MATH 343 · GROUP THEORY · CHAPTER 2

Groups

Definition · Examples · Elementary Properties

Fahd M. Alshammari

Part 1 — Binary Operations and the Definition

GOAL. Turn the four properties observed in D_4 into a definition that applies to every algebraic system.

- What exactly is an operation on a set?
- The three axioms, and where closure hides
- Abelian and non-Abelian
- What must be checked, and in what order

Binary Operations

DEFINITION. Let G be a set. A **binary operation** on G is a function that assigns to each ordered pair of elements of G an element of G.

- The requirement that the result lies **in** G is called **closure**
- It is part of the definition of the operation, not a separate axiom
- The pair is **ordered**: ab and ba need not be the same

EXAMPLES. Addition, subtraction and multiplication of integers are binary operations on $\mathbb{Z}$.

When It Is Not a Binary Operation

Division is not a binary operation on $\mathbb{Z}$. An integer divided by an integer need not be an integer: $3 \div 2 \notin \mathbb{Z}$.

Well-definedness matters too. The correspondence on $\mathbb{Q}^+$ taking $\left(\frac{a}{b}, \frac{c}{d}\right)$ to $\frac{a+c}{b+d}$ is not a binary operation: the value depends on the representatives chosen, since

$$\frac{1}{2} = \frac{2}{4}, \qquad \text{but} \qquad \frac{1+1}{2+3} = \frac{2}{5} \neq \frac{3}{7} = \frac{2+1}{4+3}.$$

The Integers Modulo n

$$\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$$

carries two binary operations: **addition modulo** n and **multiplication modulo** n.

- In some situations, we use addition only; in others, both
- The context makes clear which is intended
- Recall: $ab \bmod n$ is the unique integer r with $ab = nq + r$ and $0 \leq r < n$

Definition of a Group

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

1. **Associativity.** $(ab)c = a(bc)$ for all a, b, c in G.
2. **Identity.** There is an element e in G with $ae = ea = a$ for all a in G.
3. **Inverses.** For each a in G there is b in G with $ab = ba = e$.

Reading the Definition

In words: a group is a set with an associative operation such that there is an identity, every element has an inverse, and **any pair of elements can be combined without leaving the set**.

HOW TO CHECK. In this order:

- **Closure** — is ab in G for all a, b in G? (Be sure to check this; see the irrationals below)
- **Associativity** — usually inherited, or from function composition
- **Identity** — exhibit it, and verify both sides
- **Inverses** — for *each* element, exhibit one, and verify both sides

Abelian and Non-Abelian

DEFINITION. A group G is **Abelian** if $ab = ba$ for every pair a, b in G. It is **non-Abelian** if there is *some* pair a, b with $ab \neq ba$.

- To prove Abelian: an argument valid for **all** pairs
- To prove non-Abelian: **one** explicit pair suffices
- When meeting a new group, determine at once whether it is Abelian

Part 2 — A Stock of Examples

GOAL. Build the collection of examples that every later theorem will be tested against.

- Additive groups of numbers, vectors and matrices
- Multiplicative groups: $\mathbb{R}^*$, $\mathbb{C}^*$, roots of unity
- Matrix groups $GL(2, F)$ and $SL(2, F)$
- $U(n)$: the units modulo n
- And, just as important, the **non**-examples

Additive Groups

EXAMPLE. $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are groups under ordinary addition. In each case the identity is 0 and the inverse of a is $-a$. All are Abelian.

EXAMPLE. $\mathbb{Z}_n$ is a group under addition modulo n. The identity is 0; for $j > 0$ the inverse of j is $n - j$.

EXAMPLE. $\mathbb{R}^n = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{R}\}$ is a group under componentwise addition, with identity $(0, \ldots, 0)$ and inverse $(-a_1, \ldots, -a_n)$.

Matrices Under Addition

EXAMPLE. The set of all 2×2 matrices with real entries is a group under componentwise addition:

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

The identity is the zero matrix, and the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$.

This group is Abelian.

The Complex Numbers

EXAMPLE. $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R},\ i^2 = -1\}$ is a group under

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

with identity 0 and inverse $-a - bi$.

EXAMPLE. The nonzero complex numbers $\mathbb{C}^*$ form a group under $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$, with

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\, i.$$

Multiplicative Groups of Numbers

EXAMPLE. $\mathbb{R}^*$, the nonzero reals under multiplication: identity 1, inverse $1/a$.

EXAMPLE. $\mathbb{Q}^+$, the positive rationals under multiplication: identity 1, inverse $1/a$.

EXAMPLE. $\{1, -1, i, -i\}$ under complex multiplication. Here -1 is its own inverse, and i and $-i$ are inverses of each other.

Each of these is Abelian.

Non-Examples (1)

$\mathbb{Z}$ **under multiplication is not a group.** The identity is 1, and property 3 fails: there is no integer b with $5b = 1$.

The positive irrationals together with 1, under multiplication, is not a group. All three axioms hold, but the set is **not closed**:

$$\sqrt{2} \cdot \sqrt{2} = 2.$$

Non-Examples (2)

$\{0,1,2,3\}$ **under multiplication modulo 4 is not a group.** 1 and 3 have inverses; 0 and 2 do not.

$\mathbb{Z}$ **under subtraction is not a group.** The operation is not associative:

$$(5-3)-2=0 \qquad \text{but} \qquad 5-(3-2)=4.$$

The set of all 2×2 **real matrices is not a group under matrix multiplication.** Inverses fail to exist whenever the determinant is 0.

The General Linear Group GL(2, $\mathbb{R}$)

DEFINITION. $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$, and

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

is a **non-Abelian group** under matrix multiplication.

- Closure follows from $\det(AB) = (\det A)(\det B)$
- Associativity holds by direct (cumbersome) calculation
- Identity: the 2×2 identity matrix

Inverses in GL(2, $\mathbb{R}$)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{pmatrix}$$

The formula explains the requirement $ad - bc \neq 0$ in the definition of $GL(2, \mathbb{R})$: **the determinant of a matrix decides whether it has an inverse.**

GL(2, $\mathbb{R}$) Is Non-Abelian

Take

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

both with determinant 1, so both lie in $GL(2, \mathbb{R})$. Then

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = BA.$$

The Special Linear Group

DEFINITION. For F any of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}_p$ (p prime), the set of 2×2 matrices over F with determinant 1 is a non-Abelian group under matrix multiplication, the **special linear group** $SL(2, F)$.

For $SL(2, F)$ the inverse formula simplifies to

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

When entries come from $\mathbb{Z}_p$, all arithmetic is done modulo p.

Worked Example: SL(2, $\mathbb{Z}_5$)

Let $A = \begin{pmatrix} 3 & 4 \\ 4 & 4 \end{pmatrix}$ with entries in $\mathbb{Z}_5$.

$$\det A = (3 \cdot 4 - 4 \cdot 4) \bmod 5 = (-4) \bmod 5 = 1,$$

so $A \in SL(2, \mathbb{Z}_5)$, and

$$A^{-1} = \begin{pmatrix} 4 & -4 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix} \pmod 5.$$

Check: $\begin{pmatrix} 3 & 4 \\ 4 & 4 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ modulo 5.

Worked Example: GL(2, $\mathbb{Z}_7$)

Let $B = \begin{pmatrix} 4 & 5 \\ 6 & 3 \end{pmatrix}$ over $\mathbb{Z}_7$. Then

$$\det B = (12 - 30) \bmod 7 = (-18) \bmod 7 = 3.$$

Division by $\det B$ means multiplication by $3^{-1} = 5$, since $3 \cdot 5 \equiv 1 \pmod 7$. Hence

$$B^{-1} = 5 \begin{pmatrix} 3 & -5 \\ -6 & 4 \end{pmatrix} = 5 \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 5 & 6 \end{pmatrix} \pmod 7.$$

The Units Modulo n

DEFINITION. For a positive integer n, let

$$U(n) = \{\, k \mid 1 \le k < n,\ \gcd(k, n) = 1 \,\}.$$

Then $U(n)$ is an **Abelian group** under multiplication modulo n.

- k has a multiplicative inverse modulo n **if and only if** $\gcd(k, n) = 1$ (Chapter 0, Exercise 13)
- The identity is 1; the inverse of k is the solution of $kx \equiv 1 \pmod{n}$
- If n is prime then $U(n) = \{1, 2, \ldots, n-1\}$

The Cayley Table of U(10)

$U(10) = \{1,3,7,9\}$, since these are the integers below 10 that are relatively prime to 10.

mod 10	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Worked Example: U(20)

$$U(20) = \{1,3,7,9,11,13,17,19\}, \qquad |U(20)| = 8.$$

Inverses, each found by solving $kx \equiv 1 \pmod{20}$:

k	1	3	7	9	11	13	17	19
k^{-1}	1	7	3	9	11	17	13	19

When Is {1, 2, …, n−1} a Group?

PROPOSITION. The set $\{1,2,\ldots,n-1\}$ is a group under multiplication modulo n **if and only if** n is prime.

- If n is prime, every k with $1 \leq k < n$ satisfies $\gcd(k,n) = 1$, so the set equals $U(n)$
- If n is composite, write $n = ab$ with $1 < a, b < n$; then a lies in the set but $\gcd(a,n) = a > 1$, so a has no inverse

EXAMPLE. $\{1,2,3\}$ is not a group modulo 4, but $\{1,2,3,4\}$ is a group modulo 5.

Part 3 — Elementary Properties of Groups

GOAL. Prove, from the axioms alone, facts that every group must satisfy.

- Every group has an identity. Could it have **more than one**?
- Every element has an inverse. Could it have **more than one**?
- The examples suggest not — but **EXAMPLES CANNOT PROVE**

We must argue abstractly, from the definition and nothing else.

Theorem 2.1 — Uniqueness of the Identity

THEOREM 2.1. In a group G there is only one identity element.

PROOF. Suppose e and e' are both identities of G. Then

$$ae = a \text{ for all } a \in G, \qquad e'a = a \text{ for all } a \in G.$$

Taking $a = e'$ in the first and $a = e$ in the second gives

$$e'e = e' \quad \text{and} \quad e'e = e.$$

Hence $e = e'$.

Theorem 2.2 — Cancellation

THEOREM 2.2. In a group G both cancellation laws hold: $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.

PROOF (RIGHT CANCELLATION). Suppose $ba = ca$ and let a' be an inverse of a. Multiplying **on the right** by a',

$$(ba)a' = (ca)a'.$$

By associativity $b(aa') = c(aa')$, so $be = ce$, and therefore $b = c$. Left cancellation is proved the same way, multiplying by a' **on the left**.

Quick Check — Applying Cancellation

In a group, $ab = cb$ allows us to conclude:

- **(A)** $a = c$
- **(B)** $b = e$
- **(C)** $a = b$
- **(D)** nothing without knowing the group is Abelian

Vote now — one answer only.

A Consequence — Every Group Table Is a Latin Square

Cancellation explains the pattern first observed in the D_4 table.

CLAIM. In the Cayley table of a group, each element occurs **exactly once** in each row and each column.

WHY. If an element appeared twice in the row of a, say $ab = ac$ with $b \neq c$, left cancellation would force $b = c$ — a contradiction. The column argument uses right cancellation.

Theorem 2.3 — Uniqueness of Inverses

THEOREM 2.3. For each element a in a group G there is a **unique** element b in G with $ab = ba = e$.

PROOF. Suppose b and c are both inverses of a. Then $ab = e$ and $ac = e$, so

$$ab = ac.$$

Cancelling a on the left gives $b = c$.

NOTATION. We may therefore write a^{-1} for the inverse of a.

Exponent Notation

For a positive integer n, associativity makes the product $\underbrace{gg\cdots g}_{n \text{ factors}}$ unambiguous, and we write it g^n. Define

$$g^0 = e, \qquad g^{-n} = \left(g^{-1}\right)^n.$$

The familiar laws of exponents hold for all integers m, n:

$$g^m g^n = g^{m+n}, \qquad (g^m)^n = g^{mn}.$$

Noninteger exponents such as $g^{1/2}$ are **not** defined in an abstract group.

The Laws of Exponents Have Limits

Although $g^m g^n = g^{m+n}$ holds for a **single** element, expressions in **two** elements do not behave like real numbers:

$$(ab)^2 = abab, \qquad \text{which need not equal } a^2b^2.$$

$$(ab)^{-2} = ((ab)^{-1})^2 = \left(b^{-1}a^{-1}\right)^2 = b^{-1}a^{-1}b^{-1}a^{-1}.$$

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

FACT. $(ab)^2 = a^2b^2$ **if and only if** $ab = ba$.

Quick Check — Inverse of a Product

For elements a, b of a group, $(ab)^{-1}$ equals:

- **(A)** $a^{-1}b^{-1}$
- **(B)** $b^{-1}a^{-1}$
- **(C)** $(ba)^{-1}$
- **(D)** ab

Vote now — one answer only.

Theorem 2.4 — Socks and Shoes

THEOREM 2.4. For group elements a and b,

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

PROOF. Compute

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

By Theorem 2.3 the inverse of ab is unique, so $(ab)^{-1} = b^{-1}a^{-1}$.

Solving Equations in a Group

CONSEQUENCE. For all a, b in a group G, each of the equations

$$ax = b \qquad \text{and} \qquad xa = b$$

has a **unique** solution in G, namely $x = a^{-1}b$ and $x = ba^{-1}$ respectively.

CONTRAST. In $\{0,1,2,3,4,5\}$ under multiplication modulo 6, the equation $2x = 4$ has solutions $x = 2$ and $x = 5$. This set is **not** a group under that operation.

Quick Check — Solving in Additive Notation

In $\mathbb{Z}_{12}$ under addition modulo 12, the solution of $5 + x = 2$ is:

- **(A)** $x = 3$
- **(B)** $x = 9$
- **(C)** $x = 7$
- **(D)** there is no solution

Vote now — one answer only.

Additive Notation

When the operation is written $+$, every definition must be translated.

Multiplicative group		Additive group	
ab	multiplication	$a + b$	addition
e or 1	identity	0	zero
a^{-1}	inverse of a	$-a$	additive inverse
a^n	power of a	na	multiple of a
ab^{-1}	quotient	$a - b$	difference

Common Errors to Avoid

- Verifying **one side** of the identity or inverse condition and stopping
- Forgetting to check **closure** — the positive irrationals satisfy all three axioms and still fail
- Concluding a group is Abelian from a few commuting pairs
- Writing $(ab)^n = a^n b^n$ in a non-Abelian group
- Writing $(ab)^{-1} = a^{-1}b^{-1}$ — this holds **only** when $ab = ba$
- Treating $\mathbb{Z}_n$ as a group under multiplication modulo n
- Reading a Cayley table product in the wrong order

What to Take Away

- A **group** is a set with an associative binary operation having a two-sided identity and two-sided inverses; closure is part of "binary operation"
- The stock of examples: $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{Q}^+$, $\mathbb{R}^n$, $U(n)$, $GL(2,F)$, $SL(2,F)$, D_n, the nth roots of unity
- Identities and inverses are **unique**; cancellation holds; $(ab)^{-1} = b^{-1}a^{-1}$
- $ax = b$ has exactly one solution — which is why every group table is a Latin square

Assigned exercises (Ch. 2): 4, 5, 6(b,d), 10, 13, 14, 16, 17, 27, 34, 36, 45, 47.