'$ because H' is a subgroup. Since φ is a homomorphism, $\varphi(x)^{-1} = \varphi(x^{-1})$. Thus $x^{-1} \in \tilde{H}$.

Suppose that H' is a normal subgroup, and let $x \in \tilde{H}$ and $g \in G$. Then $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1}$, and $\varphi(x) \in H'$. Therefore $\varphi(gxg^{-1}) \in H'$, and this shows that $gxg^{-1} \in \tilde{H}$. Next, $\tilde{H}$ contains ker φ because if $x \in$ ker φ then $\varphi(x) = 1$, and $1 \in H'$. So $x \in \varphi^{-1}(H')$. The last assertion should be clear. □

8. PRODUCTS OF GROUPS

Let G, G' be two groups. The product set $G \times G'$ can be made into a group by component-wise multiplication. That is, we define multiplication of pairs by the rule

$$(a,a'),\ (b,b') \rightsquigarrow (ab, a'b'), \tag{8.1}$$

for $a,b \in G$ and $a',b' \in G'$. The pair $(1,1)$ is an identity, and $(a,a')^{-1} = (a^{-1}, a'^{-1})$. The associative law in $G \times G'$ follows from the fact that it holds in G and in G'. The group thus obtained is called the *product* of G and G' and is denoted by $G \times G'$. Its order is the product of the orders of G and G'.

The product group is related to the two factors G, G' in a simple way, which we can sum up in terms of some homomorphisms

$$\begin{tikzcd}
G \arrow[dr, "i"] & & G \\
& G \times G' \arrow[ur, "p"] \arrow[dr, "p'"'] & \\
G' \arrow[ur, "i'"'] & & G'
\end{tikzcd}, \tag{8.2}$$

defined by

$$i(x) = (x, 1), \quad i'(x') = (1, x'),$$

$$p(x, x') = x, \quad p'(x, x') = x'.$$

The maps i, i' are injective and may be used to identify G, G' with the subgroups $G \times 1$, $1 \times G'$ of $G \times G'$. The maps p, p' are surjective, $\ker p = 1 \times G'$, and $\ker p' = G \times 1$. These maps are called the *projections*. Being kernels, $G \times 1$ and $1 \times G'$ are *normal* subgroups of $G \times G'$.

(8.3) **Proposition.** *The mapping property of products:* Let H be any group. The homomorphisms $\Phi: H \longrightarrow G \times G'$ are in bijective correspondence with pairs (φ, φ') of homomorphisms

$$\varphi: H \longrightarrow G, \qquad \varphi': H \longrightarrow G'.$$

The kernel of Φ is the intersection $(\ker \varphi) \cap (\ker \varphi')$.

Proof. Given a pair (φ, φ') of homomorphisms, we define the corresponding homomorphism

$$\Phi: H \longrightarrow G \times G'$$

by the rule $\Phi(h) = (\varphi(h), \varphi'(h))$. This is easily seen to be a homomorphism. Conversely, given Φ, we obtain φ and φ' by composition with the projections, as

$$\varphi = p\Phi, \qquad \varphi' = p'\Phi.$$

Obviously, $\Phi(h) = (1, 1)$ if and only if $\varphi(h) = 1$ and $\varphi'(h) = 1$, which shows that $\ker \Phi = (\ker \varphi) \cap (\ker \varphi')$. □

It is clearly desirable to compose a given group G as a product, meaning to find two groups H and H' such that G is isomorphic to the product $H \times H'$. For the groups H, H' will be smaller and therefore simpler, and the relation between $H \times H'$ and its factors is easily understood. Unfortunately, it is quite rare that a given 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. This can be shown using the mapping property just discussed. Say that $C_6 = \{1, x, x^2, \ldots, x^5\}$, $C_2 = \{1, y\}$, $C_3 = \{1, z, z^2\}$. The rule

$$\varphi: C_6 \longrightarrow C_2 \times C_3$$

defined by $\varphi(x^i) = (y^i, z^i)$ is a homomorphism, and its kernel is the set of elements x^i such that $y^i = 1$ and $z^i = 1$. Now $y^i = 1$ if and only if i is divisible by 2, while $z^i = 1$ if and only if i is divisible by 3. There is no integer between 1 and 5 which is divisible by both 2 and 3. Therefore $\ker \varphi = \{1\}$, and φ is injective. Since both groups have order 6, φ is bijective and hence is an isomorphism. □

The same argument works for a *cyclic* group of order rs, whenever the two integers r and s have no common factor.

(8.4) **Proposition.** Let r, s be integers with no common factor. 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. For it is easily seen that 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. And, the proposition makes no assertions about a group which is not cyclic.

Let A and B be subsets of a group G. Then we denote the set of products of elements of A and B by

$$(8.5) \qquad AB = \{x \in G \mid x = ab \text{ for some } a \in A \text{ and } b \in B\}.$$

The next proposition characterizes product groups.

(8.6) **Proposition.** Let H and K be subgroups of a group G.

(a) If $H \cap K = \{1\}$, the product map $p: H \times K \longrightarrow G$ defined by $p(h,k) = hk$ is injective. Its image is the subset HK.

(b) If either H or K is a normal subgroup of G, then the product sets HK and KH are equal, and HK is a subgroup of G.

(c) If H and K are normal, $H \cap K = \{1\}$, and $HK = G$, then G is isomorphic to the product group $H \times K$.

Proof. (a) Let (h_1,k_1), (h_2,k_2) be elements of $H \times K$ such that $h_1k_1 = h_2k_2$. Multiplying both sides of this equation on the left by h_1^{-1} and on the right by k_2^{-1}, we find $k_1k_2^{-1} = h_1^{-1}h_2$. Since $H \cap K = \{1\}$, $k_1k_2^{-1} = h_1^{-1}h_2 = 1$, hence $h_1 = h_2$ and $k_1 = k_2$. This shows that p is injective.

(b) Suppose that H is a normal subgroup of G, and let $h \in H$ and $k \in K$. Note that $kh = (khk^{-1})k$. Since H is normal, $khk^{-1} \in H$. Therefore $kh \in HK$, which shows that $KH \subset HK$. The proof of the other inclusion is similar. The fact that HK is a subgroup now follows easily. For closure under multiplication, note that in a product $(hk)(h'k') = h(kh')k'$, the middle term kh' is in $KH = HK$, say $kh' = h''k''$. Then $hkh'k' = (hh'')(k''k') \in HK$. Closure under inverses is similar: $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. And of course, $1 = 1 \cdot 1 \in HK$. Thus HK is a subgroup. The proof is similar in the case that K is normal.

(c) Assume that both subgroups are normal and that $H \cap K = \{1\}$. Consider the product $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. Since K is a normal subgroup, the left side is in K. Since H is normal, the right side is in H. Thus this product is the intersection $H \cap K$, i.e., $hkh^{-1}k^{-1} = 1$. Therefore $hk = kh$. This being known, the fact that p is a homomorphism follows directly: In the group $H \times K$, the product rule is $(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2)$, and this element corresponds to $h_1h_2k_1k_2$ in G, while in G the products h_1k_1 and h_2k_2 multiply as $h_1k_1h_2k_2$. Since $h_2k_1 = k_1h_2$, the products are equal. Part (a) shows that p is injective, and the assumption that $HK = G$ shows that p is surjective. □

It is important to note that the product map $p\colon H \times K \longrightarrow G$ will not be a group homomorphism unless the two subgroups commute with each other.

9. MODULAR ARITHMETIC

In this section we discuss Gauss's definition of congruence of integers, which is one of the most important concepts in number theory. We work with a fixed, but arbitrary, positive integer n throughout this section.

Two integers a,b are said to be *congruent modulo n*, written

$$a \equiv b \text{ (modulo } n), \tag{9.1}$$

if n divides $b - a$, or if $b = a + nk$ for some integer k. It is easy to check that this is an equivalence relation. So we may consider the equivalence classes, called *congruence classes modulo n* or *residue classes modulo n*, defined by this relation, as in Section 5. Let us denote the congruence class of an integer a by the symbol $\overline{a}$. It is the set of integers

$$\overline{a} = \{\ldots, a - 2n, a - n, a, a + n, a + 2n, \ldots\}. \tag{9.2}$$

If a and b are integers, the equation $\overline{a} = \overline{b}$ means that n divides $b - a$.

The congruence class of 0 is the subgroup

$$\overline{0} = n\mathbb{Z} = \{\ldots, -n, 0, n, 2n, \ldots\}$$

of the additive group $\mathbb{Z}^+$ consisting of all multiples of n. The other congruence classes are the cosets of this subgroup. Unfortunately, we have a slight notational problem here, because the notation $n\mathbb{Z}$ is like the one we use for a coset. But $n\mathbb{Z}$ is not a coset; it is a subgroup of $\mathbb{Z}^+$. The notation for a coset of a subgroup H analogous to (6.1), but using additive notation for the law of composition, is

$$a + H = \{a + h \mid h \in H\}.$$

In order to avoid writing a coset as $a + n\mathbb{Z}$, let us denote the subgroup $n\mathbb{Z}$ by H. Then the cosets of H are the sets

$$a + H = \{a + nk \mid k \in \mathbb{Z}\}. \tag{9.3}$$

They are the congruence classes $\overline{a} = a + H$.

The n integers $0,1,\ldots,n - 1$ form a natural set of representative elements for the congruence classes:

(9.4) **Proposition.** There are n congruence classes modulo n, namely

$$\overline{0}, \overline{1}, \ldots, \overline{n - 1}.$$

Or, the index $[\mathbb{Z} : n\mathbb{Z}]$ of the subgroup $n\mathbb{Z}$ in $\mathbb{Z}$ is n.

Proof. Let a be an arbitrary integer. Then we may use division with remainder to write

$$a = nq + r,$$

where q, r are integers and where the remainder r is in the range $0 \le r < n$. Then a is congruent to the remainder: $a \equiv r$ (modulo n). Thus $\overline{a} = \overline{r}$. This shows that $\overline{a}$ is one of the congruence classes listed in the proposition. On the other hand, if a and b are distinct integers less than n, say $a \le b$, then $b - a$ is less than n and different from zero, so n does not divide $b - a$. Thus $a \not\equiv b$ (modulo n), which means that $\overline{a} \ne \overline{b}$. Therefore the n classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ are distinct. □

The main point about congruence classes is that addition and multiplication of integers preserve congruences modulo n, and therefore these laws can be used to define addition and multiplication of congruence classes. This is expressed by saying that the set of congruence classes forms a *ring*. We will study rings in Chapter 10.

Let $\overline{a}$ and $\overline{b}$ 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 defined to be the class of ab. In other words, we define

$$(9.5) \qquad \overline{a} + \overline{b} = \overline{a+b} \quad \text{and} \quad \overline{a}\,\overline{b} = \overline{ab}.$$

This definition needs some justification, because the same congruence class $\overline{a}$ can be represented by many different integers. Any integer a' congruent to a modulo n represents the same class. 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.

(9.6) **Lemma.** If $a' \equiv a$ and $b' \equiv b$ (modulo n), then $a' + b' \equiv a + b$ (modulo n) and $a'b' \equiv ab$ (modulo n).

Proof. Assume that $a' \equiv a$ and $b' \equiv b$, so that $a' = a + nr$ and $b' = b + ns$ for some integers r, s. Then $a' + b' = a + b + n(r + s)$, which shows that $a' + b' \equiv a + b$. Similarly, $a'b' = (a + nr)(b + ns) = ab + n(as + rb + nrs)$, which shows that $a'b' \equiv ab$, as required. □

The associative, commutative, and distributive laws hold for the laws of composition (9.5) because they hold for addition and multiplication of integers. For example, the formal verification of the distributive law is as follows:

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

The set of congruence classes modulo n is usually denoted by

$$(9.7) \qquad \mathbb{Z}/n\mathbb{Z}.$$

Computation of addition, subtraction, and multiplication in $\mathbb{Z}/n\mathbb{Z}$ can be made explicitly by working with integers and taking remainders on division by n. That is what the formulas (9.5) mean. They tell us that the map

$$(9.8) \qquad \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

sending an integer a to its congruence class $\overline{a}$ is compatible with addition and multiplication. Therefore computations can be made in the integers and then carried over to $\mathbb{Z}/n\mathbb{Z}$ at the end. However, doing this is not efficient, because computations are simpler if the numbers are kept small. We can keep them small by computing the remainder after some part of a computation has been made.

Thus if $n = 13$, so that

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{12}\},$$

then

$$(\overline{7} + \overline{9})(\overline{11} + \overline{6})$$

can be computed as $\overline{7} + \overline{9} = \overline{3}$, $\overline{11} + \overline{6} = \overline{4}$, $\overline{3} \cdot \overline{4} = \overline{12}$.

The bars over the numbers are a nuisance, so they are often left off. One just has to remember the following rule:

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

10. QUOTIENT GROUPS

We saw in the last section that the congruence classes of integers modulo n are the cosets of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}^+$. So addition of congruence classes gives us a law of composition on the set of these cosets. In this section we will show that a law of composition can be defined on the cosets of a normal subgroup N of any group G. We will show how to make the set of cosets into a group, called a *quotient group*.

Addition of angles is a familiar example of the quotient construction. Every real number represents an angle, and two real numbers represent the same angle if they differ by an integer multiple of 2π. This is very familiar. The point of the example is that addition of angles is defined in terms of addition of real numbers. The group of angles is a quotient group, in which $G = \mathbb{R}^+$ and N is the subgroup of integer multiples of 2π.

We recall a notation introduced in Section 8: If A and B are subsets of a group G, then

$$AB = \{ab \mid a \in A, b \in B\}.$$

We will call this the *product* of the two subsets of the group, though in other contexts the term *product* may stand for the set $A \times B$.

(10.1) **Lemma.** Let N be a normal subgroup of a group G. Then the product of two cosets aN, bN is again a coset, in fact

$$(aN)(bN) = abN.$$

Proof. Note that $Nb = bN$, by (6.18), and since N is a subgroup $NN = N$. The following formal manipulation proves the lemma:

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

This lemma allows us to define multiplication of two cosets C_1, C_2 by this rule: C_1C_2 is the product set. To compute the product coset, take any elements $a \in C_1$ and $b \in C_2$, so that $C_1 = aN$ and $C_2 = bN$. Then $C_1C_2 = abN$ is the coset containing ab. This is the way addition of congruence classes was defined in the last section.

For example, consider the cosets of the unit circle N in $G = \mathbb{C}^\times$. As we saw in Section 5, its cosets are the concentric circles

$$C_r = \{z \mid |z| = r\}.$$

Formula (10.1) amounts to the assertion that if $|\alpha| = r$ and $|\beta| = s$, then $|\alpha\beta| = rs$:

$$C_rC_s = C_{rs}.$$

The assumption that N is a *normal* subgroup of G is crucial to (10.1). If H is not a normal subgroup of G, then there will be left cosets C_1, C_2 of H in G whose products do not lie in a single left coset. For to say H is not normal means there are elements $h \in H$ and $a \in G$ so that $aha^{-1} \notin H$. Then the set

$$(10.2) \qquad (aH)(a^{-1}H)$$

does not lie in any left coset. It contains $a1a^{-1}1 = 1$, which is an element of H. So if the set (10.2) is contained in a coset, that coset must be $H = 1H$. But it also contains $aha^{-1}1$, which is not in H. $\square$

It is customary to denote the set of cosets of a normal subgroup N of G by the symbol

$$(10.3) \qquad G/N = \text{set of cosets of } N \text{ in } G.$$

This agrees with the notation $\mathbb{Z}/n\mathbb{Z}$ introduced in Section 9. Another notation we will frequently use for the set of cosets is the bar notation:

$$G/N = \overline{G} \quad \text{and} \quad aN = \overline{a},$$

so that $\overline{a}$ denotes the coset containing a. This is natural when we want to consider the map

$$(10.4) \qquad \pi: G \longrightarrow \overline{G} = G/N \quad \text{sending} \quad a \rightsquigarrow \overline{a} = aN.$$

(10.5) **Theorem.** With the law of composition defined above, $\overline{G} = G/N$ is a group, and the map π (10.4) is a homomorphism whose kernel is N.

The order of G/N is the index $[G : N]$ of N in G.

(10.6) **Corollary.** Every normal subgroup of a group G is the kernel of a homomorphism. $\square$

This corollary allows us to apply everything that we know about homomorphisms to improve our understanding of normal subgroups.

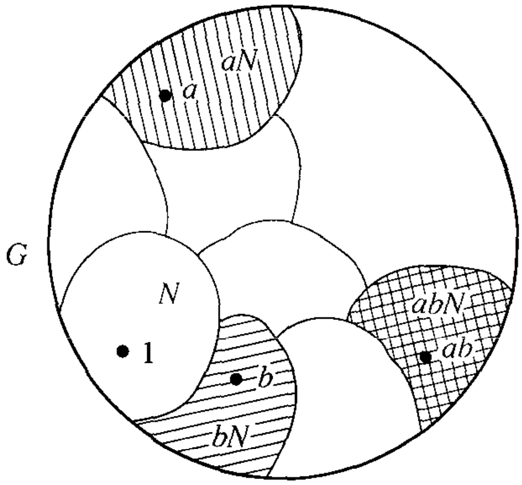
Proof of Theorem (10.5). First note that π is compatible with the laws of composition: Since multiplication of cosets is defined by multiplication of elements, $\pi(a)\pi(b) = \pi(ab)$. Moreover, the elements of G having the same image as the identity element 1 are those in N: $\overline{1} = 1N = N$. The group axioms in $\overline{G}$ follow from Lemma (10.7):

(10.7) **Lemma.** Let G be a group, and let S be any set with a law of composition. Let φ: $G \longrightarrow S$ be a surjective map which has the property $\varphi(a)\varphi(b) = \varphi(ab)$ for all a, b in G. Then S is a group.

Proof. Actually, any law concerning multiplication which holds in G will be carried over to S. The proof of the associative law is this: Let $s_1, s_2, s_3 \in S$. Since φ is surjective, we know that $s_i = \varphi(a_i)$ for some $a_i \in G$. Then

$$\begin{aligned}(s_1s_2)s_3 &= (\varphi(a_1)\varphi(a_2))\varphi(a_3) = \varphi(a_1a_2)\varphi(a_3) = \varphi(a_1a_2a_3)\\ &= \varphi(a_1)\varphi(a_2a_3) = \varphi(a_1)(\varphi(a_2)\varphi(a_3)) = s_1(s_2s_3).\end{aligned}$$

We leave the other group axioms as an exercise. □



(10.8) **Figure.** A schematic diagram of coset multiplication.

For example, let $G = \mathbb{R}^\times$ be the multiplicative group of nonzero real numbers, and let P be the subgroup of positive real numbers. There are two cosets, namely P and $-P = \{\text{negative reals}\}$, and $\overline{G} = G/P$ is the group of two elements. The multiplication rule is the familiar rule: $(Neg)(Neg) = (Pos)$, and so on.

The quotient group construction is related to a general homomorphism φ: $G \longrightarrow G'$ of groups as follows:

(10.9) **Theorem.** *First Isomorphism Theorem:* Let φ: $G \longrightarrow G'$ be a surjective group homomorphism, and let $N = \ker \varphi$. Then G/N is isomorphic to G' by the map $\overline{\varphi}$ which sends the coset $\overline{a} = aN$ to $\varphi(a)$:

$$\overline{\varphi}(\overline{a}) = \varphi(a).$$

This is our fundamental method of identifying quotient groups. For example, the absolute value map $\mathbb{C}^\times \longrightarrow \mathbb{R}^\times$ maps the nonzero complex numbers to the positive real numbers, and its kernel is the unit circle U. So the quotient group $\mathbb{C}^\times/U$ is isomorphic to the multiplicative group of positive real numbers. Or, the determinant is a surjective homomorphism $GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$, 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 $\mathbb{R}^\times$.

Proof of the First Isomorphism Theorem. According to Proposition (5.13), the nonempty fibres of φ are the cosets aN. So we can think of $\overline{G}$ in either way, as the set of cosets or as the set of nonempty fibres of φ. Therefore the map we are looking for is the one defined in (5.10) for any map of sets. It maps $\overline{G}$ bijectively onto the image of φ, which is equal to G' because φ is surjective. By construction it is compatible with multiplication: $\overline{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. □

> 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

1. The Definition of a Group

1. (a) Verify (1.17) and (1.18) by explicit computation.
   (b) Make a multiplication table for S_3.
2. (a) Prove that $GL_n(\mathbb{R})$ is a group.
   (b) Prove that S_n is a group.
3. Let S be a set with an associative law of composition and with an identity element. Prove that the subset of S consisting of invertible elements is a group.
4. Solve for y, given that $xyz^{-1}w = 1$ in a group.
5. Assume that the equation $xyz = 1$ holds in a group G. Does it follow that $yzx = 1$? That $yxz = 1$?
6. Write out all ways in which one can form a product of four elements a, b, c, d in the given order.
7. Let S be any set. Prove that the law of composition defined by $ab = a$ is associative.
8. Give an example of 2×2 matrices such that $A^{-1}B \neq BA^{-1}$.
9. Show that if $ab = a$ in a group, then $b = 1$, and if $ab = 1$, then $b = a^{-1}$.
10. Let a, b be elements of a group G. Show that the equation $ax = b$ has a unique solution in G.
11. Let G be a group, with multiplicative notation. We define an *opposite group* G^0 with law of composition $a \circ b$ as follows: The underlying set is the same as G, but the law of composition is the opposite; that is, we define $a \circ b = ba$. Prove that this defines a group.

2. Subgroups

1. Determine the elements of the cyclic group generated by the matrix $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ explicitly.
2. Let a, b be elements of a group G. Assume that a has order 5 and that $a^3b = ba^3$. Prove that $ab = ba$.
3. Which of the following are subgroups?
   (a) $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$.
   (b) $\{1, -1\} \subset \mathbb{R}^\times$.
   (c) The set of positive integers in $\mathbb{Z}^+$.
   (d) The set of positive reals in $\mathbb{R}^\times$.
   (e) The set of all matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$, in $GL_2(\mathbb{R})$.
4. Prove that a nonempty subset H of a group G is a subgroup if for all $x, y \in H$ the element xy^{-1} is also in H.
5. An nth root of unity is a complex number z such that $z^n = 1$. Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.
6. (a) Find generators and relations analogous to (2.13) for the Klein four group.
   (b) Find all subgroups of the Klein four group.
7. Let a and b be integers.
   (a) Prove that the subset $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$.
   (b) Prove that a and $b + 7a$ generate the subgroup $a\mathbb{Z} + b\mathbb{Z}$.
8. Make a multiplication table for the quaternion group H.
9. Let H be the subgroup generated by two elements a,b of a group G. Prove that if $ab = ba$, then H is an abelian group.
10. (a) Assume that an element x of a group has order rs. Find the order of x^r.
    (b) Assuming that x has arbitrary order n, what is the order of x^r?
11. Prove that in any group the orders of ab and of ba are equal.
12. Describe all groups G which contain no proper subgroup.
13. Prove that every subgroup of a cyclic group is cyclic.
14. Let G be a cyclic group of order n, and let r be an integer dividing n. Prove that G contains exactly one subgroup of order r.
15. (a) In the definition of 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 is the same as the identity in G. Show that if H has an identity at all, then it is the identity in G, so this definition would be equivalent to the one given.
    (b) Show the analogous thing for inverses.
16. (a) Let G be a cyclic group of order 6. How many of its elements generate G?
    (b) Answer the same question for cyclic groups of order 5, 8, and 10.
    (c) How many elements of a cyclic group of order n are generators for that group?
17. Prove that a group in which every element except the identity has order 2 is abelian.
18. According to Chapter 1 (2.18), the elementary matrices generate $GL_n(\mathbb{R})$.
    (a) Prove that the elementary matrices of the first and third types suffice to generate this group.
    (b) The *special linear group* $SL_n(\mathbb{R})$ is the set of real $n \times n$ matrices whose determinant is 1. Show that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

*(c) Use row reduction to prove that the elementary matrices of the first type generate $SL_n(\mathbb{R})$. Do the 2×2 case first.

19. Determine the number of elements of order 2 in the symmetric group S_4.

20. (a) Let a, b be elements of an abelian group of orders m, n respectively. What can you say about the order of their product ab?

*(b) Show by example that the product of elements of finite order in a nonabelian group need not have finite order.

21. Prove that the set of elements of finite order in an abelian group is a subgroup.

22. Prove that the greatest common divisor of a and b, as defined in the text, can be obtained by factoring a and b into primes and collecting the common factors.

3. Isomorphisms

1. Prove that the additive group $\mathbb{R}^+$ of real numbers is isomorphic to the multiplicative group P of positive reals.

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

3. Let a, b be elements of a group G, and let $a' = bab^{-1}$. Prove that $a = a'$ if and only if a and b commute.

4. (a) Let $b' = aba^{-1}$. Prove that $b'^n = ab^na^{-1}$.

(b) Prove that if $aba^{-1} = b^2$, then $a^3ba^{-3} = b^8$.

5. Let $\varphi\colon G \longrightarrow G'$ be an isomorphism of groups. Prove that the inverse function φ^{-1} is also an isomorphism.

6. Let $\varphi\colon G \longrightarrow G'$ be an isomorphism of groups, let $x, y \in G$, and let $x' = \varphi(x)$ and $y' = \varphi(y)$.

(a) Prove that the orders of x and of x' are equal.

(b) Prove that if $xyx = yxy$, then $x'y'x' = y'x'y'$.

(c) Prove that $\varphi(x^{-1}) = x'^{-1}$.

7. Prove that the matrices $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$ are conjugate elements in the group $GL_2(\mathbb{R})$ but that they are not conjugate when regarded as elements of $SL_2(\mathbb{R})$.

8. Prove that the matrices $\begin{bmatrix} 1 & \\ & 2 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ & 2 \end{bmatrix}$ are conjugate in $GL_2(\mathbb{R})$.

9. Find an isomorphism from a group G to its opposite group G^0 (Section 2, exercise 12).

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

11. Prove that the set Aut G of automorphisms of a group G forms a group, the law of composition being composition of functions.

12. Let G be a group, and let $\varphi\colon G \longrightarrow G$ be the map $\varphi(x) = x^{-1}$.

(a) Prove that φ is bijective.

(b) Prove that φ is an automorphism if and only if G is abelian.

13. (a) Let G be a group of order 4. Prove that every element of G has order 1, 2, or 4.

(b) Classify groups of order 4 by considering the following two cases:

(i) G contains an element of order 4.

(ii) Every element of G has order < 4.

14. Determine the group of automorphisms of the following groups.

(a) $\mathbb{Z}^+$, (b) a cyclic group of order 10, (c) S_3.

15. Show that the functions $f = 1/x$, $g = (x - 1)/x$ generate a group of functions, the law of composition being composition of functions, which is isomorphic to the symmetric group S_3.
16. Give an example of two isomorphic groups such that there is more than one isomorphism between them.

4. Homomorphisms

1. Let G be a group, with law of composition written $x \# y$. Let H be a group with law of composition $u \circ v$. What is the condition for a map $\varphi: G \longrightarrow H'$ to be a homomorphism?
2. Let $\varphi: G \longrightarrow G'$ be a group homomorphism. Prove that for any elements $a_1, \ldots, a_k$ of G, $\varphi(a_1 \cdots a_k) = \varphi(a_1) \cdots \varphi(a_k)$.
3. Prove that the kernel and image of a homomorphism are subgroups.
4. Describe all homomorphisms $\varphi: \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$, and determine which are injective, which are surjective, and which are isomorphisms.
5. Let G be an abelian group. Prove that the nth power map $\varphi: G \longrightarrow G$ defined by $\varphi(x) = x^n$ is a homomorphism from G to itself.
6. Let $f: \mathbb{R}^+ \longrightarrow \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism, and determine its kernel and image.
7. Prove that the absolute value map $|\ |: \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$ sending $\alpha \rightsquigarrow |\alpha|$ is a homomorphism, and determine its kernel and image.
8. (a) Find all subgroups of S_3, and determine which are normal.
   (b) Find all subgroups of the quaternion group, and determine which are normal.
9. (a) Prove that the composition $\varphi \circ \psi$ of two homomorphisms φ, ψ is a homomorphism.
   (b) Describe the kernel of $\varphi \circ \psi$.
10. Let $\varphi: G \longrightarrow G'$ be a group homomorphism. Prove that $\varphi(x) = \varphi(y)$ if and only if $xy^{-1} \in \ker \varphi$.
11. Let G, H be cyclic groups, generated by elements x, y. Determine the condition on the orders m, n of x and y so that the map sending $x^i \rightsquigarrow y^i$ is a group homomorphism.
12. Prove that the $n \times n$ matrices M which have the block form $\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ with $A \in GL_r(\mathbb{R})$ and $D \in GL_{n-r}(\mathbb{R})$ form a subgroup P of $GL_n(\mathbb{R})$, and that the map $P \longrightarrow GL_r(\mathbb{R})$ sending $M \rightsquigarrow A$ is a homomorphism. What is its kernel?
13. (a) Let H be a subgroup of G, and let $g \in G$. The *conjugate subgroup* gHg^{-1} is defined to be the set of all conjugates ghg^{-1}, where $h \in H$. Prove that gHg^{-1} is a subgroup of G.
    (b) Prove that a subgroup H of a group G is normal if and only if $gHg^{-1} = H$ for all $g \in G$.
14. Let N be a normal subgroup of G, and let $g \in G$, $n \in N$. Prove that $g^{-1}ng \in N$.
15. Let φ and ψ be two homomorphisms from a group G to another group G', and let $H \subset G$ be the subset $\{x \in G \mid \varphi(x) = \psi(x)\}$. Prove or disprove: H is a subgroup of G.
16. Let $\varphi: G \longrightarrow G'$ be a group homomorphism, and let $x \in G$ be an element of order r. What can you say about the order of $\varphi(x)$?
17. Prove that the center of a group is a normal subgroup.

18. Prove that the center of $GL_n(\mathbb{R})$ is the subgroup $Z = \{cI \mid c \in \mathbb{R}, c \neq 0\}$.

19. Prove that if a group contains exactly one element of order 2, then that element is in the center of the group.

20. Consider the set U of real 3×3 matrices of the form

$$\begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix}.$$

(a) Prove that U is a subgroup of $SL_n(\mathbb{R})$.

(b) Prove or disprove: U is normal.

*(c) Determine the center of U.

21. Prove by giving an explicit example that $GL_2(\mathbb{R})$ is not a normal subgroup of $GL_2(\mathbb{C})$.

22. Let $\varphi \colon G \longrightarrow G'$ be a surjective homomorphism.

(a) Assume that G is cyclic. Prove that G' is cyclic.

(b) Assume that G is abelian. Prove that G' is abelian.

23. Let $\varphi \colon G \longrightarrow G'$ be a surjective homomorphism, and let N be a normal subgroup of G. Prove that $\varphi(N)$ is a normal subgroup of G'.

5. *Equivalence Relations and Partitions*

1. Prove that the nonempty fibres of a map form a partition of the domain.

2. Let S be a set of groups. Prove that the relation $G \sim H$ if G is isomorphic to H is an equivalence relation on S.

3. Determine the number of equivalence relations on a set of five elements.

4. Is the intersection $R \cap R'$ of two equivalence relations $R, R' \subset S \times S$ an equivalence relation? Is the union?

5. Let H be a subgroup of a group G. Prove that the relation defined by the rule $a \sim b$ if $b^{-1}a \in H$ is an equivalence relation on G.

6. (a) Prove that the relation x conjugate to y in a group G is an equivalence relation on G.

(b) Describe the elements a whose conjugacy class (= equivalence class) consists of the element a alone.

7. Let R be a relation on the set $\mathbb{R}$ of real numbers. We may view R as a subset of the (x, y)-plane. Explain the geometric meaning of the reflexive and symmetric properties.

8. With each of the following subsets R of the (x, y)-plane, determine which of the axioms (5.2) are satisfied and whether or not R is an equivalence relation on the set $\mathbb{R}$ of real numbers.

(a) $R = \{(s,s) \mid s \in \mathbb{R}\}$.

(b) R = empty set.

(c) R = locus $\{y = 0\}$.

(d) R = locus $\{xy + 1 = 0\}$.

(e) R = locus $\{x^2y - xy^2 - x + y = 0\}$.

(f) R = locus $\{x^2 - xy + 2x - 2y = 0\}$.

9. Describe the smallest equivalence relation on the set of real numbers which contains the line $x - y = 1$ in the (x, y)-plane, and sketch it.

10. Draw the fibres of the map from the (x,z)-plane to the y-axis defined by the map $y = zx$.

11. Work out rules, obtained from the rules on the integers, for addition and multiplication on the set (5.8).
12. Prove that the cosets (5.14) are the fibres of the map φ.

6. Cosets

1. Determine the index $[\mathbb{Z} : n\mathbb{Z}]$.
2. Prove directly that distinct cosets do not overlap.
3. Prove that every group whose order is a power of a prime p contains an element of order p.
4. Give an example showing that left cosets and right cosets of $GL_2(\mathbb{R})$ in $GL_2(\mathbb{C})$ are not always equal.
5. Let H, K be subgroups of a group G of orders $3, 5$ respectively. Prove that $H \cap K = \{1\}$.
6. *Justify (6.15) carefully.*
7. (a) Let G be an abelian group of odd order. Prove that the map $\varphi: G \longrightarrow G$ defined by $\varphi(x) = x^2$ is an automorphism.
   (b) Generalize the result of (a).
8. Let W be the additive subgroup of $\mathbb{R}^m$ of solutions of a system of homogeneous linear equations $AX = 0$. Show that the solutions of an inhomogeneous system $AX = B$ form a coset of W.
9. Let H be a subgroup of a group G. Prove that the number of left cosets is equal to the number of right cosets **(a)** if G is finite and **(b)** in general.
10. (a) Prove that every subgroup of index 2 is normal.
    (b) Give an example of a subgroup of index 3 which is not normal.
11. Classify groups of order 6 by analyzing the following three cases.
    (a) G contains an element of order 6.
    (b) G contains an element of order 3 but none of order 6.
    (c) All elements of G have order 1 or 2.
12. Let G, H be the following subgroups of $GL_2(\mathbb{R})$:

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

An element of G can be represented by a point in the (x, y)-plane. Draw the partitions of the plane into left and into right cosets of H.

7. Restriction of a Homomorphism to a Subgroup

1. Let G and G' be finite groups whose orders have no common factor. Prove that the only homomorphism $\varphi: G \longrightarrow G'$ is the trivial one $\varphi(x) = 1$ for all x.
2. Give an example of a permutation of even order which is odd and an example of one which is even.
3. (a) Let H and K be subgroups of a group G. 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.

4. Prove Proposition (7.1).
5. Let H, N be subgroups of a group G, with N normal. Prove that $HN = NH$ and that this set is a subgroup.
6. Let $\varphi: G \longrightarrow G'$ be a group homomorphism with kernel K, and let H be another subgroup of G. Describe $\varphi^{-1}(\varphi(H))$ in terms of H and K.
7. Prove that a group of order 30 can have at most 7 subgroups of order 5.

*8. Prove the *Correspondence Theorem:* Let $\varphi: G \longrightarrow G'$ be a surjective group homomorphism with kernel N. The set of subgroups H' of G' is in bijective correspondence with the set of subgroups H of G which contain N, the correspondence being defined by the maps $H \rightsquigarrow \varphi(H)$ and $\varphi^{-1}(H') \leftsquigarrow H'$. Moreover, normal subgroups of G correspond to normal subgroups of G'.

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

8. Products of Groups

1. Let G, G' be groups. What is the order of the product group $G \times G'$?
2. Is the symmetric group S_3 a direct product of nontrivial groups?
3. Prove that a finite cyclic group of order rs is isomorphic to the product of cyclic groups of orders r and s if and only if r and s have no common factor.
4. In each of the following cases, determine whether or not G is isomorphic to the product of H and K.
   (a) $G = \mathbb{R}^\times$, $H = \{\pm 1\}$, $K = \{$positive real numbers$\}$.
   (b) $G = \{$invertible upper triangular 2×2 matrices$\}$, $H = \{$invertible diagonal matrices$\}$, $K = \{$upper triangular matrices with diagonal entries 1$\}$.
   (c) $G = \mathbb{C}^\times$ and $H = \{$unit circle$\}$, K ⫧ $\{$positive reals$\}$.
5. Prove that the product of two infinite cyclic groups is not infinite cyclic.
6. Prove that the center of the product of two groups is the product of their centers.
7. (a) Let H, K be subgroups of a group G. Show that the set of products $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup if and only if $HK = KH$.
   (b) Give an example of a group G and two subgroups H, K such that HK is not a subgroup.
8. Let G be a group containing normal subgroups of orders 3 and 5 respectively. Prove that G contains an element of order 15.
9. Let G be a finite group whose order is a product of two integers: $n = ab$. Let H, K be subgroups of G of orders a and b respectively. Assume that $H \cap K = \{1\}$. Prove that $HK = G$. Is G isomorphic to the product group $H \times K$?
10. Let $x \in G$ have order m, and let $y \in G'$ have order n. What is the order of (x, y) in $G \times G'$?
11. Let H be a subgroup of a group G, and let $\varphi: G \longrightarrow H$ be a homomorphism whose restriction to H is the identity map: $\varphi(h) = h$, if $h \in H$. Let $N = \ker \varphi$.
    (a) Prove that if G is abelian then it is isomorphic to the product group $H \times N$.
    (b) Find a bijective map $G \longrightarrow H \times N$ without the assumption that G is abelian, but show by an example that G need not be isomorphic to the product group.

9. Modular Arithmetic

1. Compute (7 + 14)(3 − 16) modulo 17.
2. **(a)** Prove that the square a^2 of an integer a is congruent to 0 or 1 modulo 4.
   (b) What are the possible values of a^2 modulo 8?
3. **(a)** Prove that 2 has no inverse modulo 6.
   (b) Determine all integers n such that 2 has an inverse modulo n.
4. Prove that every integer a is congruent to the sum of its decimal digits modulo 9.
5. Solve the congruence $2x \equiv 5$ **(a)** modulo 9 and **(b)** modulo 6.
6. Determine the integers n for which the congruences $x + y \equiv 2$, $2x - 3y \equiv 3$ (modulo n) have a solution.
7. Prove the associative and commutative laws for multiplication in $\mathbb{Z}/n\mathbb{Z}$.
8. Use Proposition (2.6) to prove the *Chinese Remainder Theorem:* Let m, n, a, b be integers, and assume that the greatest common divisor of m and n is 1. Then there is an integer x such that $x \equiv a$ (modulo m) and $x \equiv b$ (modulo n).

10. Quotient Groups

1. Let G be the group of invertible real upper triangular 2×2 matrices. Determine whether or not the following conditions describe normal subgroups H of G. If they do, use the First Isomorphism Theorem to identify the quotient group G/H.
   (a) $a_{11} = 1$. **(b)** $a_{12} = 0$ **(c)** $a_{11} = a_{22}$ **(d)** $a_{11} = a_{22} = 1$
2. Write out the proof of (10.1) in terms of elements.
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 which contains 1. Prove that N is a normal subgroup of G and that P is the set of its cosets.
4. **(a)** Consider the presentation (1.17) of the symmetric group S_3. Let H be the subgroup $\{1, y\}$. Compute the product sets $(1H)(xH)$ and $(1H)(x^2H)$, and verify that they are not cosets.
   (b) Show that a cyclic group of order 6 has two generators satisfying the rules $x^3 = 1$, $y^2 = 1$, $yx = xy$.
   (c) Repeat the computation of (a), replacing the relations (1.18) by the relations given in part (b). Explain.
5. Identify the quotient group $\mathbb{R}^\times/P$, where P denotes the subgroup of positive real numbers.
6. 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, and prove that G/H is isomorphic to G.
7. Find all normal subgroups N of the quaternion group H, and identify the quotients H/N.
8. Prove that the subset H of $G = GL_n(\mathbb{R})$ of matrices whose determinant is positive forms a normal subgroup, and describe the quotient group G/H.
9. Prove that the subset $G \times 1$ of the product group $G \times G'$ is a normal subgroup isomorphic to G and that $(G \times G')/(G \times 1)$ is isomorphic to G'.
10. Describe the quotient groups $\mathbb{C}^\times/P$ and $\mathbb{C}^\times/U$, where U is the subgroup of complex numbers of absolute value 1 and P denotes the positive reals.
11. Prove that the groups $\mathbb{R}^+/\mathbb{Z}^+$ and $\mathbb{R}^+/2\pi\mathbb{Z}^+$ are isomorphic.

Miscellaneous Problems

1. What is the product of all mth roots of unity in $\mathbb{C}$?

2. Compute the group of automorphisms of the quaternion group.

3. Prove that a group of even order contains an element of order 2.

4. Let $K \subset H \subset G$ be subgroups of a finite group G. Prove the formula $[G : K] = [G : H][H : K]$.

***5.** A *semigroup* S is a set with an associative law of composition and with an identity. But elements are not required to have inverses, so the cancellation law need not hold. The 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 the whole set S. For example, the relations $s^2 = 1$ and $s^2 = s$ describe two different semigroup structurès on the set $\{1, s\}$. Define isomorphism of semigroups, and describe all isomorphism classes of semigroups having a generator.

6. Let S be a semigroup with finitely many elements which satisfies the Cancellation Law (1.12). Prove that S is a group.

***7.** 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 interval $[0, 1]$ with values in $\mathbb{R}^k$, that is, a function $f\colon [0, 1] \longrightarrow \mathbb{R}^k$, sending $t \rightsquigarrow f(t) = (x_1(t), \ldots, x_k(t))$, such that $f(0) = a$ and $f(1) = b$. If S is a subset of $\mathbb{R}^k$ and if $a, b \in S$, we define $a \sim b$ if a and b can be joined by a path lying entirely in S.

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

(b) A subset S of $\mathbb{R}^k$ is called *path connected* if $a \sim b$ for any two points $a, b \in S$. Show that every subset S is partitioned into path-connected subsets with the property that two points in different subsets can not be connected by a path in S.

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

***8.** The set of $n \times n$ matrices can be identified with the space $\mathbb{R}^{n \times n}$. Let G be a subgroup of $GL_n(\mathbb{R})$. Prove each of the following.

(a) If $A, B, C, D \in G$, 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 which can be joined to the identity I forms a normal subgroup of G (called the *connected component* of G).

***9.** (a) Using the fact that $SL_n(\mathbb{R})$ is generated by elementary matrices of the first type (see exercise 18, Section 2), prove that this group is path-connected.

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

10. Let H, K be subgroups of a group G, and let $g \in G$. The set

$$HgK = \{x \in G \mid x = hgk \text{ for some } h \in H, k \in K\}$$

is called a *double coset*.

(a) Prove that the double cosets partition G.

(b) Do all double cosets have the same order?

11. Let H be a subgroup of a group G. Show that the double cosets HgH are the left cosets gH if H is normal, but that if H is not normal then there is a double coset which properly contains a left coset.

***12.** Prove that the double cosets in $GL_n(\mathbb{R})$ of the subgroups $H = \{\text{lower triangular matrices}\}$ and $K = \{\text{upper triangular matrices}\}$ are the sets HPK, where P is a permutation matrix.