CHAPTER 2

Groups

DEFINITION (Binary Operation). Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.

NOTE. This condition of assigning an element of G to each ordered pair of G is called the closure of the set G under the given binary operation.

EXAMPLE. Addition, subtraction, and multiplication in $\mathbb{Z}$ are binary operations; division in $\mathbb{Z}$ is not ($8 \div 3 \notin \mathbb{Z}$).

EXAMPLE. Let $Z_n = \{0, 1, 2, \ldots, n-1\}$, the integers modulo n. Addition modulo n and multiplication modulo n are binary operations.

DEFINITION (Group). Let G be a nonempty set together with a binary operation on G (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element of G denoted by ab. G is a group under this operation if

(1) The operation is associative:

$$(ab)c = a(bc) \ \forall \ a, b, c \in G.$$

(2) There is an identity element e in G such that

$$ae = ea = a \ \forall \ a \in G.$$

(3) For each $a \in G$, there is an inverse element $b \in G$ such that

$$ab = ba = e.$$

NOTE. b is often denoted as a^{-1}.

A group G is Abelian (or commutative) if $ab = ba \; \forall \; a, b \in G$. It is non-Abelian if there exist $a, b \in G$ such that $ab \neq ba$.

EXAMPLE.

(1) $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are groups under $+$ with identity 0 and inverse $-a$ for a. None of these are groups under $\times$ since 1 is the multiplicative identity and so 0 has no inverse in each case.

However, $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ and $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ are groups under $\times$, but $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$ is not (e.g., 3 has no inverse).

(2) $\{1, -1, i, -i\}$ is a group under complex multiplication. 1 and -1 are their own inverses, and i and $-i$ are inverses of each other.

(3) The set S of positive irrational numbers along with 1 satisfy properties (1), (2), and (3) of the definition of group under $\times$. But S is not a group since $\times$ is not a binary operation on S. Closure fails (e.g., $\sqrt{2}\sqrt{2} = 2 \notin S$).

(4) Let $M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$, the set of 2×2 matrices with

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}.$$

M is a group with this operation. $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

(5) $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is a group under addition modulo n where, for $j > 0$, $n - j$ is the inverse of j. This is the group of integers modulo n.

(6) The determinant of the 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\det A = ad - bc$. Consider

$$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

with multiplication

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}.$$

Multiplication is closed in $GL(2, \mathbb{R})$ since $\det(AB) = (\det A)(\det B)$. Associativity is true, but messy; the identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is

$$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

This is the general linear group of 2×2 matricies over $\mathbb{R}$. Since

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} 10 & 13 \\ 22 & 29 \end{bmatrix} \text{ and } \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 11 & 16 \\ 19 & 28 \end{bmatrix},$$

$GL(2, \mathbb{R})$ is non-Abelian.

The set of all 2×2 matrices over $\mathbb{R}$ with matrix multiplication is not a group since matrices with 0 determinant do not have inverses.

(7) Consider $\mathbb{Z}_n$ with multiplication modulo n. Are there multiplicative inverses? If so, we have a group.

Suppose $a \in \mathbb{Z}_n$ and $ax \bmod n = 1$ has a solution (i.e., a has an inverse). Then $ax = qn + 1$ for some $q \in \mathbb{Z} \implies ax + n(-q) = 1 \implies a$ and n are relatively prime by Theorem 0.2.

Now suppose a is relatively prime to n. Then, again by Theorem 0.2,

$\exists\, s, t \in \mathbb{Z} \ni as+nt = 1 \implies as = (-t)n+1 \implies as \bmod n = 1 \implies s = a^{-1}$.

Thus we have proven Page 24 # 11:

LEMMA (Restatement of Page 24 # 11). *$a \in \mathbb{Z}$ has a multiplicative inverse modulo $n \iff a$ and n are relatively prime.*

DEFINITION ($U(n)$).

For each $n > 1$, define

$$U(n) = \{x \in \mathbb{Z}_n | x \text{ and } n \text{ are relatively prime}\}.$$

$U(n)$ will be a group under multiplication if multiplication modulo n is closed.

LEMMA. *If $a, b \in U(n)$, then $ab \in U(n)$.*

PROOF.

$a, b \in U(n) \implies \exists\ s_1, t_1, s_2, t_2 \in \mathbb{Z} \ni as_1 + nt_1 = 1$ and $bs_2 + nt_2 = 1 \implies as_1 = 1 - nt_1$ and $bs_2 = 1 - nt_2 \implies (ab)(s_1 s_2) = 1 - nt_1 - nt_2 + n^2 t_1 t_2 \implies (ab)(s_1 s_2) + n(t_1 + t_2 + n^2 t_1 t_2) = 1$.

Let $s = s_1 s_2$ and $t = t_1 + t_2 + n^2 t_1 t_2$. Then $(ab)s + nt = 1 \implies ab$ and n are relatively prime $\implies ab \in U(n)$. □

So multiplication modulo n is closed in $U(n)$, and $U(n)$ is an Abelian group.

EXAMPLE. Consider $U(14) = \{1, 3, 5, 9, 11, 13\}$.

mod 14	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

COROLLARY. *$\mathbb{Z}_n^*$ (the nonzero integers modulo n) is a group under multiplication modulo $n \iff n$ is prime.*

(8) $\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) | a_1, a_2, \ldots, a_n \in \mathbb{R}\}$ is an Abelian group under vector addition.

(9) For $(a, b, c) \in \mathbb{R}^3$, define $T_{a,b,c} : \mathbb{R}^3 \to \mathbb{R}^3$ by

$$T_{a,b,c}(x, y, z) = (x + a, y + b, z + c).$$

Then $T = \{T_{a,b,c} | a, b, c \in \mathbb{R}\}$ is a group under function composition.

$$T_{a,b,c} T_{d,e,f} = T_{a+d,b+e,c+f}.$$

$T_{0,0,0}$ is the identity, and the inverse of $T_{a,b,c}$ is $T_{-a,-b,-c}$. This translation group is Abelian.

(10) Let p be prime and $F \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p\}$.

The special linear group $SL(2, F)$ is

$$SL(2, F) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in F, ad - bc = 1 \right\},$$

where the operation is matrix multiplication (modulo p in $\mathbb{Z}_p$). It is a non-Abelian group. The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

In $SL(2, \mathbb{Z}_7)$, consider $A = \begin{bmatrix} 6 & 2 \\ 4 & 5 \end{bmatrix}$. $\det A = 6 \cdot 5 - 2 \cdot 4 = 22 = 1 \bmod 7$.

$$A^{-1} = \begin{bmatrix} 5 & -2 \\ -4 & 6 \end{bmatrix} = \begin{bmatrix} 5 & 5 \\ 3 & 6 \end{bmatrix} \bmod 7 \text{ since}$$

$$AA^{-1} = \begin{bmatrix} 6 & 2 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 5 & 5 \\ 3 & 6 \end{bmatrix} = \begin{bmatrix} 36 & 42 \\ 35 & 50 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 7 \text{ and}$$

$$A^{-1}A = \begin{bmatrix} 5 & 5 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 6 & 2 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} 50 & 35 \\ 42 & 36 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 7.$$

$GL(2, F)$ is also a group under matrix multiplication (modulo p for $\mathbb{Z}_p$). Also, in the case of $\mathbb{Z}_p$, interpret division by $ad - bc$ as multiplication by the inverse of $ad - bc$ modulo p. $GL(2, F)$ is non-Abelian.

In $GL(2, \mathbb{Z}_{11})$, consider $A = \begin{bmatrix} 9 & 6 \\ 8 & 7 \end{bmatrix}$. $\det A = 63 - 48 = 15 = 4 \bmod 11$. The inverse of 4 mod 11 is 3 mod 11 since $4 \cdot 3 = 12 = 1 \bmod 11$. Then

$$A^{-1} = \begin{bmatrix} 7 \cdot 3 & -6 \cdot 3 \\ -8 \cdot 3 & 9 \cdot 3 \end{bmatrix} = \begin{bmatrix} 21 & -18 \\ -24 & 27 \end{bmatrix} = \begin{bmatrix} 10 & 4 \\ 9 & 5 \end{bmatrix} \bmod 11 \text{ since}$$

$$AA^{-1} = \begin{bmatrix} 9 & 6 \\ 8 & 7 \end{bmatrix} \begin{bmatrix} 10 & 4 \\ 9 & 5 \end{bmatrix} = \begin{bmatrix} 144 & 66 \\ 143 & 67 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 11 \text{ and}$$

$$A^{-1}A = \begin{bmatrix} 10 & 4 \\ 9 & 5 \end{bmatrix} \begin{bmatrix} 9 & 6 \\ 8 & 7 \end{bmatrix} = \begin{bmatrix} 122 & 88 \\ 121 & 89 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 11.$$

THEOREM (2.1 — Uniqueness of the Identity).

The identity of a group G is unique.

PROOF. Suppose e and e' are identity elements of G. Then

$$e = ee' = e'$$

from the definition of identity element, so $e = e'$ and the identity is unique. □

THEOREM (2.2 — Cancellation).

In a group G, the right and left cancellation laws hold; that is, $ba = ca \implies b = c$ and $ab = ac \implies b = c$.

PROOF. Suppose $ba = ca$ and let a' be an inverse of a. Then

$(ba)a' = (ca)a' \implies b(aa') = c(aa')$ by associativity $\implies$

$be = ce \implies b = c$.

The proof for left cancellation is similar. □

THEOREM (2.3 — Uniqueness of Inverses).

For each element a in a group G, there exists a unique $b \in G$ such that $ab = ba = e$.

PROOF.

Suppose b and c are inverses of a. Then $ab = e$ and $ac = e \implies ab = ac \implies b = c$ by cancellation. □

NOTE. This allows us to ambiguously denote the inverse of $g \in G$ as g^{-1}.

NOTATION.

$$g^0 = e, \quad g^n = \underbrace{ggg \cdots g}_{n \text{ factors, } n \text{ positive}} \quad \text{(unambiguous by associativity).}$$

For $n < 0$,

$$g^n = (g^{-1})^{|n|}, \text{ e.g., } g^{-4} = (g^{-1})^4.$$

For every $m, n \in \mathbb{Z}$ snd $g \in G$,

$$g^m g^n = g^{m+n} \text{ and } (g^m)^n = g^{mn}.$$

However, in general,

$$(ab)^n \neq a^n b^n.$$

Translations to use if the group operation is "+" instead of "·."

multiplicative	additive
ab or $a \cdot b$	$a + b$
e or 1	0
a^{-1}	$-a$
a^n	na
ab^{-1}	$a - b$

THEOREM (2.4 — Socks-Shoes Property). *In a group G, $(ab)^{-1} = b^{-1}a^{-1}$.*

PROOF.

By definition and Theorem 2.3, $(ab)^{-1}$ is the unique element in G such that

$$(ab)(ab)^{-1} = (ab)^{-1}(ab) = e.$$

But

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

and

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

so

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

(In other words, $b^{-1}a^{-1}$ is the inverse of ab since it acts like an inverse, and the inverse is unique.) □

PROBLEM (Page 56 # 25).

A group G is Abelian $\iff$ $(ab)^{-1} = a^{-1}b^{-1}$ $\forall$ $a, b \in G$.

PROOF.

G is Abelian $\iff$ $ab = ba$ $\forall$ $a, b \in G$ $\iff$ $aba^{-1} = baa^{-1}$ $\iff$

$aba^{-1} = b$ $\iff$ $aba^{-1}b^{-1} = bb^{-1}$ $\iff$

$aba^{-1}b^{-1} = e$ $\iff$ $(ab)^{-1} = a^{-1}b^{-1}$. □

THEOREM (2). *If G is a group and $a, b \in G$, there exist unique $c, d \in G \ni ac = b$ and $da = b$ (i.e., the equations $ax = b$ and $xa = b$ have unique solutions in G).*

PROOF.

Let $c = a^{-1}b$. Then $ac = a(a^{-1}b) = (aa^{-1})b = eb = b$, so c is a solution of $ax = b$.

Suppose also $ac' = b$. Then

$$c = ec = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b = a^{-1}(ac') = (a^{-1}a)c' = ec' = c'.$$

Thus the solution of $ax = b$ is unique.

The proof of the second half is similar. □