Chapter 1 – Introduction to Group Theory

Harley Caham Combest

Fa2025 MATH5353 Lecture Notes – Mk1

1.1: Basic Axioms and Examples

Historical Context. The group concept arose from several streams:

- **Number Theory.** Addition modulo n and multiplicative units modulo n.
- **Geometry.** Symmetries (rigid motions) of regular figures.
- **Permutation Theory.** Galois' analysis of permutations of roots of polynomials.

The axioms isolate the common algebraic pattern in these examples.

Binary Operations.

Definition 1. A *binary operation* on a set G is a function $*\colon G \times G \to G$. For $a, b \in G$, write $a * b$ for $*(a, b)$.

Definition 2. A binary operation $*$ on G is

- *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$;
- *commutative* if $a * b = b * a$ for all $a, b \in G$.

Calculative 1 (Binary operations)**.** *1.* $(\mathbb{Z}, +)$*: associative and commutative.*

2. $(\mathbb{Z}, -)$*: subtraction is a binary operation but is neither associative nor commutative.*

3. $(\mathbb{Z}^+, -)$*: not a binary operation (e.g.* $3 - 5 \notin \mathbb{Z}^+$*).*

Groups.

Definition 3. A *group* is a set G with a binary operation $*$ such that:

1. (Associativity) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
2. (Identity) There exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
3. (Inverses) For every $a \in G$ there exists $a^{-1} \in G$ with $a * a^{-1} = a^{-1} * a = e$.

If additionally $a * b = b * a$ for all $a, b \in G$, the group is *abelian*.

Calculative 2 (First encounters)**.** *1.* $(\mathbb{Z}, +)$*: identity* 0*, inverse of* a *is* $-a$*.*

2. $(\mathbb{Q} \setminus \{0\}, \cdot)$*: identity* 1*, inverse of* a *is* $a^{-1} = 1/a$*.*

3. $(\mathbb{Z} \setminus \{0\}, \cdot)$ *is not a group: e.g.* 2 *has no multiplicative inverse in* $\mathbb{Z}$*.*

4. $(\mathbb{Z}/n\mathbb{Z}, +)$ *is a finite abelian group of order* n*.*

Basic Properties (with full proofs).

Proposition 3 (Uniqueness and inverse algebra)**.** *Let* G *be a group. Then:*

1. The identity element is unique.

2. Each $a \in G$ *has a unique inverse.*

3. $(a^{-1})^{-1} = a$ *for all* $a \in G$*.*

4. $(ab)^{-1} = b^{-1}a^{-1}$ *for all* $a, b \in G$*.*

Proof. (1) Suppose e and f are identities. Then $e = e * f = f$ by the defining property of f and e. Hence $e = f$.

(2) Suppose b and c are both inverses of a. Then

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c,$$

where we used the existence of an identity e, associativity, and the inverse property. Hence inverses are unique.

(3) Since $a * a^{-1} = e$, a is an inverse of a^{-1}. By uniqueness of inverses, $(a^{-1})^{-1} = a$.

(4) Let $x := b^{-1}a^{-1}$. Then

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

and similarly

$$x(ab) = b^{-1}\,(a^{-1}a)\,b = b^{-1}\,e\,b = b^{-1}b = e.$$

Thus x is a two-sided inverse of ab, so by uniqueness of inverses, $(ab)^{-1} = x = b^{-1}a^{-1}$. □

Proposition 4 (Cancellation and linear equations)**.** *Let G be a group.*

1. *(Left/Right cancellation) If $au = av$, then $u = v$; if $ub = vb$, then $u = v$.*
2. *(Solving $ax = b$) For each $a, b \in G$, the equation $ax = b$ has the unique solution $x = a^{-1}b$.*
3. *(Solving $ya = b$) For each $a, b \in G$, the equation $ya = b$ has the unique solution $y = ba^{-1}$.*

Proof. (1) If $au = av$, multiply on the left by a^{-1} to get $u = v$. The right case is analogous.

(2) Existence: $x = a^{-1}b$ satisfies $a(a^{-1}b) = (aa^{-1})b = eb = b$. Uniqueness: If $ax = b$, then by left cancellation $x = a^{-1}b$.

(3) Existence: $y = ba^{-1}$ satisfies $(ba^{-1})a = b(a^{-1}a) = be = b$. Uniqueness: If $ya = b$, then by right cancellation $y = ba^{-1}$. □

Generalized Associative Law.

Proposition 5 (Bracket independence)**.** *For any $n \geq 1$ and any $a_1, \ldots, a_n \in G$, the product $a_1a_2\cdots a_n$ is well-defined (independent of parenthesization).*

Proof. Induct on n. For $n = 1, 2$ the claim is trivial; for $n = 3$ it is precisely associativity. Assume the statement holds up to $n = k$. Consider any parenthesization of $a_1 \cdots a_{k+1}$. It splits as $(A)(B)$, where A is a parenthesized product of the first r terms and B of the last $k + 1 - r$ terms, for some $1 \leq r \leq k$. By the induction hypothesis, $A = a_1 \cdots a_r$ and $B = a_{r+1} \cdots a_{k+1}$ regardless of their internal bracketing. Thus any parenthesization evaluates to $(a_1 \cdots a_r)(a_{r+1} \cdots a_{k+1})$. But any two such choices of r correspond to regroupings that are related by repeated use of associativity at the outermost level; hence all values coincide. Therefore the product is well-defined for $k + 1$. □

Notation. Henceforth for abstract groups we suppress $*$ and write ab for $a * b$. For $x \in G$ and $n \in \mathbb{Z}_{>0}$ define $x^n = \underbrace{xx\cdots x}_{n \text{ factors}}$, $x^{-n} = (x^{-1})^n$, and $x^0 = e$.

Order of an Element.

Definition 4. The *order* of $x \in G$, denoted $|x|$, is the least $n \in \mathbb{Z}_{>0}$ with $x^n = e$, if such an n exists; otherwise x has infinite order.

Lemma 6 (Divisibility characterization of powers)**.** *Let $x \in G$ have finite order $|x| = n$. Then for any $m \in \mathbb{Z}_{\geq 0}$, $x^m = e$ if and only if $n \mid m$.*

Proof. ($\Rightarrow$) By the Division Algorithm, write $m = qn+r$ with $q \in \mathbb{Z}_{\geq 0}$ and $0 \leq r < n$. Then

$$x^m = x^{qn+r} = (x^n)^q x^r = e^q x^r = x^r.$$

If $x^m = e$, then $x^r = e$. By minimality of n, we must have $r = 0$, hence $n \mid m$.

($\Leftarrow$) If $m = qn$, then $x^m = (x^n)^q = e^q = e$. □

Corollary 7. *If $|x| = n < \infty$, then the elements $e, x, x^2, \ldots, x^{n-1}$ are pairwise distinct, and $\langle x \rangle = \{x^k : k \in \mathbb{Z}\}$ has cardinality n.*

Proof. If $x^i = x^j$ with $0 \leq i < j \leq n-1$, then $e = x^{j-i}$ with $0 < j - i < n$, contradicting minimality of n. The subgroup $\langle x \rangle$ is precisely $\{e, x, \ldots, x^{n-1}\}$ since any x^k reduces to one of these by the Division Algorithm and the lemma. □

Lemma 8. *For any $x \in G$, $|x| = |x^{-1}|$ (including the infinite case).*

Proof. If $x^n = e$, then $(x^{-1})^n = (x^n)^{-1} = e$. Conversely, if $(x^{-1})^n = e$, invert both sides to get $x^n = e$. Minimal such n coincide. □

Calculative 9 (Orders in familiar groups)**.**

1. *In $(\mathbb{Z}, +)$ (viewed multiplicatively as $(\mathbb{Z}, \oplus)$ with a^n meaning n-fold $\oplus$), every nonzero element has infinite order.*
2. *In $(\mathbb{Z}/9\mathbb{Z}, +)$, $[6]$ has order 3 since $6 + 6 + 6 \equiv 0 \pmod 9$ and no smaller positive multiple of 6 is $0 \bmod 9$.*
3. *In $\big((\mathbb{Z}/7\mathbb{Z})^\times, \cdot\big)$, $[2]$ has order 3 because $2^3 = 8 \equiv 1 \pmod 7$ and $2, 2^2 \not\equiv 1 \pmod 7$.*

Further Calculative Checks.

Calculative 10 (Cancellation in practice)**.** *In $(\mathbb{Z}/12\mathbb{Z}, +)$, if $[a] + [x] = [a] + [y]$, then by adding $[-a]$ to both sides we obtain $[x] = [y]$. This models abstract left cancellation.*

Calculative 11 (Solving $ax = b$)**.** *In $\big((\mathbb{Z}/12\mathbb{Z})^\times, \cdot\big)$ the units are $[1], [5], [7], [11]$. Solve $[5]\,[x] = [7]$: multiply by $[5]^{-1} = [5]$ (since $5^2 \equiv 1 \bmod 12$) to get $[x] = [5][7] = [35] = [11]$.*

1.2: Dihedral Groups

Historical Context. The dihedral groups arise naturally as the groups of symmetries of regular polygons. If $n \geq 3$, let P_n be a regular n-gon in the plane. The rigid motions (rotations and reflections) that carry P_n to itself form a group under composition. This group has $2n$ elements and is called the *dihedral group of order* $2n$, denoted D_{2n}. The dihedral groups give some of the simplest non-abelian examples, and historically were among the first to be studied systematically in geometry.

Definition via Symmetries.

Definition 5. Fix $n \geq 3$. The *dihedral group* D_{2n} is the set of symmetries of a regular n-gon, with operation given by composition of functions. Thus D_{2n} consists of:

1. n rotations about the center, including the identity,
2. n reflections across symmetry axes of the polygon.

Proposition 12. $|D_{2n}| = 2n$.

Proof. Label the vertices $1, 2, \ldots, n$ clockwise. A symmetry is determined uniquely by the image of the ordered pair $(1, 2)$. Vertex 1 can be sent to any of n vertices. Once its image is chosen, vertex 2 must be sent either to the clockwise or counterclockwise adjacent vertex. Thus there are $2n$ possible placements, each realized by exactly one symmetry. Hence $|D_{2n}| = 2n$. □

Algebraic Presentation.

Proposition 13. *Let r be rotation clockwise by $2\pi/n$, and s reflection across the vertical axis through vertex 1. Then:*

1. $r^n = 1$,
2. $s^2 = 1$,
3. $srs = r^{-1}$.

Moreover, every element of D_{2n} can be written uniquely in the form r^k or sr^k with $0 \leq k < n$. Thus

$$D_{2n} = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1} \rangle.$$

Proof. (1) Rotating n times completes a full turn. (2) Reflecting twice is the identity. (3) Geometrically, conjugating a rotation by a reflection reverses orientation, so $srs = r^{-1}$. To see generation: every symmetry is either a rotation or reflection followed by a rotation. To see uniqueness: if $r^i = sr^j$, then r^i is orientation-preserving and sr^j is orientation-reversing, a contradiction. Similarly, $sr^i = sr^j \implies r^i = r^j \implies i \equiv j \pmod{n}$. □

Orders of Elements.

Proposition 14. *In D_{2n}:*

1. *$|r| = n$,*
2. *$|s| = 2$,*
3. *every reflection sr^k has order 2,*
4. *the subgroup $\langle r \rangle$ of rotations is cyclic of order n.*

Proof. (1) By construction $r^n = 1$ and no smaller positive power equals 1. (2) Immediate from $s^2 = 1$. (3) Compute $(sr^k)^2 = s(r^k s)r^k = (sr^{-k})r^k = s^2 = 1$, using $srs = r^{-1}$. (4) Clear: $\{1, r, r^2, \ldots, r^{n-1}\}$ is a cyclic subgroup of order n. □

Calculative 15 (Elements of D_6)**.** *For a regular triangle ($n = 3$), D_6 has 6 elements:*

$$\{1, r, r^2, s, sr, sr^2\}.$$

Here $|r| = 3$, and each of s, sr, sr^2 has order 2. D_6 is non-abelian, since $sr \neq rs$ but $sr = r^{-1}s$.

Calculative 16 (Square symmetries)**.** *For a square ($n = 4$), D_8 has 8 elements:*

$$\{1, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

Here r is 90° rotation, r^2 is 180°, and s is reflection across the vertical axis. Check: $(sr)^2 = 1$, but $rs \neq sr$.

Non-Abelianness.

Proposition 17. *D_{2n} is non-abelian for all $n \geq 3$.*

Proof. By the relation $srs = r^{-1}$, we obtain $sr \neq rs$ whenever $n \geq 3$ (since $r \neq r^{-1}$). Therefore the group is non-abelian. □

1.3: Symmetric Groups

Historical Context. The notion of permutation groups was crystallized in the work of Évariste Galois (1830s). Permutations describe the reordering of finite sets, and the group of all permutations of n objects is called the *symmetric group* S_n. These groups are fundamental: they encode all possible symmetries of a finite set, and every finite group can be realized as a subgroup of some S_n (Cayley's Theorem). They are the first and most important family of non-abelian finite groups.

Definition.

Definition 6. Let X be a finite set with $|X| = n$. A *permutation* of X is a bijection $\sigma\colon X \to X$. The set of all permutations of X, with composition as the operation, forms a group called the *symmetric group on* X, denoted S_X. When $X = \{1, 2, \ldots, n\}$, this group is denoted S_n and is called the *symmetric group of degree* n.

Proposition 18. $|S_n| = n!$.

Proof. A permutation is an injective function $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, hence also bijective. To define such σ, choose $\sigma(1)$ in n ways, then $\sigma(2)$ in $n-1$ ways, $\sigma(3)$ in $n-2$ ways, and so on, finally $\sigma(n)$ in 1 way. By the multiplication principle, the total is $n(n-1)(n-2)\cdots 1 = n!$. □

Cycle Notation.

Definition 7. A *cycle* $(a_1\, a_2\, \ldots\, a_m)$ in S_n denotes the permutation that sends $a_i \mapsto a_{i+1}$ for $1 \le i < m$, sends $a_m \mapsto a_1$, and fixes all other points.

Calculative 19. *In* S_5*, the cycle* $(1\,3\,5)$ *maps* $1 \mapsto 3$*,* $3 \mapsto 5$*,* $5 \mapsto 1$*, and fixes* $2, 4$*.*

Proposition 20. *Every permutation in* S_n *can be written uniquely (up to ordering of factors) as a product of disjoint cycles.*

Sketch. Starting from any $a \in \{1, \ldots, n\}$, follow the orbit $a, \sigma(a), \sigma^2(a), \ldots$ until it returns to a. This produces a cycle. Repeating with unused elements produces a decomposition into disjoint cycles. Uniqueness follows since the orbits under σ partition the set $\{1, \ldots, n\}$. □

Definition 8. The *length* of a cycle $(a_1\, a_2\, \ldots\, a_m)$ is m. A 1-cycle is the identity on that element, and by convention is often omitted in notation.

Orders of Permutations.

Proposition 21. *The order of a cycle of length m is m.*

Proof. Let $\sigma = (a_1\, a_2\, \ldots\, a_m)$. Then σ^k maps $a_i \mapsto a_{i+k}$, indices mod m. Thus $\sigma^m(a_i) = a_i$ for all i, so $\sigma^m = 1$. If $0 < k < m$ then $\sigma^k(a_1) = a_{1+k} \neq a_1$, so $\sigma^k \neq 1$. Hence the order of σ is m. □

Proposition 22. *Let $\sigma \in S_n$ have disjoint cycle decomposition with cycle lengths $m_1, \ldots, m_r$. Then the order of σ is $\operatorname{lcm}(m_1, \ldots, m_r)$.*

Proof. If $\sigma = \gamma_1\gamma_2\cdots\gamma_r$ with disjoint cycles γ_i of length m_i, then the cycles commute. Thus $\sigma^k = 1$ iff $\gamma_i^k = 1$ for all i. But $\gamma_i^k = 1$ iff $m_i \mid k$. Hence the order of σ is the least k divisible by all m_i, i.e. $\operatorname{lcm}(m_1, \ldots, m_r)$. □

Calculative Examples.

Calculative 23 (Cycle decomposition in S_3)**.** *The elements of S_3 are:*

$$1,\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2).$$

The three 2-cycles (transpositions) have order 2; the two 3-cycles have order 3.

Calculative 24 (Order computation in S_4)**.** *Let $\sigma = (1\,2\,3)(4\,5) \in S_5$. The cycle lengths are 3 and 2, so $|\sigma| = \operatorname{lcm}(3, 2) = 6$.*

Calculative 25 (Non-abelianness of S_n)**.** *In S_3, compute $(1\,2)(2\,3) = (1\,2\,3)$ while $(2\,3)(1\,2) = (1\,3\,2)$. Since these differ, S_3 is non-abelian. For $n \geq 3$, S_n contains S_3 as a subgroup, so S_n is non-abelian.*

Concluding Remarks. The symmetric groups S_n are the prototypical non-abelian finite groups. Their subgroup structure, conjugacy classes, and representations form the foundation for much of group theory.

1.4: Matrix Groups

Historical Context. Matrix groups arise when we consider invertible linear transformations of vector spaces. Given a field F, the set of all invertible $n \times n$ matrices with entries in F, under matrix multiplication, forms a group called the *general linear group*. These groups are central in linear algebra, geometry, and representation theory. They provide large families of finite non-abelian groups, as well as the prototypes for Lie groups in analysis.

Fields and Invertibility.

Definition 9. A *field* F is a set equipped with two operations $+$ and $\cdot$ such that:

1. $(F, +)$ is an abelian group with identity 0.
2. $(F \setminus \{0\}, \cdot)$ is an abelian group with identity 1.
3. Distributivity holds: $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

Definition 10. For $n \geq 1$, let $M_n(F)$ be the set of all $n \times n$ matrices with entries in F. Matrix multiplication is defined in the usual way and is associative.

Definition 11. The *general linear group* of degree n over F is

$$GL_n(F) = \{A \in M_n(F) : \det(A) \neq 0\},$$

with group operation given by matrix multiplication.

Basic Properties.

Proposition 26. *$GL_n(F)$ is a group under matrix multiplication.*

Proof. (Closure) If $A, B \in GL_n(F)$, then $\det(AB) = \det(A)\det(B) \neq 0$, hence $AB \in GL_n(F)$. (Associativity) Matrix multiplication is associative in $M_n(F)$. (Identity) The identity matrix I_n satisfies $AI_n = I_nA = A$ for all A. (Inverses) If $A \in GL_n(F)$ then $\det(A) \neq 0$, so A has an inverse matrix A^{-1} with entries in F. Then $AA^{-1} = A^{-1}A = I_n$. Hence $GL_n(F)$ is a group. □

Proposition 27. *$GL_n(F)$ is non-abelian for all $n \geq 2$.*

Proof. For $n = 2$, consider

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad BA = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Since $AB \neq BA$, the group is non-abelian. For $n > 2$, embed these 2×2 matrices in the upper-left corner of $n \times n$ identity matrices to produce non-commuting elements in $GL_n(F)$. Thus $GL_n(F)$ is non-abelian for all $n \geq 2$. □

Order in the Finite Case.

Theorem 28. *If $|F| = q$ is finite, then*

$$|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Proof. To construct an invertible matrix, choose its columns one by one:

- First column: any nonzero vector in F^n, so $q^n - 1$ choices.
- Second column: any vector not in the span of the first, so $q^n - q$ choices.
- Third column: any vector not in the span of the first two, so $q^n - q^2$ choices.
- Continue: for the k-th column, exclude the span of the previous $k-1$ columns, which has q^{k-1} elements.

Multiply to obtain the formula. □

Calculative Examples.

Calculative 29 ($GL_2(\mathbb{F}_2)$)**.** *The field $\mathbb{F}_2 = \{0, 1\}$ has $q = 2$ elements. Then*

$$|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 3 \cdot 2 = 6.$$

Thus $GL_2(\mathbb{F}_2)$ has order 6. In fact $GL_2(\mathbb{F}_2) \cong S_3$.

Calculative 30 (Exhibiting non-commutativity)**.** *In $GL_2(\mathbb{R})$, take*

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \quad BA = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}.$$

Since $AB \neq BA$, $GL_2(\mathbb{R})$ is non-abelian.

Calculative 31 (Determinant condition)**.** *In $M_2(\mathbb{R})$, the matrix*

$$C = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$$

has $\det(C) = 0$, so $C \notin GL_2(\mathbb{R})$. This illustrates the necessity of the determinant condition.

1.5: The Quaternion Group

Historical Context. Quaternions were discovered by William Rowan Hamilton in 1843 as a non-commutative extension of complex numbers. Their multiplicative structure contains a remarkable finite subgroup of order 8, called the *quaternion group*, denoted Q_8. This group is one of the smallest non-abelian groups and plays an important role in algebra and geometry. It also provides a counterexample to many naive conjectures about finite groups.

Definition.

Definition 12. The *quaternion group* is

$$Q_8 = \{\pm 1,\ \pm i,\ \pm j,\ \pm k\},$$

with multiplication determined by the rules

$$i^2 = j^2 = k^2 = -1, \qquad ij = k, \quad jk = i, \quad ki = j,$$

together with the relations $ji = -k$, $kj = -i$, $ik = -j$. Multiplication by -1 anticommutes: $(-1) \cdot a = a \cdot (-1) = -a$ for any $a \in Q_8$.

Proposition 32. *Q_8 is a group of order 8.*

Proof. (Closure) Products of generators reduce via the relations to one of the 8 listed elements. (Associativity) This is inherited from the associativity of quaternion multiplication in $\mathbb{H}$. (Identity) The element 1 satisfies $1 \cdot a = a \cdot 1 = a$. (Inverses) Each element is its own inverse up to sign: $i^{-1} = -i$, $j^{-1} = -j$, $k^{-1} = -k$, and $(-1)^{-1} = -1$. Therefore all group axioms hold and $|Q_8| = 8$. □

Orders of Elements.

Proposition 33. *In Q_8:*

1. $|1| = 1$, $|-1| = 2$,
2. $|i| = |j| = |k| = 4$,

3. elements $-i, -j, -k$ also have order 4.

Proof. Compute: $i^2 = -1$, so $i^4 = (i^2)^2 = (-1)^2 = 1$ and no smaller positive power of i is 1. Thus $|i| = 4$. Similarly for j, k. For $-i$, $(-i)^2 = (-1)^2 i^2 = i^2 = -1$, hence $(-i)^4 = 1$, so order 4. The cases $-j, -k$ are analogous. Clearly $|-1| = 2$. □

Non-Abelianness.

Proposition 34. *Q_8 is non-abelian.*

Proof. Compute $ij = k$ but $ji = -k \neq k$. Thus $ij \neq ji$, so Q_8 is non-abelian. □

Center and Subgroups.

Proposition 35. *The center of Q_8 is $Z(Q_8) = \{\pm 1\}$.*

Proof. Clearly ± 1 commute with all elements. Conversely, suppose $x \in Q_8$ commutes with i. If $x \in \{\pm j, \pm k\}$, then $xi = -ix \neq ix$, so x does not commute with i. Thus the only central elements are ± 1. □

Proposition 36. *Q_8 has subgroups*

$$\langle i \rangle = \{1, -1, i, -i\}, \quad \langle j \rangle = \{1, -1, j, -j\}, \quad \langle k \rangle = \{1, -1, k, -k\},$$

each cyclic of order 4, and the subgroup $\{1, -1\}$ of order 2.

Proof. Each listed subset is easily verified closed under multiplication, contains inverses, and the identity. The orders follow from the element orders proved above. □

Calculative Examples.

Calculative 37 (Multiplication table)**.** *The full multiplication table of Q_8 is:*

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Calculative 38 (Checking subgroup)**.** *Consider $\{1, -1, i, -i\}$. Multiplying any two elements stays within the set, e.g. $i \cdot (-i) = -1$, $(-i) \cdot (-i) = -1$, etc. Thus this is a subgroup of order 4.*

1.6: Homomorphisms and Isomorphisms

Historical Context. The language of *homomorphisms* captures "structure-preserving" maps between groups. Rather than studying a group in isolation, we compare it to others via maps that respect the multiplication. This viewpoint unlocks classification results, reduction of problems from one group to another, and ultimately the fundamental isomorphism theorems.

Definitions and Basic Consequences.

Definition 13. Let $(G, \cdot)$ and $(H, *)$ be groups. A function $\varphi : G \to H$ is a *group homomorphism* if for all $x, y \in G$,

$$\varphi(x \cdot y) = \varphi(x) * \varphi(y).$$

If φ is bijective and a homomorphism, it is an *isomorphism*; in this case we write $G \cong H$.

Definition 14. For a homomorphism $\varphi : G \to H$ the *kernel* and *image* are

$$\ker \varphi = \{g \in G : \varphi(g) = e_H\}, \qquad \operatorname{Im} \varphi = \{\varphi(g) : g \in G\} \leq H.$$

Proposition 39 (Homomorphisms preserve identity, inverses, and powers)**.** *Let $\varphi : G \to H$ be a homomorphism. Then*

1. *$\varphi(e_G) = e_H$.*
2. *$\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G$.*
3. *$\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$ and $x \in G$ (where $x^0 = e_G$ and $x^{-n} = (x^{-1})^n$).*

Proof. (1) Since $e_G \cdot e_G = e_G$ we have $\varphi(e_G) = \varphi(e_G) * \varphi(e_G)$. Left-cancel $\varphi(e_G)$ in H to obtain $\varphi(e_G) = e_H$.

(2) $e_H = \varphi(e_G) = \varphi(xx^{-1}) = \varphi(x) * \varphi(x^{-1})$, so $\varphi(x^{-1}) = \varphi(x)^{-1}$.

(3) For $n \geq 0$, use induction: the case $n = 0$ is (1), and $\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n \varphi(x) = \varphi(x)^{n+1}$. For $n < 0$, write $n = -m$ with $m > 0$: $\varphi(x^n) = \varphi((x^{-1})^m) = \varphi(x^{-1})^m = \varphi(x)^{-m} = \varphi(x)^n$. □

Proposition 40 (Kernel and image are subgroups)**.** *Let $\varphi : G \to H$ be a homomorphism. Then* $\ker\varphi \leq G$ *and* $\operatorname{Im}\varphi \leq H$*.*

Proof. For $\ker\varphi$: $e_G \in \ker\varphi$ by the previous proposition. If $a, b \in \ker\varphi$ then $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H e_H^{-1} = e_H$, hence $ab^{-1} \in \ker\varphi$. Thus $\ker\varphi \leq G$ by the one-step subgroup test.

For $\operatorname{Im}\varphi$: If $y_1 = \varphi(a)$ and $y_2 = \varphi(b)$ lie in the image, then $y_1 y_2^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \operatorname{Im}\varphi$. Also $e_H = \varphi(e_G) \in \operatorname{Im}\varphi$. Hence $\operatorname{Im}\varphi \leq H$. □

Proposition 41 (Injectivity and the kernel)**.** *A homomorphism $\varphi : G \to H$ is injective if and only if* $\ker\varphi = \{e_G\}$*.*

Proof. ($\Rightarrow$) If φ is injective and $x \in \ker\varphi$, then $\varphi(x) = e_H = \varphi(e_G)$, so $x = e_G$.

($\Leftarrow$) If $\ker\varphi = \{e_G\}$ and $\varphi(x) = \varphi(y)$, then $e_H = \varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1})$. Hence $xy^{-1} \in \ker\varphi$, so $xy^{-1} = e_G$, i.e. $x = y$. □

Isomorphisms and Invariants.

Definition 15. A bijective homomorphism $\varphi : G \to H$ is an *isomorphism*; a bijective homomorphism $G \to G$ is an *automorphism*. The set of automorphisms of G is denoted $\operatorname{Aut}(G)$ (with composition as the operation).

Proposition 42 (Inverse of an isomorphism)**.** *If $\varphi : G \to H$ is an isomorphism, then $\varphi^{-1} : H \to G$ is also a homomorphism (hence an isomorphism).*

Proof. Let $a, b \in H$. Since φ is bijective, choose $x, y \in G$ with $\varphi(x) = a$ and $\varphi(y) = b$. Then

$$\varphi^{-1}(ab) = \varphi^{-1}(\varphi(x)\varphi(y)) = \varphi^{-1}(\varphi(xy)) = xy = \varphi^{-1}(a)\,\varphi^{-1}(b).$$

Thus φ^{-1} is a homomorphism. □

Proposition 43 (Isomorphism invariants)**.** *If $\varphi : G \xrightarrow{\cong} H$ is an isomorphism, then:*

1. $|G| = |H|$ *(finite order).*
2. *G is abelian $\iff$ H is abelian.*
3. *For each $x \in G$, $|\varphi(x)| = |x|$ (orders of elements are preserved).*
4. *G is cyclic $\iff$ H is cyclic; more generally, $\varphi(\langle x\rangle) = \langle\varphi(x)\rangle$.*

Proof. (1) A bijection preserves cardinality. (2) If G is abelian, then for $a, b \in H$ write $a = \varphi(x)$, $b = \varphi(y)$. Then $ab = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = ba$. The converse follows by symmetry. (3) Since $\varphi(x^n) = \varphi(x)^n$, we have $\varphi(x)^n = e_H \iff x^n = e_G$. Thus the least positive such n is the same in G and H. (4) If $G = \langle x \rangle$, then $\operatorname{Im}\varphi = \langle \varphi(x) \rangle = H$ by surjectivity. Conversely, if $H = \langle y \rangle$ and φ is an isomorphism, let $x = \varphi^{-1}(y)$; then $G = \langle x \rangle$. The equality $\varphi(\langle x \rangle) = \langle \varphi(x) \rangle$ follows because $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$. □

Orders Through a Homomorphism.

Proposition 44 (Order divides under homomorphism)**.** *Let $\varphi : G \to H$ be a homomorphism and $x \in G$ have finite order $|x| = n$. Then $|\varphi(x)|$ divides n. Moreover, $|\varphi(x)| = n$ if and only if $\ker\varphi \cap \langle x \rangle = \{e_G\}$, equivalently if $\varphi|_{\langle x \rangle}$ is injective.*

Proof. Since $\varphi(x)^n = \varphi(x^n) = \varphi(e_G) = e_H$, the order $m = |\varphi(x)|$ divides n. If $\varphi|_{\langle x \rangle}$ is injective, then $x^k = e_G$ is the only solution of $\varphi(x^k) = e_H$, hence $m = n$. Conversely, if $m = n$, then $\varphi(x^k) = e_H \Rightarrow n \mid k$, so $x^k = e_G$; thus the restriction is injective. □

Standard Constructions and Examples.

Proposition 45 (Composition)**.** *If $\varphi : G \to H$ and $\psi : H \to K$ are homomorphisms, then $\psi \circ \varphi : G \to K$ is a homomorphism.*

Proof. For all $x, y \in G$, $(\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = (\psi \circ \varphi)(x)\,(\psi \circ \varphi)(y)$. □

Proposition 46 (Inner automorphisms)**.** *Fix $g \in G$. The map $\iota_g : G \to G$ defined by $\iota_g(x) = gxg^{-1}$ is an automorphism.*

Proof. $\iota_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \iota_g(x)\,\iota_g(y)$, so ι_g is a homomorphism. It is bijective with inverse $\iota_{g^{-1}}$, hence an automorphism. □

Calculative Examples.

Calculative 47 (Reduction modulo n)**.** *$\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\varphi(k) = [k]_n$ is a surjective homomorphism. Kernel:* $\ker\varphi = n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$. *By injectivity criterion, φ is injective iff $n = 1$.*

Calculative 48 (Determinant)**.** *$\det : GL_n(F) \to F^\times$ is a surjective homomorphism. Kernel:* $\ker(\det) = SL_n(F) = \{A \in GL_n(F) : \det A = 1\}$, *a subgroup of $GL_n(F)$.*

Calculative 49 (Sign of a permutation)**.** $\operatorname{sgn} : S_n \to \{\pm 1\}$ *is a surjective homomorphism with kernel* A_n *(the alternating group). Hence* $S_n/A_n \cong \{\pm 1\}$ *(the quotient is discussed in later chapters).*

Calculative 50 (Orientation homomorphism on dihedral groups)**.** *Define* $\varepsilon : D_{2n} \to C_2 = \{\bar{0}, \bar{1}\}$ *by* $\varepsilon(r^k) = \bar{0}$ *(orientation-preserving),* $\varepsilon(sr^k) = \bar{1}$ *(orientation-reversing). Then* ε *is a surjective homomorphism with kernel* $\langle r \rangle \cong C_n$*.*

Calculative 51 (Injective but not surjective)**.** $\varphi : \mathbb{Z} \to \mathbb{Z}$*,* $\varphi(k) = 3k$ *is a homomorphism. Kernel* $\{0\}$*, hence injective. Image* $3\mathbb{Z} \neq \mathbb{Z}$*, so not surjective.*

Remarks. The study of kernels and images foreshadows the isomorphism theorems: roughly, a homomorphism $G \to H$ factors G into its kernel and image. Formal statements and proofs require quotient groups and will appear in later chapters.

1.7: Group Actions

Historical Context. The concept of a group action formalizes the idea of a group "acting as symmetries" on a set. It arose in the 19th century in the study of permutation representations of groups (Cayley's Theorem). Group actions connect algebra to geometry, combinatorics, and number theory: they allow us to count orbits, study stabilizers, and understand the structure of groups via their interaction with other objects.

Definition.

Definition 16. Let G be a group and X a set. A *(left) group action* of G on X is a map

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

satisfying:

1. $e \cdot x = x$ for all $x \in X$,
2. $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$, $x \in X$.

Definition 17. For $g \in G$, the map $\alpha_g : X \to X$, $\alpha_g(x) = g \cdot x$ is a permutation of X. The homomorphism $\varphi : G \to S_X$ defined by $g \mapsto \alpha_g$ is called the *permutation representation* associated with the action.

Orbits and Stabilizers.

Definition 18. For $x \in X$:

- The *orbit* of x is $G \cdot x = \{g \cdot x : g \in G\}$.
- The *stabilizer* of x is $\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$.

Proposition 52. $\mathrm{Stab}_G(x) \leq G$.

Proof. If $g, h \in \mathrm{Stab}_G(x)$ then $(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x$, so $gh^{-1} \in \mathrm{Stab}_G(x)$. Also $e \cdot x = x$, so $e \in \mathrm{Stab}_G(x)$. Hence $\mathrm{Stab}_G(x)$ is a subgroup of G. □

Orbit–Stabilizer Theorem.

Theorem 53 (Orbit–Stabilizer)**.** *Let G act on X, and $x \in X$. Then*

$$|G \cdot x| = [G : \mathrm{Stab}_G(x)] = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

Proof. Define $\varphi : G \to G \cdot x$ by $\varphi(g) = g \cdot x$. If $g_1 \cdot x = g_2 \cdot x$, then $(g_2^{-1} g_1) \cdot x = x$, so $g_2^{-1} g_1 \in \mathrm{Stab}_G(x)$, hence $g_1 \mathrm{Stab}_G(x) = g_2 \mathrm{Stab}_G(x)$. Thus φ factors through the coset space $G/\mathrm{Stab}_G(x)$, and induces a well-defined bijection

$$G/\mathrm{Stab}_G(x) \longrightarrow G \cdot x, \quad g\mathrm{Stab}_G(x) \mapsto g \cdot x.$$

Therefore $|G \cdot x| = [G : \mathrm{Stab}_G(x)]$. If G is finite, $[G : \mathrm{Stab}_G(x)] = |G|/|\mathrm{Stab}_G(x)|$. □

Transitive and Faithful Actions.

Definition 19. An action of G on X is:

- *transitive* if $G \cdot x = X$ for some (equivalently any) $x \in X$,
- *faithful* if the associated homomorphism $\varphi : G \to S_X$ is injective, i.e. if the only element acting trivially on X is e.

Proposition 54 (Cayley's Theorem)**.** *Every group G is isomorphic to a subgroup of S_G.*

Proof. Let G act on itself by left multiplication: $g \cdot x = gx$. The associated map $\varphi : G \to S_G$, $\varphi(g)(x) = gx$ is a homomorphism. If $\varphi(g) = \mathrm{id}$, then $gx = x$ for all $x \in G$, in particular $g = e$. Thus φ is injective. Therefore $G \cong \varphi(G) \leq S_G$. □

Calculative Examples.

Calculative 55 (Dihedral group action on vertices)**.** *D_{2n} acts on the set of vertices of a regular n-gon by permutation. For $n = 4$, D_8 acts transitively on the set $\{1, 2, 3, 4\}$. Stabilizer of vertex 1 has size 2 (the identity and the reflection fixing vertex 1), so orbit–stabilizer gives orbit size $8/2 = 4$, which equals the number of vertices.*

Calculative 56 (Symmetric group action on subsets)**.** *S_n acts on the set of k-element subsets of $\{1, \ldots, n\}$ by permutation. This action is transitive: any k-subset can be mapped to any other by a suitable permutation.*

Calculative 57 (Faithful action of $\mathbb{Z}_n$ on the n-th roots of unity)**.** *Let $G = \mathbb{Z}_n = \langle 1 \rangle$. Define $k \cdot \zeta = \zeta^k$ for ζ an n-th root of unity. This is a faithful action: if $k \cdot \zeta = \zeta$ for all ζ, then $\zeta^{k-1} = 1$ for all primitive ζ, so $n \mid (k-1)$, i.e. $k \equiv 1 \pmod{n}$.*