2. An Introduction to Group Theory

2.1. **Definitions.** In this section we introduce the concept of a *group*.

Definition 1. A *Group*, G, is a set of elements on which an operation * is defined satisfying

(a) $\forall A, B \in G, \quad A * B \in G.$ $A * B$ is unique. That is G is closed under $*$.
(b) $\forall A, B, C \in G, \quad A * (B * C) = (A * B) * C$. That is, * is associative.
(c) $\exists I \in G, \quad \forall A \in G, \quad A * I = I * A = A$. I is the *identity* in G.
(d) $\forall A \in G, \quad \exists B \in G, \quad A * B = B * A = I$. B is the *inverse* of A, and will be denoted by A^{-1}.

The identity is unique. For, if I_1, I_2 are two identities,

$$I_1 = I_1 * I_2 = I_2.$$

The first equality comes from the fact that I_2 is an identity, and the second comes from the fact that I_1 is an identity.

The inverse is also unique. If A has two inverses, B, C then

$$A*B = I. \quad \therefore C*(A*B) = C; \quad \therefore (C*A)*B = C; \quad \therefore I*B = C; \quad \therefore B = C.$$

Definition 2. If $\forall A, B \in G$ we have $A * B = B * A$ then G is called an *Abelian* group. If a given pair $A, B \in G$ satisfies $A * B = B * A$, they are said to *commute*.

Examples

(1) Any ring $(S, +, \cdot)$ with * being $+$. The identity is z, the zero element, and the inverse of a non-zero element $a \in S$ is $-a$. The resulting group is Abelian because addition in a ring is commutative.
(2) The set $1, 2, \ldots, p-1$ for any prime p with * being modular multiplication. The identity is 1, and the inverse of an element $a \in Z_p$ is p where $pa + qm = 1$.
(3) Z under addition. This is an *infinite* Abelian group.
(4) Let p be a prime. Let $(1/p, a/p, b/p)$ be a point in 3-dimensions, where a, b are integers with $1 \leq a, b \leq p-1$. Then the set of points
$$\left\{ (\{k/p\}, \{ka/p\}, \{kb/p\}), k \in Z \right\}$$
where $\{x\}$ = fractional part of x, form an Abelian group under addition. For an arbitrary prime p, this is a finite group.
(5) Let A be an $n \times s$ matrix of integers. Then the set of all integer linear combinations of the rows of A give an Abelian group under addition. This is also called a *lattice*. It is an infinite group.
(6) The set of $n \times n$ integer matrices whose determinant is ± 1. If A is such a matrix, then $A^{-1} = (1/det(A)) \cdot Adj(A)$, where $Adj(A)$ is the matrix whose elements are determinants of $(n-1) \times (n-1)$ minors of A, and are therefore integers. Therefore the set of matrices with

$*$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

$*$	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

FIGURE 1. Two groups of size 4

determinant ± 1 is closed under multiplication and inverse. This is another infinite group. It is a non-Abelian group.

(7) Let $S = \{I, A, B, C\}$. In how many ways can a group of size 4 be constructed from these elements? Two possibilities are shown in Figure 1. It will be shown later that these are the only groups of size 4.

Are these isomorphic? The definition of isomorphic for groups is essentially the same as for rings.

Definition 3. Two groups G_1, G_2 are isomorphic if there is a one-to-one and onto function $f : G_1 \to G_2$, such that

$$\forall A, B \in G_1, \quad f(A * B) = f(A) * f(B).$$

This implies that $f(I_1) = I_2$, and $f(A^{-1}) = (f(A))^{-1}$. The above two groups cannot be isomorphic because every element in the first one is its own inverse. This is not the case in the second one. However, the second group *is* isomorphic to the Abelian group of integers mod 4, under addition. Simply take $f : \{I, A, B, C\} = \{0, 1, 2, 3\}$. (Prove this.) See also exercise (1) in Section 2.5.

Any two finite groups can be represented by a table, as in the two groups in Figure 1. Then two groups of the same size are isomorphic if there exists a permutation of the rows and columns of the representating table for one which results in the table for the other.

How many non-isomorphic groups of size 3 are there? How many of size 2?

2.2. **Axioms for Finite Groups.** If G is a *finite* group then the four axioms for a group may be replaced by three. The first two are the same, but axioms (c), (d) may be combined into one axiom, namely:

$$\forall A, B, C \in G, \quad (A * C = B * C) \vee (C * A = C * B) \to \quad A = B.$$

To prove that this gives the same definition of a group we must show that the above statement implies that the axioms (c), (d) in the first definition hold.

Proof: Let $X \in G$ be arbitrary. Let the elements of G be $\{A_1, A_2, \ldots, A_k\}$, one of which is X. For each $j, 1 \leq j \leq k$, form $X * A_j$. There are k of these products, and every one must be distinct. For if $X * A_j = X * A_m$ then by the above axiom, $A_j = A_m$. Therefore if Z is an arbitrary element of G, one of the products must be Z. That is $X * A_j = Z$, for some j.

Similarly there is an integer $m, 1 \leq m \leq k$ with $A_m * X = Z$. With $Z = X$, this says that there are two elements U, V such that $U * X = X * V = X$. Then for arbitrary Z:

$$Z * V = A_m * X * V = A_m * X = Z; \quad U * Z = U * X * A_j = X * A_j = Z.$$

Therefore $U * Z = Z * V = Z$ for all $Z \in G$. Therefore $U * V = U = V$. Hence U is the identity.

In addition, for some j, $X * A_j = U$, and for some m, $A_m * X = U$, so that X has a left and right inverse. Let these be E, F. Then

$$E * X = U; \quad X * F = U;$$

$$\therefore E * X * F = U * F = F;$$

$$\therefore F = E * (X * F) = E * U = E.$$

That is each element has a unique inverse. This argument relies on G being finite.

What is being shown here is that, in the case of a finite group, the axioms given in Section 2.1 are not independent.

2.3. **The Order of an Element.** Let G be a finite group. If $A \in G$, then we can write $A*A = A^2$, and in general $A*A*\ldots*A$ (k terms) can be written as A^k. Denote A^0 by I and A^1 by A. The usual rules for exponents hold; for example $A^j * A^k = A^{j+k}$. By extension of this definition we will define A^{-k} to mean $(A^{-1})^k$. Let G be *finite* of size n. Then form the products

$$A^0, A^1, A^2, A^3, \ldots, A^n.$$

There are $n+1$ of these, and only n elements in G. Therefore by the pigeon hole principle two of them must be the same. That is, there are two distinct integers j, k, $0 \leq j, k \leq n$ such that $A^j = A^k$. Assume that $j < k$. (One must be less that the other.) Then by multiplying both sides by A^{-j} we get $A^{k-j} = I$.

Definition 4. Let G be an arbitrary. The smallest non-negative integer t such that $A^t = I$ is called the *order* of A in the group G. If G is finite, the number of elements in G is called the order of the group.

Definition 5. If G is a group of order n, and A is an element of order n in the group, then $G = A^0, A^1, A^2, A^3, \ldots, A^{n-1}$, and A is called a *generator* of G.

In the first of the two examples of groups of order 4 given in Section 2.1 all the elements have order 2. In the second example, A and C have order 4, and C has order 2. A requirement for two groups to be isomorphic is that they each have the same number of elements of a given order.

Examples

(8) If A has order t, and $A^q = I$, then $t|q$. For suppose that

$$q = at + r, 0 < r < t. \quad \therefore I = A^q = A^{at+r} = A^{at} * A^r = (A^t)^a * A^r = A^r$$

since $A^t = I$. Therefore $A^r = I$, which is a contradiction since $r < t$ and t is the smallest power of A to give I. $\therefore r = 0$, and $q = at$, i.e. $t \mid q$.

(9) If the group G has m elements, and if there is an element with order m, then for every k which divides m there is an element of order k. If an element A of G has order t, then $t|m$.

First, if $A \in G$ is an element of the group its order is $\leq m$. If the order was $t > m$, then $A^0, A^1, A^2, \ldots, A^{t-1}$ would be t distinct elements in G, which is impossible since G contains only $m < t$ elements. Therefore the order, t, of A is $\leq m$. If $k|m$ then $\frac{m}{k}$ is an integer, and $A^{\frac{m}{k}}$ has order k.

Suppose that A has order $t < m$. Then

$$A_1 = \{A^0 = I, A^1, A^2, \ldots, A^{t-1}\}$$

consists of t distinct elements of G. Since $t < m$ there is an element of G, say B_1 such that $B_1 \notin A_1$. Then

$$A_2 = \{B_1, B_1 * A, B_1 * A^2, \ldots, B_1 * A^{t-1}\}$$

gives t more distinct elements, none of which is in A_1, that is the sets $A_1, A_2, \ldots, A_r$ form a partition of G. (*Why?*) We can continue this process so long as the set $A_1 \cup A_2 \cup \ldots \cup A_r$ is not the whole of G. Each set A_j contains t distinct elements not in any other set A_i. Therefore the number of elements of G is a multiple of t.

Hence, the order of an element divides the order of the group.

(10) There is only one group (up to isomorphism) of size p for p a prime. These are groups in which every element is a power of one element, of the form $\{I, A, A^2, A^3, \ldots, A^{p-1}\}$. This is because the non-identity elements can have order p only. Such a group is called *cyclic*.

(11) If G has 4 elements, then every non-identity element may have order 2 or 4 only. If one element A is order 4, then the group is $\{I, A, A^2, A^3\}$, the cyclic group of size 4. This is the second group in example (7), Section 2.1.

If there is an element of order 2, say A, then the remaining 2 elements must also have order 2, since if either has order 4 then the group is the cyclic group. This is the first group in example (7), Section 2.1.

$*$	I	A	A^2	B	BA	AB
I	I	A	A^2	B	BA	AB
A	A	A^2	I	AB	B	BA
A^2	A^2	I	A	BA	AB	B
B	B	BA	AB	I	A	A^2
BA	BA	AB	B	A^2	I	A
AB	AB	B	BA	A	A^2	I

FIGURE 2. A non-Abelian group of order 6

There is only one group with 2, 3, 5 elements. How many 6 element groups are there? One example is given in Figure 2. This represents the group of rotations and reflections of an equilateral triangle.

2.4. **Subgroups of Groups.** Let G be a finite group with n elements. Let $A = \{A_1, A_2, \ldots, A_p\}$ be a subset of the elements of G. If B is a second subset of G, containing $\{B_1, B_2, \ldots, B_q\}$ then we define

$$A * B = \{X | \ X = A_r * B_s, \ \ 1 \leq k, \ \ 1 \leq q\}.$$

Definition A *subgroup* of a group G is a subset, H, of G which obey the group axioms. That is, H is closed under $*$, $I \in H$, and if $X \in H$, then $X^{-1} \in H$.

Examples

(12) The cyclic group of size 6, generated by $A^j, j = 0, 1, 2, 3, 4, 5$ has a subgroup of size 2 containing $\{I, A^3\}$. There is also a subgroup of size 3 containing $\{I, A^2, A^4\}$. Verify that there are subgroups of sizes 2,3 in the non-abelian group of size 6. Both of these are cyclic (see exercise (10) in 2.5).

(13) In the first group in example (7), Section 2.1, $\{I, A\}, \{I, B\}, \{I, C\}$ are subgroups. The second group in example (7) is cyclic, with $A^2 = B$ and $A^3 = C$. It also has a subgroup of order 2, namely $\{I, B\}$.

Theorem Let $H \subseteq G$. Then H is a subgroup if and only if $H * H = H$.

For example, if G is the cyclic group of size 6 and $H = \{I, A^2, A^4\}$, then $H * H = \{I, A^2, A^4, A^2,$
$A^4, A^6, A^4, A^6, A^8\} = H$, since $A^6 = I$.

Proof:

Only if: Let H be a subgroup of G. Form $H * H$. Since H contains I, then $H * H$ contains I. If $A \in H$ then $I * A \in H * H$. Therefore $H \subseteq H * H$. But since H is a group $H * H \subseteq H$. Therefore $H * H = H$.

If: Now suppose that $H * H = H$ Let $H = \{A_1, A_2, \ldots, A_p\}$. Form the products $A_1 * A_j, j = 1, 2, \ldots, p$. These all remain in H, and they are distinct *Why?*. Therefore for some j, $A_1 * A_j = A_1$. Therefore one element in H is I. In addition, since the p elements produce every element in H, then for some k, $A_1 * A_k = A_j$, the identity. Therefor, A_1^{-1} is in H. Therefore H is a subgroup of G.

Given a subgroup H and an element, P of G, not in H, then $K = P*H*P^{-1}$ is a subgroup isomorphic to H. It may actually coincide with H. In fact, if $P \in H$ then $P * H * P^{-1} = H$. (*Why?*)

Proof If $A, B \in K$ then $\exists C, D \in H, \quad A = P * C * P^{-1}, D = P * D * P^{-1}$. Then

$$A*B = P*C*P^{-1}*P*D*P^{-1} = P*C*I*D*P^{-1} = P*C*D*P^{-1} \quad \in K.$$

Hence K is closed under *.

Also, since $I \in H$, then $P*I*P^{-1} = I \in K$. And finally, if $P*A*P^{-1} \in K$, then its inverse is $P * A^{-1} * P^{-1}$. (exercise)

The isomorphism is

$$f(A) = P * A * P^{-1}.$$

We can now give a characterization of sets $H \subseteq G$ which are groups.

Theorem: H is a subgroup of G if and only if $\forall P \in G$ the set $P * H * P^{-1}$ is a subgroup.

Proof Let $K = P * H * P^{-1}$. Then, by an earlier theorem, K is a subgroup if and only if $K * K = K$. But

$$K*K = P*H*P^{-1}*P*H*P^{-1} = P*H*I*H*P^{-1} = P*H*H*P^{-1} = P*H*P^{-1} = K.$$

2.5. **Exercises.**

(1) Prove that the second group in Figure 1 is isomorphic to the non-zero elements of $\mathbb{Z}_5$ under multiplication.
(2) Derive a group of order 7. Explain how you get this.
(2) Find all subgroups of $\mathbb{Z}_{13}^+$ under multiplication.
(4) Find all subgroups of $\mathbb{Z}_{13}$ under addition.
(5) Let $S = \mathbb{R}^+ \times \mathbb{R}$. Define the binary operator $\circ$ on S by $(u, v) \circ (x, y) = (ux, vx+y)$. Prove that S is a group under $\circ$. Is it Abelian? Explain.
(6) Find all elements of order 12 in the cyclic group $\mathbb{Z}_{12}$ under addition.
(7) Find all the elements of order 10 in $\mathbb{Z}_{40}$.
(8) Find all the units in the ring $(\mathbb{Z}_{14}, +, \cdot)$. Prove that these form a group under multiplication.
(9) Prove that $\mathbb{Z}_6$ under $+$ is isomorphic to $\mathbb{Z}_7$ under $\times$. Are these groups cyclic? Explain. If they are cyclic, find an element whose order is 6.
(10) Prove that any subgroup of a cyclic group is cyclic.

Bibliography

Garrett Birkhoff and Saunders MacLane, *A Survey of Modern Algbra*, Macmillan Company, 1941.

David M. Burton, *Abstract Algebra*, Wm. C. Brown Publishers, 1988.

Ralph P. Grimaldi, *Discrete and Combinatorial Mathematics*, Addison-Wesley, 1989.

John D. Lipson, *Elements of Algebra and Algebraic Computing*, Addison-Wesley, 1981.