

CHAPTER 1

Groups

We concern ourselves with sets G of objects a, b, c, \dots called elements. The sentence “ a is an element of G ” will be denoted symbolically by $a \in G$. Assume an operation called “multiplication” which assigns to an ordered pair of objects a, b of G another object $a \cdot b$ (or simply ab) the *product* of a and b . It is useful to require that G be *closed* with respect to multiplication, namely:

- (1) If $a, b \in G$, then $a \cdot b \in G$.

EXAMPLES.

- (a) Let G be the set of positive integers. If subtraction is taken as the “multiplication” in G , then G is certainly not closed, e.g., $3 \cdot 5 = 3 - 5 = -2$. If taking the greatest common divisor is our multiplication, then closure is obvious.
- (b) Take G to be the set of functions of one variable. If $f(x), g(x) \in G$ define $f(x) \cdot g(x) = f[g(x)]$, e.g., $e^x \cdot \log x = e^{\log x} = x$.

EXERCISE 1. Write out the multiplication table and thereby show closure for the set of functions

$$f_1 = x, \quad f_2 = \frac{1}{x}, \quad f_3 = 1 - x, \quad f_4 = \frac{1}{1 - x}, \quad f_5 = \frac{x}{x - 1}, \quad f_6 = \frac{x - 1}{x}.$$

SOLUTION.

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_2	f_6	f_3	f_1
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_3	f_5	f_1	f_2	f_4

where $f_i \cdot f_j$ is listed in the i^{th} row and j^{th} column.

We make the further requirement that multiplication obey the *associative law*:

- (2) If $a, b, c \in G$, then $(ab)c = a(bc)$. This is a rather strong condition. It is not generally satisfied; consider, e.g., subtraction among the integers. For functions of one variable, as above, it is valid, however. If $f(x), g(x), h(x)$ are any three functions we have

$$(fg)h = f(g(h(x))) = f(gh).$$

EXERCISE 2. Deduce the associative law for four elements from (2), that is, show that the five possible products of four elements written in a given sequence are all equal. Furthermore, attempt to determine the number of possible products of n elements given in a linear order. For example, the elements a_1, a_2, a_3, a_4 in that order yield the products $(a_1a_2)(a_3a_4)$, $a_1(a_2(a_3a_4))$, etc. *Hint*: Let α_n be the number of products of a_1, a_2, \dots, a_n . Find a recursion formula for α_n and use the Lagrange generating function

$$f(x) = \alpha_1x + \alpha_2x^2 + \dots + \alpha_nx^n + \dots .$$

EXERCISE 3. The associative law for n elements states that all possible products of n elements written in a prescribed order, e.g., a_1, a_2, \dots, a_n , yield the same result. Prove the associative law for any number of elements using only (2) (the associative law for three elements).

PROOF FOR EXERCISE 3: We assume the validity of the associative law for all products of m factors, $m \leq n$, and show that this implies the validity of the law for $n + 1$. Consider the particular product $(n + 1) \prod_{k=1}^{n+1} a_k$ which is obtained from the $n + 1$ elements a_1, a_2, \dots, a_{n+1} by successively multiplying on the right, i.e.,

$$\begin{aligned} \prod_{k=1}^1 a_k &= a_1, \\ \prod_{k=1}^{n+1} a_k &= \left(\prod_{k=1}^n a_k \right) a_{n+1}. \end{aligned}$$

Let P_{n+1} be any product of the $n + 1$ elements a_1, a_2, \dots, a_{n+1} taken in that order. Since P_{n+1} is the result of at least one multiplication, we may write

$$P_{n+1} = P_1^m P_{m+1}^{n+1}, \quad 1 \leq m \leq n,$$

where P_1^m is some product of the elements a_1, a_2, \dots, a_m in that order and P_{m+1}^{n+1} of the remaining elements $a_{m+1}, a_{m+2}, \dots, a_{n+1}$. By the induction hypothesis we have

$$P_\mu^\nu = \prod_{k=\mu}^\nu a_k$$

for any μ, ν such that $\nu - \mu + 1 \leq n$. Specifically, we have

$$\begin{aligned} P_{n+1} &= \left(\prod_{j=1}^m a_j \right) \left(\prod_{k=m+1}^{n+1} a_k \right) = \prod_{j=1}^m a_j \cdot \left[\left(\prod_{k=m+1}^n a_k \right) \cdot a_{n+1} \right] \\ &= \left(\prod_{j=1}^m a_j \prod_{k=m+1}^n a_k \right) \cdot a_{n+1} \\ &= \left(\prod_{k=1}^n a_k \right) \cdot a_{n+1} = \prod_{k=1}^{n+1} a_k, \end{aligned}$$

each step being a simple application of (2). □

1.1. The Concept of a Group

A set G will be called a *group* if it satisfies the following conditions:

- (1) *Closure*. There exists an operation called multiplication which assigns to any ordered pair $a, b \in G$ a product $ab \in G$.
- (2) *Associative Law*. If $a, b, c \in G$ then $(ab)c = a(bc)$.
- (3) *Identity*. There exists an $e \in G$, called the (left) *identity*, such that $ea = a$ for all $a \in G$.
- (4) *Inverse*. For every $a \in G$ there is an $a^{-1} \in G$, called the (left) *inverse* of a , such that $a^{-1}a = e$.

Let us examine the product

$$(a^{-1})^{-1}a^{-1}aa^{-1}.$$

On one hand,

$$[(a^{-1})^{-1}a^{-1}][aa^{-1}] = e[aa^{-1}] = aa^{-1},$$

and on the other

$$[(a^{-1})^{-1}][a^{-1}a] = [(a^{-1})^{-1}][ea^{-1}] = (a^{-1})^{-1}a^{-1} = e.$$

Consequently,

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

The existence of the left inverse implies the existence of a right inverse. A similar result holds for the identity; for consider the product

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

First we have

$$aa^{-1}a = (aa^{-1})a = ea = a.$$

But also

$$aa^{-1}a = a(a^{-1}a) = ae.$$

Consequently,

$$ae = a,$$

and the existence of the right identity implies the existence of a left identity.

EXERCISE 4. Two systems of postulates are said to be equivalent if either system can be derived logically from the other. Show that the system (1), (2), (3), (4) is equivalent to the system in which (3) and (4) are replaced by:

- (3') There is a right identity $e \in G$ such that $ae = a$ for all $a \in G$.
- (4') To each $a \in G$ there is a right inverse $a^{-1} \in G$ such that $aa^{-1} = e$.

Apparently the words *right* and *left* need not be included in (3), (4), (3'), or (4').

EXERCISE 5. Consider the postulate system in which (3) and (4) are replaced by:

- (3*) There exists a left identity $e \in G$; that is, $ea = a$ for all $a \in G$.
 - (4*) To each $a \in G$ there is a right inverse $a^{-1} \in G$; that is, $aa^{-1} = e$.
- Determine whether this system of postulates defines a group. If not, give a counterexample.

SOLUTION. For any $a \in G$ define multiplication by $ax = x$ for all $x \in G$. This system satisfies the postulates (1), (2), (3*), and (4*). What group property does it not satisfy?

For ordinary numbers, the quotient $b \div a$ of two numbers can be defined as the solution of the equation $ax = b$. Consider similar equations for elements of G :

$$(a) \ ax = b, \quad (b) \ xa = b, \quad (c) \ axb = c$$

If (a) is true for some x , then

$$a^{-1}ax = a^{-1}b = ex = x.$$

Hence, if there is a solution, it is $a^{-1}b$ and it is therefore unique; $a^{-1}b$ is in fact a solution. Similar reasoning shows that (b) possesses the unique solution $x = ba^{-1}$ and (c) the unique solution $a^{-1}cb^{-1}$. The existence of a unique solution for each of the above equations demonstrates a property of the group analogous to division.

Since a^{-1} is the solution of the equation $xa = e$, a^{-1} is unique. Similarly, e is the unique solution of $xa = a$. We observe that the solution of $x(ab) = e$ is $(ab)^{-1} = b^{-1}a^{-1}$. In general, the inverse of a product

$$(a_1a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1}a_1^{-1}.$$

If $x = (a^{-1})^{-1}$, then x satisfies the equation $xa^{-1} = e$, which has the unique solution $x = a$. Thus the inverse of the inverse of an element is the element itself.

EXERCISE 6. Show that postulates (3) and (4) may be replaced by

(3⁺) If $a, b \in G$, the equations

$$xa = b, \quad ay = b,$$

possess (not necessarily unique) solutions $x, y \in G$.

A group that satisfies the *commutative* law,

(5) If $a, b \in G$, then $ab = ba$,

is said to be commutative or abelian.

EXERCISE 7. Show that the six functions of Exercise 1 form a noncommutative group with respect to their rule of multiplication. Determine the identity element and the inverse to each function.

1.2. Subgroups

If G is a group and S is a subset of G that is itself a group under the same operation as G , then S is called a *subgroup* of G .

EXAMPLE. Take G to be the set of rational numbers other than zero under ordinary multiplication. G has, e.g., the subgroups

- (a) the positive rational numbers
- (b) the powers of any element
- (c) the set consisting of $+1$ and -1

Trivially, (d) the set G itself or (e) the set consisting of the element 1.

THEOREM 1.1 *Necessary and sufficient conditions for a subset S of G to be a subgroup are:*

- (i) Closure. *If $s_1, s_2 \in S$, then $s_1s_2 \in S$.*
- (ii) Inverse. *If $s \in S$, then $s^{-1} \in S$.*

PROOF: *Necessity.* If S is a subgroup, (i) holds by definition. The identity $e \in S$ by the uniqueness in G and existence in S by the solution of the equation

$$xs = s.$$

Note that (ii) is similarly established through the equation $xs = e$.

Sufficiency. If (i) and (ii) hold, then S is a subgroup. From (ii) if $s \in S$ then s^{-1} is an element of S and hence (i) gives $e \in S$. The associative law holds for elements of S since they are elements of G . The proof of the theorem is complete. \square

If S is a subgroup of G and $a \in G$, the *coset* aS is defined to be the set of all elements $a \cdot s$, where $s \in S$.

EXAMPLE. Take for G the set of all rational numbers excluding zero under ordinary multiplication. Let S be the set of all positive elements of G . There are only two cosets, S and $-S = -1S$. These have no elements in common and both sets together cover G . If we take instead $S = \{+1, -1\}$ then the cosets are $aS = \{+a, -a\}$. Here the same coset is given by $+a$ and $-a$. Note again that no two cosets overlap and that the cosets cover G . These results are valid in general.

Let S be a subgroup of G and take $a, b \in G$.

LEMMA 1.2 *If the cosets aS and bS have an element c in common, then $aS = bS$.*

Assume for some $s, s' \in S$ we have $c = as = bs'$. Therefore $b = as(s')^{-1}$. From Theorem 1.1, $s(s')^{-1} = s'' \in S$ and consequently $bS = as''S$. Now $s''S = S$, since if we suppose S to be any group, s any element of S , we have

$$sS \subset S$$

(read: sS is a subset of S , or all elements of sS are elements of S). Also,

$$s^{-1}s \subset S \quad \text{or} \quad S \subset sS.$$

Therefore

$$sS = S.$$

In the above argument we may now write $bS = as''S = aS$.

LEMMA 1.3 *Every $a \in G$ is contained in some coset*

$$a \in aS \quad \text{since} \quad e \in S$$

and hence $ae = a \in aS$. G is covered by the cosets of S .

If G is a finite group, then the number of its elements is called the *order* of G .

THEOREM 1.4 *Let G be a finite group of order N and S a subgroup of order n . The number n of elements in the subgroup is a divisor of N .*

PROOF: The cosets aS have the same number of elements as S . For let S consist of the distinct elements s_1, s_2, \dots, s_n . aS consist of as_1, as_2, \dots, as_n , where

$$as_1 \neq as_k, \quad i \neq k.$$

For otherwise we would have $as_i = as_k$ and hence $s_i = s_k, i \neq k$, contrary to the definition of the s_i .

Consequently, aS consists of exactly n elements. Let j be the number of cosets. By Lemmas 1.2 and 1.3 the cosets cover G without overlapping. It follows that

$$N = jn. \quad \square$$

Take $a \in G$. We denote aa by a^2 or, in general, we define all the integral powers a^μ of a by

$$\begin{aligned} a^\mu &= aa \cdots a \quad (\mu \text{ times}) \text{ for } \mu > 0, \\ a^0 &= e, \\ a^\mu &= a^{-1}a^{-1} \cdots a^{-1} \quad (-\mu \text{ times}) \text{ for } \mu < 0. \end{aligned}$$

The set of all powers of a is a group and clearly the smallest group containing a . The problem of determining the smallest group containing as few as two elements is already of an entirely different nature. For example, what can be said about

$$(ab)^n = ab \cdot ab \cdots ab \quad (n \text{ times})?$$

If multiplication is commutative such products can be handled, but this does not apply in general.

EXERCISE 8. Show that the powers of elements obey the usual properties of exponents

$$\begin{aligned} a^\mu a^\nu &= a^{\mu+\nu}, \\ (a^\nu)^\mu &= a^{\nu\mu}. \end{aligned}$$

The first property implies the commutative law for multiplication of powers of a .

The set S of all powers of a forms a subgroup since S is closed under multiplication and inverses exist (cf. Theorem 1.1).

Case 1. The powers of a are all distinct. S is then called an *infinite cyclic group*.

Case 2. There exist integers i and k with, say, $i < k$ such that $a^i = a^k$. Multiplying on both sides by a^{-i} we obtain $e = a^{k-i}$. Thus the set of positive integers for which $a^\mu = e$ is not empty. Let d be the smallest such integer

$$a^d = e \Rightarrow a^{qd} = e \quad \text{for all integers } q$$

(read: “implies” for “ \Rightarrow ”). Conversely, if $a^m = e$, m is a multiple of d , for we may write $m = qd + r$ where $0 \leq r < d$

$$a^r = a^{m-qd} = a^m a^{-qd} = e.$$

But d is the smallest positive integer for which $a^d = e$. Hence r must be zero whence $m = qd$. The powers

$$a^0, a^1, a^2, \dots, a^{d-1}$$

are all distinct for otherwise we would have

$$a^i = a^k, \quad 0 \leq i < k < d, \quad \text{or} \quad a^{k-i} = e;$$

this equation is impossible for $0 < k - i < d$. Any other power of a must be equal to one of these, for example $a^d = e, a^{d+1} = a, \dots$, or, in general,

$$a^{qd+r} = a^r, \quad 0 \leq r < d.$$

Thus there are only d distinct powers of a . S is called a *cyclic* subgroup of order d and d is called the *period* of a .

THEOREM 1.5 *The period of any element of a finite group is a divisor of the order of the group.*

PROOF: This is an immediate consequence of Theorem 1.4. Let G be a finite group of order N and a any element of G . If d is the period of a , we may write $N = dj$. From $a^d = e$ we have

$$a^{dj} = a^N = e.$$

This statement for prime N is equivalent to Fermat's theorem in arithmetic. \square

COROLLARY *If the order of G is p , a prime, then G must be cyclic.*

PROOF: The period of any element must be a divisor of p and is therefore either p or 1. The only element of period 1 is e . Consequently, if $a \in G$ and $a \neq e$ the period of a must be p . \square

There is "essentially" one cyclic group of order n . Phrased differently, two cyclic groups of the same order have the "same structure." The notion of "same structure" will be examined later in more detail.

EXAMPLES. Let us determine all possible structures of groups of order 4. The period of any element must be 1, 2, or 4. If there is an element a of period 4 then e, a, a^2, a^3 exhaust the group. On the other hand, if there is no element of period 4, then all elements but e must have the period 2. Thus if e, a, b, c denote the different elements of the group we have $a^2 = b^2 = c^2 = e$. Consider the element $x = ab$. From $ax = aab = b$ we have clearly $x \neq e, x \neq a$. From the uniqueness of the solution $y = e$ of the equation $yb = b$ it follows that $x \neq b$. Therefore x must be c . The commutative law holds in this group, for if $x \in G$ then $x = x^{-1}$ and consequently $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. It is a simple matter to write out the multiplication table:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

We have shown that there are essentially two groups of order 4 and both are commutative.

Groups of order 6 are essentially of two kinds, the cyclic group and the noncommutative group given in Exercise 1. This last is the simplest example of a noncommutative group. One of the unsolved problems of algebra is that of classifying all the groups of order n . There is, of course, always the cyclic group of order n and for n prime, only the cyclic group. For nonprimes there is no general theory although a classification has been achieved for special cases. The table below gives a summary for the first few cases:

N	4	6	8	9	10	12	14	15
μ	2	2	5	2	2	5	2	1
ν	0	1	2	0	1	3	1	0

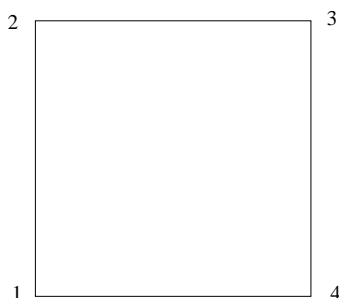
where μ is the total number and ν the number of noncommutative groups of order N .

EXERCISE 9. The two noncommutative groups of order 8 are essentially:

- (a) The symmetries of the square, i.e., the rotations in space which take the square into itself.
- (b) The group formed by the quaternion units $\pm 1, \pm i, \pm j, \pm k$.

Construct the multiplication table for those two groups and show that they do not have the same structure.

(a) The symmetries of the square.



If a rotation replaces the vertices (1234) by the vertices $(a_1a_2a_3a_4)$, then denote the rotation simply by $(a_1a_2a_3a_4)$. The identity is clearly $e = (1234)$. Denote by $a = (2341)$ the counterclockwise rotation through 90° . Let $a^2 = b = (3412)$ and $c = a^3 = (4123)$. We have $a^4 = e$. The powers of a form a group S of order 4. If s denotes a rotation of 180° about the axis 1–3 we have $s = (1432)$.

The coset sS is simply

$$s = (1432), \quad sa = (2143) = t, \\ sa^2 = (3214) = u, \quad sa^3 = (4321) = v;$$

these together with the powers of a exhaust the symmetries of the square:

	e	a	b	c	s	t	u	v
e	e	a	b	c	s	t	u	v
a	a	b	c	e	v	s	t	u
b	b	c	e	a	u	v	s	t
c	c	e	a	b	t	u	v	s
s	s	t	u	v	e	a	b	c
t	t	u	v	s	c	e	a	b
u	u	v	s	t	b	c	e	a
v	v	s	t	u	a	b	c	e

(b) The quaternion group.

This is obtained at once by the ordinary rules of multiplication of the quaternion units

	+1	+i	+j	+k	-1	-i	-j	-k
+1	+1	+i	+j	+k	-1	-i	-j	-k
+i	+i	-1	+k	-j	-i	+1	-k	+j
+j	+j	-k	-1	+i	-j	+k	+1	-i
+k	+k	+j	-i	-1	-k	-j	+i	+1
-1	-1	-i	-j	-k	+1	+i	+j	+k
-i	-i	+1	-k	+j	+i	-1	+k	-j
-j	-j	+k	+1	-i	+j	-k	-1	+i
-k	-k	-j	+i	+1	+k	+j	-i	-1

The two groups do not have the same structure since the group of symmetries has 5 elements of period 2 while the quaternion group has only one such element.