2. Groups

2.1 Definitions

There are many situations where we encounter seemingly different objects, but where the same set of "rules" is obeyed. So even though they may appear different, there will be certain shared properties.

Definition
A **group** is a set G together with an operation $*$ on G (a way of combining elements of G together) such that:

1. G is **closed** under this operation;
$$a * b \in G \quad \text{for all } a, b \in G$$

2. The operation is **associative**:
$$a * (b * c) = (a * b) * c \quad \text{for all } a, b, c \in G$$

3. G contains an **identity element**:
$$\exists\, e \in G \text{ s.t. } \quad a * e = a = e * a \quad \text{for all } a \in G.$$

4. G is closed under **inverses**:
For each $a \in G$ there exists some element $a^{-1} \in G$ s.t.
$$a * a^{-1} = e = a^{-1} * a.$$

Often the operation is understood, & we write simply

ab instead of $a*b$.

clear about

Sometimes, we might need to be [redacted] what operation is being used, then we might write it out, as $a*b$ or $a \circ b$ or whatever is appropriate in the current context

IF the operation is commutative, [redacted] which means that

$$ab = ba \quad \text{for all } a, b \in G,$$

then G is said to be an abelian group

or a commutative group.

the

Ex: The group of symmetries of [redacted] square.

G is a set of 8 functions.

The operation is composition of functions.

This is a nonabelian group under this operation.

finite

Definition

The order of a group is the # of elements in the group (or the cardinality of the group if it is infinite).

Write:

$\#G$ or $|G|$ or $o(G)$ (our book (Herstein))

Ex: If $G = \{\text{symmetries of the square}\}$ then $\#G = 8$, or $|G| = 8$ or $o(G) = 8$

Generic group notations

When talking about a generic group, we usually use a "multiplicative-type" notation for the group operation. We write

ab	for	$a*b$
a^{-1}	for	inverse element
e	for	identity element

On the other hand, when talking specifically about an abelian group, we often use an "additive-type" notation, and write

$a+b$	for	$a*b$
$-a$	for	the inverse element
0	for	the identity element

In either case, this is just a notation to denote an operation. The actual operation might be an actual kind of multiplication or addition, or something much more exotic, like composition of functions.

Examples

a. $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ under $+$ (abelian)

b. $\mathbb{R}$ (real line) under $+$ (abelian)

Example

Consider $\mathbb{Z}$ under multiplication:

1. Closed under multiplication ✓
2. Multiplication is associative ✓
3. $\exists$ identity: $1n = n1 = n \ \forall n$ ✓
4. Inverses: NO.

   $\nexists$ integer n s.t. $2n = 1$.

NOT a group.

Example

Try $\mathbb{R}$ under multiplication.

Now 2 has an inverse: $2 \cdot \frac{1}{2} = 1$

But 0 does not: $\nexists x$ s.t. $0x = 1$

Example

$\mathbb{R}^* = \mathbb{R} \setminus \{0\} = \{x \in \mathbb{R} : x \neq 0\}$ under multiplication.

Exercise: This is a group. (& is abelian)

Example Let M be the set of all 2×2 invertible matrices. Exercise: Show this is a nonabelian group under the operation of matrix multiplication.

The identity element is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

The inverse of $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is

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

(Recall from linear algebra that

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible $\iff$ $\det(A) = ad - bc \neq 0$)

Example

Set $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$.

Define $m * n = mn \bmod 5$

where $k \bmod 5$ = remainder when k is divided by 5.

$$12 \bmod 5 = 2$$
$$28 \bmod 5 = 3$$
$$30 \bmod 5 = 0 \quad \text{etc}$$

This operation $*$ is a "multiplicative-like" operation.

Exercise: $\mathbb{Z}_5^\times$ is a group under $*$.
(& is abelian)

The identity element is 1

Find the inverse of each element: $1^{-1} = ?$

$2^{-1} = ?$

$3^{-1} = ?$

What is the multiplication table? $4^{-1} = ?$

Example An abelian group that contains 6 elements.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ (This is not exactly the def of $\mathbb{Z}_6$ that we'll use later, but it is an "isomorphic" def.)

Operation: $m \oplus n = m + n \bmod 6$.

"Multiplication" (Addition) table:

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1						
2			4			
3				0		
4					2	
5						4

Commutative!

Fill in the table!

$3 \oplus 3 = 0$ so the inverse of 3 is 3.

We are writing "additively," so we denote inverses by

$$-3 = 3$$

Similarly:

$-1 = 5$
$-2 = 4$
$-3 = 3$
$-4 = 2$
$-5 = 1$
$-0 = 0$

Exercise: Show $\oplus$ is commutative: $m \oplus n = n \oplus m$.

Show $\oplus$ is associative $(m \oplus n) \oplus k = m \oplus (n \oplus k)$

Associativity is harder to prove than commutativity.

Example

Let

$$GL_n(\mathbb{R}) = \{A : A \text{ is an invertible } n \times n \text{ matrix}\}$$

(we'll assume matrices have real entries, but this works for complex entries as well; we call that group $GL_n(\mathbb{C})$).

Exercise: $GL_n(\mathbb{R})$ is a group under matrix multiplication.

Show that $GL_1(\mathbb{R}) = \mathbb{R}^*$, the set of nonzero real nos. under ordinary multiplication.

Show that $GL_n(\mathbb{R})$ is nonabelian $\forall n \geq 2$.

Matrices do not commute: AB is usually not the same as BA

Examples: The affine group ("ax+b group")

Given $a, b \in \mathbb{R}$, $a \neq 0$, define a function

$$T_{a,b} : \mathbb{R} \to \mathbb{R} \quad \text{by} \quad T_{a,b}(x) = ax + b$$

Let

$$G = \{ T_{a,b} : a, b \in \mathbb{R},\ a \neq 0 \}$$

This is a set of functions!

Claim: G is a group under composition of functions.

Closure under composition

$$\begin{aligned}
(T_{a,b} \circ T_{c,d})(x) &= T_{a,b}(T_{c,d}(x)) \\
&= T_{a,b}(cx + d) \\
&= a(cx + d) + b \\
&= acx + ad + b \\
&= T_{ac,\, ad+b}(x).
\end{aligned}$$

So

$$T_{a,b} \circ T_{c,d} = T_{ac,\, ad+b} \in G.$$

This is the "multiplication rule" in this group!

Exercise: Show $T_{1,0}$ is the identity element.

Find $(T_{a,b})^{-1}$

Why don't we have to worry about associativity?

Thus, G is a group.

Exercise: Show G is nonabelian.

Remark
Not every operation is associative!

Example
Consider subtraction on $\mathbb{R}$:

$$(a-b)-c \neq a-(b-c) \quad !$$

Powers of an element: Assume G is a group.

Let $a \in G$. Then we set

$$a^n = \underbrace{a \cdots a}_{n \text{ times}} \quad \text{for } n \geq 1$$

$$a^0 = e$$

$$a^{-n} = \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ times}} \quad \text{for } n \geq 1$$

$$= (a^{-1})^n.$$

Note G closed under compositions — so all the powers must be in G

If G is finite then powers must repeat

Note: We use "multiplicative" notation when we are talking about general groups. If we know the operation is more like "addition" then we use an additive notation.

$$\underbrace{a + \cdots + a}_{n \text{ times}} = na$$

instead of a^n, call these multiples instead of powers

$-a$ instead of a^{-1}

$-a - \cdots - a = -na$ instead of a^{-n}

Ex. In the group $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ under multiplication.

Powers of 2:

$2^0 = 1$ $\qquad 2^{-1} = \frac{1}{2}$

$2^1 = 2$ $\qquad 2^{-2} = \frac{1}{4}$

$2^2 = 4 = 2 \cdot 2$

$2^3 = 8 = 2 \cdot 2 \cdot 2$

$\vdots$ $\qquad \vdots$

In the group $\mathbb{Z}$ under addition

"Powers" of 2:

Are Multiples of 2:

$0 \cdot 2 = 0$

$1 \cdot 2 = 2$

$2 \cdot 2 = 4 = 2 + 2$

$3 \cdot 2 = 6 = 2 + 2 + 2$

$-1 \cdot 2 = -2$

$-2 \cdot 2 = -4 = -2 - 2$

$\vdots$

Ex: In the group $\mathbb{Z}_7 = \{0,1,\dots,6\}$ under + mod 7
(addition mod 7)

$0 \cdot 2 = 0$
$1 \cdot 2 = 2$
$2 \cdot 2 = 4$
$3 \cdot 2 = 6$
$4 \cdot 2 = 1$
$5 \cdot 2 = 3$
$6 \cdot 2 = 5$
$7 \cdot 2 = 0$
Then they repeat!

$-2 = 5$ because $2+5=0$!
$-4 = -2-2 = 5+5 = 3$

Ex. In the group $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ under $\cdot$ mod 7

$2^0 = 1$
$2^2 = 2$
$2^3 = 4$
$2^4 = 1$!

Then the powers repeat. There are only 3 possible powers!

$$\{2^n \bmod 7 \mid n \in \mathbb{Z}\} = \{1,2,4\}$$