MATH 343 · GROUP THEORY · CHAPTER 6

Isomorphisms

Definition and Examples · Properties of Isomorphisms · Automorphisms · Cayley's Theorem

Fahd M. Alshammari

Part 1 — What an Isomorphism Is

GOAL. Make precise what it means for two groups to be the same group written in different notation.

- The definition, and the four steps of a proof
- Examples: cyclic groups, $\mathbb{R}$ and $\mathbb{R}^+$, conjugation of matrices
- Non-examples, and how to prove that no isomorphism exists

Same Group, Different Names

- D_4 has already appeared twice: as motions of a square ($R_{90}, H, \ldots$) in Chapter 1, and as permutations of its corners ($(1234), (12)(34), \ldots$) in Chapter 5
- In a cyclic group $\langle a \rangle$ of order n, $a^r a^s = a^{(r+s) \bmod n}$: multiplying powers of a is adding exponents mod n

$U(43)$ and $U(49)$ are both cyclic of order 42. Are they the same group?

Definition — Group Isomorphism

DEFINITION. Let G and $\overline{G}$ be groups. A map $\varphi: G \to \overline{G}$ is an **isomorphism** if

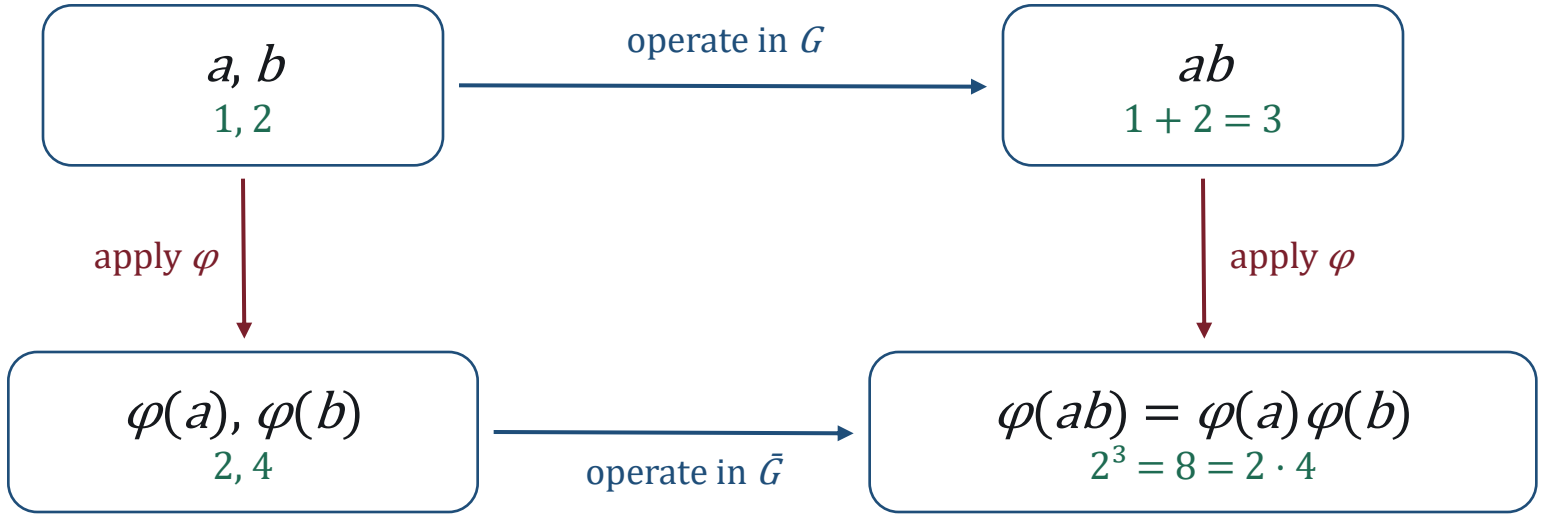
- φ is one-to-one,
- φ is onto, and
- φ preserves the operation: $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

If there is an isomorphism $\varphi: G \to \overline{G}$, then G and $\overline{G}$ are **isomorphic**, written $G \cong \overline{G}$.

- In $\varphi(ab)$ the product is taken in G; in $\varphi(a)\varphi(b)$ it is taken in $\overline{G}$
- Gallian's book writes $G \approx \overline{G}$ for $G \cong \overline{G}$

Operate, Then Map — or Map, Then Operate

EXAMPLE. Operation-preserving means the two routes around the square below always end at the same element.



Green: Example 1, ϕ(x) = 2^x from $\mathbb{R}$ under addition to $\mathbb{R}^+$ under multiplication, with a = 1, b = 2. Across the top then down, or down then across the bottom: both routes end at 8.

Which Operation Goes Where

WARNING. Use each group's own operation on each side. For $\varphi: \mathbb{R} \to \mathbb{R}^+$, from addition to multiplication, the condition reads $\varphi(a+b) = \varphi(a)\varphi(b)$.

operation in G	operation in $\bar{G}$	operation-preserving means
·	·	ϕ(a · b) = ϕ(a) · ϕ(b)
·	+	ϕ(a · b) = ϕ(a) + ϕ(b)
+	·	ϕ(a + b) = ϕ(a) · ϕ(b)
+	+	ϕ(a + b) = ϕ(a) + ϕ(b)

Proving G ≅ Ḡ in Four Steps

First define a map $\varphi: G \to \overline{G}$ by a formula. Then check:

Step 1 (well defined). For every $x \in G$, $\varphi(x)$ is one element of $\overline{G}$ — the same element however x is written.

Step 2 (one-to-one). If $a, b \in G$ and $\varphi(a) = \varphi(b)$, then $a = b$.

Step 3 (onto). For every $y \in \overline{G}$ there is $x \in G$ with $\varphi(x) = y$.

Step 4 (operation-preserving). $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

If all four steps hold, φ is an isomorphism and $G \cong \overline{G}$.

$\mathbb{R}$ Under Addition and $\mathbb{R}^+$ Under Multiplication

EXAMPLE. Let $\mathbb{R}$ be the reals under addition and $\mathbb{R}^+$ the positive reals under multiplication. Define $\varphi: \mathbb{R} \to \mathbb{R}^+$ by $\varphi(x) = 2^x$.

Step 1 (well defined). For $x \in \mathbb{R}$, 2^x is a positive real number, so $\varphi(x) \in \mathbb{R}^+$.

Step 2 (one-to-one). If $\varphi(x) = \varphi(y)$, then $2^x = 2^y$; taking $\log_2$ gives $x = y$.

Step 3 (onto). Let $y \in \mathbb{R}^+$. Then $x = \log_2 y \in \mathbb{R}$ and $\varphi(x) = 2^{\log_2 y} = y$.

Step 4 (operation-preserving). For $x, y \in \mathbb{R}$, $\varphi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x)\varphi(y)$.

So φ is an isomorphism, and $\mathbb{R} \cong \mathbb{R}^+$.

Cyclic Groups Are $\mathbb{Z}$ or $\mathbb{Z}_n$ in Disguise

PROPOSITION. Let $G = \langle a \rangle$ be a cyclic group.

(1) If $|a| = n$, then $\varphi: G \to \mathbb{Z}_n$, $\varphi(a^k) = k \bmod n$, is an isomorphism. So $G \cong \mathbb{Z}_n$.

(2) If $|a|$ is infinite, then $\varphi: G \to \mathbb{Z}$, $\varphi(a^k) = k$, is an isomorphism. So $G \cong \mathbb{Z}$.

CONSEQUENCE. Two cyclic groups of the same order are isomorphic: if $|a| = |b| = n$, the same four steps show that $a^k \mapsto b^k$ is an isomorphism from $\langle a \rangle$ to $\langle b \rangle$. So $U(43) \cong U(49)$.

Proof of the Proposition — |a| = n

PROOF (FINITE ORDER). Every element of G is a power a^k with $k \in \mathbb{Z}$, and by Theorem 4.1, $a^i = a^j$ exactly when n divides $i - j$. Define $\varphi: G \to \mathbb{Z}_n$ by $\varphi(a^k) = k \bmod n$.

Step 1 (well defined). One element may be written a^i and also a^j, so we check that both names give the same value. If $a^i = a^j$, then n divides $i - j$, so $i \bmod n = j \bmod n$.

Step 2 (one-to-one). If $\varphi(a^i) = \varphi(a^j)$, then $i \bmod n = j \bmod n$, so n divides $i - j$, and therefore $a^i = a^j$ by Theorem 4.1.

Proof of the Proposition — |a| = n, Continued

Step 3 (onto). Let $r \in \mathbb{Z}_n = \{0,1,\ldots,n-1\}$. Then $a^r \in G$ and $\varphi(a^r) = r$.

Step 4 (operation-preserving). G is written multiplicatively and $\mathbb{Z}_n$ additively, so we show $\varphi(xy) = \varphi(x) + \varphi(y)$. Let $x = a^i$ and $y = a^j$. Then

$$\varphi(xy) = \varphi\left(a^{i+j}\right) = (i+j) \bmod n,$$

$$\varphi(x) + \varphi(y) = (i \bmod n + j \bmod n) \bmod n = (i+j) \bmod n.$$

So φ is an isomorphism, and $G \cong \mathbb{Z}_n$.

Proof of the Proposition — |a| Infinite

PROOF (INFINITE ORDER). By Theorem 4.1, $a^i = a^j$ exactly when $i = j$. Define $\varphi: G \to \mathbb{Z}$ by $\varphi(a^k) = k$.

Step 1 (well defined). If $a^i = a^j$, then $i = j$, so $\varphi(a^i) = \varphi(a^j)$.

Step 2 (one-to-one). If $\varphi(a^i) = \varphi(a^j)$, then $i = j$, so $a^i = a^j$.

Step 3 (onto). For every $k \in \mathbb{Z}$, $\varphi(a^k) = k$.

Step 4 (operation-preserving). For $x = a^i$ and $y = a^j$, $\varphi(xy) = \varphi(a^{i+j}) = i + j = \varphi(x) + \varphi(y)$.

So φ is an isomorphism, and $G \cong \mathbb{Z}$.

Relabelling the Table: U(10) ≅ $\mathbb{Z}_4$

EXAMPLE. $U(10) = \langle 3 \rangle$ has order 4, so by the Proposition $\varphi: U(10) \to \mathbb{Z}_4$, $\varphi(3^k) = k \bmod 4$, is an isomorphism. It renames 1,3,9,7 as 0,1,2,3:

·	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

U(10), multiplication mod 10

$\varphi(3^k) = k$

$1, 3, 9, 7 \mapsto 0, 1, 2, 3$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4$, addition mod 4

Amber: ϕ(3 · 9) = ϕ(7) = 3 = 1 + 2 = ϕ(3) + ϕ(9). Every cell is renamed the same way.

A Bijection That Is Not an Isomorphism

NON-EXAMPLE. Let $\mathbb{R}$ be the reals under addition, and define $\varphi: \mathbb{R} \to \mathbb{R}$ by $\varphi(x) = x^3$. Steps 1–3 hold: φ is a one-to-one map of $\mathbb{R}$ onto $\mathbb{R}$, with inverse $y \mapsto \sqrt[3]{y}$. But Step 4 fails. Take $a = b = 1$:

$$\varphi(a + b) = \varphi(2) = 8, \qquad \varphi(a) + \varphi(b) = 1 + 1 = 2.$$

- One counterexample is enough to show that Step 4 fails
- The same formula is an isomorphism from $\mathbb{R}^*$ to $\mathbb{R}^*$ under multiplication, since $(xy)^3 = x^3y^3$: the operation decides

No Isomorphism from $\mathbb{Q}$ to $\mathbb{Q}^*$

EXAMPLE. $\mathbb{Q}$ under addition is not isomorphic to $\mathbb{Q}^*$, the nonzero rationals under multiplication.

PROOF. Suppose, for a contradiction, that $\varphi: \mathbb{Q} \to \mathbb{Q}^*$ is an isomorphism. Since φ is onto and $-1 \in \mathbb{Q}^*$, there is $a \in \mathbb{Q}$ with $\varphi(a) = -1$. Let $b = a/2$. Then $b \in \mathbb{Q}$ and $a = b + b$, so

$$-1 = \varphi(a) = \varphi(b + b) = \varphi(b)\varphi(b) = [\varphi(b)]^2.$$

But $\varphi(b)$ is a rational number, and no rational number has square -1. So no isomorphism $\varphi: \mathbb{Q} \to \mathbb{Q}^*$ exists.

Conjugation by a Matrix Is an Isomorphism

EXAMPLE. Let $G = SL(2, \mathbb{R})$, the 2×2 real matrices of determinant 1, under multiplication. Fix $M \in G$ and define $\varphi_M : G \to G$ by $\varphi_M(A) = MAM^{-1}$.

Step 1 (well defined). Let $A \in G$. Then $\det(MAM^{-1}) = (\det M)(\det A)(\det M)^{-1} = 1$, so $\varphi_M(A) \in G$.

Step 2 (one-to-one). Let $A, B \in G$ with $\varphi_M(A) = \varphi_M(B)$, that is, $MAM^{-1} = MBM^{-1}$. Multiply on the left by M^{-1} and on the right by M: $A = B$.

Conjugation by a Matrix, Continued

Step 3 (onto). Let $B \in G$ and put $A = M^{-1}BM$. Then $\det A = 1$, so $A \in G$, and $\varphi_M(A) = M\left(M^{-1}BM\right)M^{-1} = B$.

Step 4 (operation-preserving). Let $A, B \in G$. Then

$$\varphi_M(AB) = M(AB)M^{-1} = MA\left(M^{-1}M\right)BM^{-1}$$
$$= \left(MAM^{-1}\right)\left(MBM^{-1}\right) = \varphi_M(A)\varphi_M(B).$$

So φ_M is an isomorphism from G onto G, called **conjugation by** M. Nothing in Steps 2–4 uses matrices: the same steps work for $x \mapsto axa^{-1}$ in any group (Part 3).

Part 2 — Properties of Isomorphisms

GOAL. See what an isomorphism must preserve, and use that to prove two groups are **not** isomorphic.

- Theorem 6.1: what an isomorphism does to elements
- Theorem 6.2: what it does to groups and subgroups
- Five quick tests for “not isomorphic”, and their limits

Theorem 6.1 — Isomorphisms Acting on Elements

THEOREM 6.1. Let $\varphi: G \to \overline{G}$ be an isomorphism, and let e and $\overline{e}$ be the identities of G and $\overline{G}$. Then:

(1) $\varphi(e) = \overline{e}$.

(2) $\varphi(a^n) = [\varphi(a)]^n$ for every $a \in G$ and every integer n. Additively, $\varphi(na) = n\varphi(a)$.

(3) a and b commute if and only if $\varphi(a)$ and $\varphi(b)$ commute.

(4) $G = \langle a \rangle$ if and only if $\overline{G} = \langle \varphi(a) \rangle$.

Theorem 6.1, Continued

THEOREM 6.1 (CONTINUED).

(5) $|a| = |\varphi(a)|$ for every $a \in G$: isomorphisms preserve orders.

(6) For a fixed integer k and a fixed $b \in G$, the equation $x^k = b$ has as many solutions x in G as the equation $y^k = \varphi(b)$ has solutions y in $\overline{G}$.

(7) If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

Proof of Theorem 6.1 — Parts 1 and 2

PROOF (1). Since $ee = e$, in $\overline{G}$ we have $\overline{e}\,\varphi(e) = \varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$. Cancelling $\varphi(e)$ on the right gives $\overline{e} = \varphi(e)$.

PROOF (2). Fix $a \in G$. For $n = 0$, $\varphi(a^0) = \varphi(e) = \overline{e} = [\varphi(a)]^0$ by (1). For $n > 0$, use induction: if $\varphi(a^n) = [\varphi(a)]^n$, then

$$\varphi(a^{n+1}) = \varphi(a^n a) = \varphi(a^n)\varphi(a) = [\varphi(a)]^{n+1}.$$

For $n < 0$, put $m = -n > 0$. Then $\overline{e} = \varphi(a^m a^{-m}) = \varphi(a^m)\varphi(a^{-m}) = [\varphi(a)]^m \varphi(a^{-m})$, so $\varphi(a^{-m}) = [\varphi(a)]^{-m}$.

Proof of Theorem 6.1 — Parts 3 and 4

PROOF (3). If $ab = ba$, then $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a)$. Conversely, if $\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$, then $\varphi(ab) = \varphi(ba)$, so $ab = ba$ because φ is one-to-one.

PROOF (4). Suppose $G = \langle a \rangle$, and let $y \in \overline{G}$. As φ is onto, $y = \varphi(x)$ with $x \in G$, and $x = a^k$ for some k. By (2), $y = \varphi\left(a^k\right) = [\varphi(a)]^k$. So $\overline{G} = \langle \varphi(a) \rangle$.

Conversely, suppose $\overline{G} = \langle \varphi(a) \rangle$, and let $x \in G$. Then $\varphi(x) = [\varphi(a)]^k = \varphi\left(a^k\right)$ for some k, so $x = a^k$ because φ is one-to-one. So $G = \langle a \rangle$.

Proof of Theorem 6.1 — Part 5

PROOF (5). Let $a \in G$ and let k be an integer. Since φ is one-to-one, and by (1) and (2),

$$a^k = e \Leftrightarrow \varphi\left(a^k\right) = \varphi(e) \Leftrightarrow [\varphi(a)]^k = \overline{e}.$$

So the integers k with $a^k = e$ are exactly the integers k with $[\varphi(a)]^k = \overline{e}$.

The order of an element is the least positive such k, or infinite if there is none. So $|a| = |\varphi(a)|$.

Proof of Theorem 6.1 — Parts 6 and 7

PROOF (6). Let $S = \{x \in G \mid x^k = b\}$ and $\overline{S} = \{y \in \overline{G} \mid y^k = \varphi(b)\}$. If $x \in S$, then $[\varphi(x)]^k = \varphi\left(x^k\right) = \varphi(b)$, so $\varphi(x) \in \overline{S}$. If $y \in \overline{S}$, then $y = \varphi(x)$ for some $x \in G$, since φ is onto; and $\varphi\left(x^k\right) = [\varphi(x)]^k = \varphi(b)$, so $x^k = b$, since φ is one-to-one. Thus $x \in S$. So φ maps S one-to-one onto $\overline{S}$, and $|S| = \left|\overline{S}\right|$.

PROOF (7). By (5), $x \in G$ has order k exactly when $\varphi(x)$ has order k. As φ is one-to-one and onto, it maps the elements of order k in G one-to-one onto those of order k in $\overline{G}$.

Theorem 6.2 — Isomorphisms Acting on Groups

THEOREM 6.2. Let $\varphi: G \to \overline{G}$ be an isomorphism. Then:

(1) $\varphi^{-1}: \overline{G} \to G$ is an isomorphism.

(2) G is Abelian if and only if $\overline{G}$ is Abelian.

(3) G is cyclic if and only if $\overline{G}$ is cyclic.

(4) If $K \leq G$, then $\varphi(K) = \{\varphi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

(5) If $\overline{K} \leq \overline{G}$, then $\varphi^{-1}\left(\overline{K}\right) = \{g \in G \mid \varphi(g) \in \overline{K}\}$ is a subgroup of G.

(6) $\varphi\big(Z(G)\big) = Z\left(\overline{G}\right)$.

Proof of Theorem 6.2 — Parts 1 and 2

PROOF (1). As φ is one-to-one and onto, it has an inverse map $\varphi^{-1}: \overline{G} \to G$, which is also one-to-one and onto: Steps 1–3 hold. For Step 4, let $x, y \in \overline{G}$ and put $a = \varphi^{-1}(x)$, $b = \varphi^{-1}(y)$. Then $\varphi(ab) = \varphi(a)\varphi(b) = xy$, so

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

PROOF (2). Suppose G is Abelian, and let $x, y \in \overline{G}$. As φ is onto, $x = \varphi(a)$ and $y = \varphi(b)$ with $a, b \in G$. Then

$$xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx.$$

For the converse, apply the same argument to the isomorphism φ^{-1} of (1).

Proof of Theorem 6.2 — Parts 3 and 4

PROOF (3). If $G = \langle a \rangle$, then $\overline{G} = \langle \varphi(a) \rangle$ by Theorem 6.1(4). Conversely, if $\overline{G} = \langle b \rangle$, the same argument for the isomorphism φ^{-1} of (1) gives $G = \langle \varphi^{-1}(b) \rangle$.

PROOF (4). Let $K \leq G$. The set $\varphi(K)$ is not empty, since $\overline{e} = \varphi(e) \in \varphi(K)$. Let $x, y \in \varphi(K)$, say $x = \varphi(k_1)$ and $y = \varphi(k_2)$ with $k_1, k_2 \in K$. By Theorem 6.1(2) with $n = -1$, $y^{-1} = \varphi\left(k_2^{-1}\right)$, so

$$xy^{-1} = \varphi(k_1)\varphi\left(k_2^{-1}\right) = \varphi\left(k_1 k_2^{-1}\right) \in \varphi(K),$$

because $k_1 k_2^{-1} \in K$. By the One-Step Subgroup Test, $\varphi(K) \leq \overline{G}$.

Proof of Theorem 6.2 — Parts 5 and 6

PROOF (5). Since φ is one-to-one and onto, $\varphi^{-1}\left(\overline{K}\right) = \{g \in G \mid \varphi(g) \in \overline{K}\}$ is the image of $\overline{K}$ under the isomorphism φ^{-1} of (1). So it is a subgroup of G, by (4) applied to φ^{-1}.

PROOF (6). Let $z \in Z(G)$ and $y \in \overline{G}$. As φ is onto, $y = \varphi(x)$ for some $x \in G$, and $zx = xz$. So

$$\varphi(z)\, y = \varphi(z)\varphi(x) = \varphi(zx) = \varphi(xz) = \varphi(x)\varphi(z) = y\, \varphi(z).$$

Hence $\varphi\big(Z(G)\big) \subseteq Z\left(\overline{G}\right)$. The same argument for φ^{-1} gives $\varphi^{-1}\left(Z\left(\overline{G}\right)\right) \subseteq Z(G)$, and applying φ to both sides, $Z\left(\overline{G}\right) \subseteq \varphi\big(Z(G)\big)$.

Showing Two Groups Are Not Isomorphic

By Theorems 6.1 and 6.2, isomorphic groups agree on each property below. So $G \ncong \overline{G}$ if they differ on any one:

- the order: $|G| \neq \left|\overline{G}\right|$
- one group is cyclic and the other is not
- one group is Abelian and the other is not
- the largest orders of elements differ
- the numbers of elements of some order differ

WARNING. These tests prove only "not isomorphic". Groups that agree on all five need not be isomorphic.

Three Groups of Order 12

EXAMPLE. $\mathbb{Z}_{12}$, D_6 and A_4 all have order 12, and no two of them are isomorphic. For instance, if $\varphi\colon \mathbb{Z}_{12} \to D_6$ were an isomorphism, then $|\varphi(1)| = |1| = 12$ by Theorem 6.1(5); but D_6 has no element of order 12.

	$\mathbb{Z}_{12}$	D_6	A_4
cyclic?	yes	no	no
Abelian?	yes	no	no
largest element order	12	6	3
elements of order 2	1	7	3

$\mathbb{Q}$ and $\mathbb{Q}^*$ Again — Orders Settle It

EXAMPLE. A second proof that $\mathbb{Q} \ncong \mathbb{Q}^*$.

PROOF. Suppose $\varphi: \mathbb{Q} \to \mathbb{Q}^*$ is an isomorphism. Then $\varphi^{-1}: \mathbb{Q}^* \to \mathbb{Q}$ is an isomorphism (Theorem 6.2(1)). Let $a = \varphi^{-1}(-1) \in \mathbb{Q}$. Since $|-1| = 2$ in $\mathbb{Q}^*$, Theorem 6.1(5) gives $|a| = 2$: so $a \neq 0$ and $a + a = 0$. But $a + a = 2a = 0$ forces $a = 0$. This contradiction shows that $\mathbb{Q} \ncong \mathbb{Q}^*$.

Isomorphic Groups Share Every Group Property

- Any property that can be stated in the language of groups — orders, commuting, subgroups, numbers of solutions of equations — holds in G exactly when it holds in $\overline{G}$
- That is why isomorphic groups are called "the same": $\overline{G}$ is G in camouflage
- Properties of the **names** do not transfer: $\mathbb{Z}_4$ is written with $+$ and contains the integer 2; $U(10) \cong \mathbb{Z}_4$ is written with $\cdot$ and does not contain 2
- So a hard question about G can be moved to an easier $\overline{G}$ — Chapters 8 and 11 do this constantly

Part 3 — Automorphisms

GOAL. Study the isomorphisms from a group onto itself. They form a group of their own.

- Automorphisms, and the inner automorphisms $x \mapsto axa^{-1}$
- Theorem 6.3: $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups
- Theorem 6.4: $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$

Automorphisms

DEFINITION. An **automorphism** of a group G is an isomorphism $\varphi: G \to G$, from G onto itself.

EXAMPLE. Define $\varphi: \mathbb{C} \to \mathbb{C}$ by $\varphi(a + bi) = a - bi$. Then φ is an automorphism of $\mathbb{C}$ under addition, and its restriction to $\mathbb{C}^*$ is an automorphism of $\mathbb{C}^*$ under multiplication (Exercise 39).

EXAMPLE. Define $\varphi: \mathbb{R}^2 \to \mathbb{R}^2$ by $\varphi(a, b) = (b, a)$. Then φ is an automorphism of $\mathbb{R}^2$ under componentwise addition — the four steps are on the next slide.

An Automorphism of $\mathbb{R}^2$, Step by Step

EXAMPLE. Define $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$ by $\varphi(a,b) = (b,a)$.

Step 1 (well defined). For $(a,b) \in \mathbb{R}^2$, $(b,a) \in \mathbb{R}^2$.

Step 2 (one-to-one). If $\varphi(a,b) = \varphi(c,d)$, then $(b,a) = (d,c)$, so $b = d$ and $a = c$: $(a,b) = (c,d)$.

Step 3 (onto). Let $(c,d) \in \mathbb{R}^2$. Then $\varphi(d,c) = (c,d)$.

Step 4 (operation-preserving). For $(a,b),(c,d) \in \mathbb{R}^2$,

$$\varphi\big((a,b)+(c,d)\big) = \varphi(a+c,\ b+d) = (b+d,\ a+c)$$

$$= (b,a) + (d,c) = \varphi(a,b) + \varphi(c,d).$$

Geometrically, φ reflects the plane in the line $y = x$.

Inner Automorphisms

DEFINITION. Let G be a group and $a \in G$. Define $\varphi_a : G \to G$ by $\varphi_a(x) = axa^{-1}$. The map φ_a is the **inner automorphism of G induced by a.**

NOTATION. $\mathrm{Aut}(G)$ is the set of all automorphisms of G, and $\mathrm{Inn}(G) = \{\varphi_a \mid a \in G\}$ is the set of all inner automorphisms of G.

- In an Abelian group, $\varphi_a(x) = axa^{-1} = x$ for every x, so every inner automorphism is the identity map

Inner Automorphisms Are Automorphisms

PROPOSITION. For every $a \in G$, the map $\varphi_a: G \to G$, $\varphi_a(x) = axa^{-1}$, is an automorphism of G.

Step 1 (well defined). For $x \in G$, $axa^{-1} \in G$ by closure.

Step 2 (one-to-one). If $\varphi_a(x) = \varphi_a(y)$, then $axa^{-1} = aya^{-1}$; cancel a on the left and a^{-1} on the right: $x = y$.

Step 3 (onto). Let $y \in G$ and put $x = a^{-1}ya$. Then $\varphi_a(x) = a\left(a^{-1}ya\right)a^{-1} = y$.

Step 4 (operation-preserving). For $x, y \in G$,

$$\varphi_a(xy) = a(xy)a^{-1} = ax\left(a^{-1}a\right)ya^{-1} = \left(axa^{-1}\right)\left(aya^{-1}\right) = \varphi_a(x)\varphi_a(y).$$

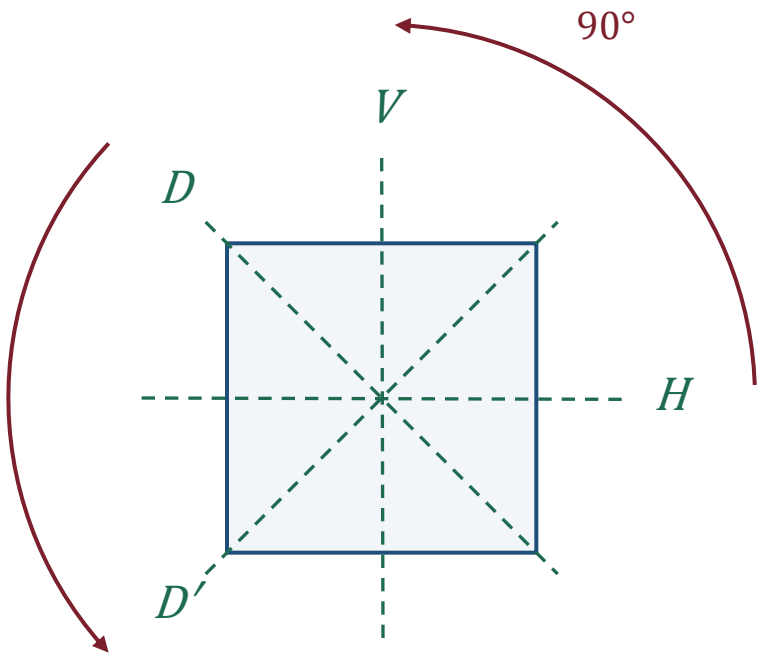
Conjugation by R_{90} in D_4

EXAMPLE. In D_4, take $a = R_{90}$, so $\varphi_{R_{90}}(x) = R_{90}xR_{90}^{-1} = R_{90}xR_{270}$. From the Cayley table,

$$\varphi_{R_{90}}(H) = R_{90}HR_{270} = D'R_{270} = V.$$

- $\varphi_{R_{90}}$ fixes R_0, R_{90}, R_{180} and R_{270}, because rotations commute
- it swaps $H \leftrightarrow V$ and $D \leftrightarrow D'$

$R_{90}HR_{90}^{-1}$ is the reflection in the axis of H turned through $90°$.



Conjugating by R_{90} turns each mirror line through 90°: H onto V, and D onto D'.

Theorem 6.3 — Aut(G) and Inn(G) Are Groups

THEOREM 6.3. Let G be a group. Under composition of functions, $\mathrm{Aut}(G)$ is a group, and so is $\mathrm{Inn}(G)$.

PROOF. Exercise 17, which is on your list. The key identity for $\mathrm{Inn}(G)$ is $\varphi_a \varphi_b = \varphi_{ab}$ for all $a, b \in G$ (Exercise 13).

- Listing $\mathrm{Inn}(G)$ is routine — $\varphi_e, \varphi_a, \varphi_b, \ldots$ — but the list can repeat: $\varphi_a = \varphi_b$ is possible with $a \neq b$
- Finding $\mathrm{Aut}(G)$ is in general much harder

$\mathrm{Inn}(D_4)$

EXAMPLE. The eight maps $\varphi_{R_0}, \varphi_{R_{90}}, \varphi_{R_{180}}, \varphi_{R_{270}}, \varphi_H, \varphi_V, \varphi_D, \varphi_{D'}$ are not all different. For every $x \in D_4$:

- $R_{180} \in Z(D_4)$, so $\varphi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = xR_{180}R_{180}^{-1} = x = \varphi_{R_0}(x)$
- $R_{270} = R_{90}R_{180}$, so $\varphi_{R_{270}}(x) = R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1} = \varphi_{R_{90}}(x)$
- in the same way, $H = R_{180}V$ and $D' = R_{180}D$ give $\varphi_H = \varphi_V$ and $\varphi_D = \varphi_{D'}$

So $\mathrm{Inn}(D_4) = \{\varphi_{R_0}, \varphi_{R_{90}}, \varphi_H, \varphi_D\}$, and these four are distinct (Exercise 15).

Conjugate Subgroups Are Isomorphic

EXAMPLE. In S_4, let H be the copy of D_4 from Chapter 5: (1), (1234), $(13)(24)$, (1432), $(12)(34)$, (24), $(14)(23)$, (13). For $\alpha \in S_4$, φ_α is an automorphism of S_4, so by Theorem 6.2(4), $\varphi_\alpha(H) = \alpha H \alpha^{-1}$ is a subgroup of S_4; and φ_α, restricted to H, is an isomorphism from H onto $\alpha H \alpha^{-1}$:

- $(12)H(12)$: (1), (1342), $(14)(23)$, (1243), $(12)(34)$, (14), $(13)(24)$, (23)
- $(123)H(132)$: (1), (1423), $(12)(34)$, (1324), $(14)(23)$, (34), $(13)(24)$, (12)

$\mathrm{Aut}(\mathbb{Z}_{10})$: What an Automorphism Must Do

EXAMPLE. Let $\alpha \in \mathrm{Aut}(\mathbb{Z}_{10})$.

α is determined by $\alpha(1)$. We have $\alpha(0) = 0$ by Theorem 6.1(1), and for $1 \le k \le 9$, using Step 4 repeatedly,

$$\alpha(k) = \alpha(1 + 1 + \cdots + 1) = \alpha(1) + \alpha(1) + \cdots + \alpha(1) = k\,\alpha(1) \bmod 10,$$

with k terms on each side.

$\alpha(1)$ is a generator. By Theorem 6.1(5), $|\alpha(1)| = |1| = 10$, so $\alpha(1) \in \{1,3,7,9\}$.

So α is one of the maps $\alpha_r(x) = rx \bmod 10$ with $r = 1,3,7,9$.

Aut($\mathbb{Z}_{10}$): Each Candidate Is an Automorphism

EXAMPLE (CONTINUED). Fix $r \in U(10) = \{1,3,7,9\}$, let s be the inverse of r in $U(10)$, so that $rs \bmod 10 = 1$, and define $\alpha_r : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ by $\alpha_r(x) = rx \bmod 10$.

Step 1 (well defined). For $x \in \mathbb{Z}_{10}$, $rx \bmod 10$ is one element of $\mathbb{Z}_{10}$.

Step 2 (one-to-one). If $\alpha_r(x) = \alpha_r(y)$, then $rx \equiv ry \pmod{10}$. Multiply by s: $x \equiv y \pmod{10}$, so $x = y$.

Step 3 (onto). For $y \in \mathbb{Z}_{10}$, $\alpha_r(sy \bmod 10) = rsy \bmod 10 = y$.

Step 4 (operation-preserving). $\alpha_r(a + b) = r(a + b) = ra + rb = \alpha_r(a) + \alpha_r(b)$, all mod 10.

$\mathrm{Aut}(\mathbb{Z}_{10}) \cong U(10)$

EXAMPLE (CONTINUED). By the last two slides, $\mathrm{Aut}(\mathbb{Z}_{10}) = \{\alpha_1, \alpha_3, \alpha_7, \alpha_9\}$. Also $(\alpha_3\alpha_3)(1) = \alpha_3(3) = 9$, so $\alpha_3^2 = \alpha_9$; likewise $\alpha_3^3 = \alpha_7$ and $\alpha_3^4 = \alpha_1$. Hence $\mathrm{Aut}(\mathbb{Z}_{10}) = \langle \alpha_3 \rangle$ is cyclic, and its table is the table of $U(10)$:

U(10)	1	3	7	9	$\mathrm{Aut}(\mathbb{Z}_{10})$	α_1	α_3	α_7	α_9
1	1	3	7	9	α_1	α_1	α_3	α_7	α_9
3	3	9	1	7	α_3	α_3	α_9	α_1	α_7
7	7	1	9	3	α_7	α_7	α_1	α_9	α_3
9	9	7	3	1	α_9	α_9	α_7	α_3	α_1

Theorem 6.4 — Aut($\mathbb{Z}_n$) ≅ U(n)

THEOREM 6.4. For every positive integer n, $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$.

PROOF. Define $T: \mathrm{Aut}(\mathbb{Z}_n) \to U(n)$ by $T(\alpha) = \alpha(1)$.

Step 1 (well defined). Let $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$. Since 1 generates $\mathbb{Z}_n$, so does $\alpha(1)$ (Theorem 6.1(4)). The generators of $\mathbb{Z}_n$ are the elements of $U(n)$ (Chapter 4), so $T(\alpha) \in U(n)$.

Step 2 (one-to-one). Let $T(\alpha) = T(\beta)$, that is, $\alpha(1) = \beta(1)$. As for $\mathbb{Z}_{10}$, $\alpha(k) = k\alpha(1) \bmod n$ and $\beta(k) = k\beta(1) \bmod n$ for every $k \in \mathbb{Z}_n$. So $\alpha(k) = \beta(k)$ for every k, that is, $\alpha = \beta$.

Proof of Theorem 6.4, Continued

Step 3 (onto). Let $r \in U(n)$. The map $\alpha_r : \mathbb{Z}_n \to \mathbb{Z}_n$, $\alpha_r(x) = rx \bmod n$, is an automorphism of $\mathbb{Z}_n$ (Exercise 31; the case $n = 10$ was done above), and $T(\alpha_r) = \alpha_r(1) = r$.

Step 4 (operation-preserving). Let $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}_n)$. Using $\alpha(k) = k\alpha(1)$ with $k = \beta(1)$,

$$T(\alpha\beta) = (\alpha\beta)(1) = \alpha\big(\beta(1)\big) = \beta(1)\,\alpha(1) = \alpha(1)\beta(1) = T(\alpha)T(\beta),$$

with products taken mod n, in $U(n)$.

So T is an isomorphism. In particular $\mathrm{Aut}(\mathbb{Z}_n)$ has $|U(n)|$ elements, one for each generator of $\mathbb{Z}_n$.

Part 4 — Cayley's Theorem

GOAL. Show that every group is a group of permutations, up to isomorphism.

- The permutations $T_g(x) = gx$
- Theorem 6.5 (Cayley, 1854) and its proof
- The left regular representations of $U(12)$ and D_4

Theorem 6.5 — Cayley's Theorem

THEOREM 6.5 (CAYLEY, 1854). Every group is isomorphic to a group of permutations.

PROOF (SETTING UP). Let G be a group. For $g \in G$ define $T_g: G \to G$ by $T_g(x) = gx$.

(a) T_g is a permutation of G. One-to-one: if $T_g(x) = T_g(y)$, then $gx = gy$, so $x = y$. Onto: for $y \in G$, $T_g\left(g^{-1}y\right) = y$.

(b) $T_g T_h = T_{gh}$. For every $x \in G$, $\left(T_g T_h\right)(x) = T_g(hx) = g(hx) = (gh)x = T_{gh}(x)$.

(c) $\overline{G} = \{T_g \mid g \in G\}$ is a group under composition, with identity T_e and $\left(T_g\right)^{-1} = T_{g^{-1}}$ (Exercise 9).

Proof of Cayley's Theorem

PROOF (CONTINUED). Define $\varphi: G \to \overline{G}$ by $\varphi(g) = T_g$.

Step 1 (well defined). For $g \in G$, $T_g \in \overline{G}$ by the definition of $\overline{G}$.

Step 2 (one-to-one). If $\varphi(g) = \varphi(h)$, then $T_g = T_h$, so $T_g(e) = T_h(e)$: $ge = he$, and $g = h$.

Step 3 (onto). Every element of $\overline{G}$ is $T_g = \varphi(g)$ for some $g \in G$.

Step 4 (operation-preserving). For $a, b \in G$, $\varphi(ab) = T_{ab} = T_a T_b = \varphi(a)\varphi(b)$, by (b).

So $G \cong \overline{G}$. The group $\overline{G}$ is the **left regular representation** of G; if $|G| = n$, it is a subgroup of S_n.

The Left Regular Representation of U(12)

EXAMPLE. $U(12) = \{1,5,7,11\}$, and $T_x(y) = xy \bmod 12$:

$$T_1 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{bmatrix}, \quad T_5 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{bmatrix},$$

$$T_7 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{bmatrix}, \quad T_{11} = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{bmatrix}.$$

- The bottom row of T_x is the row of x in the multiplication table of $U(12)$

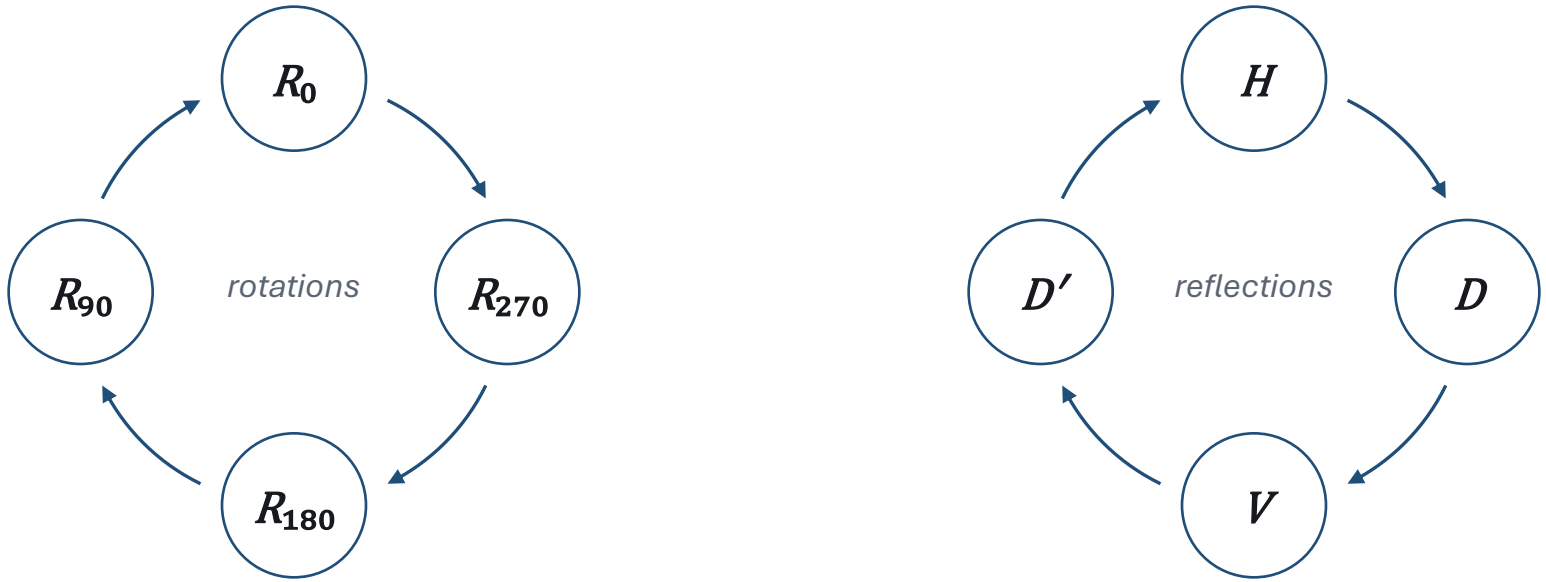
Comparing the Two Tables

EXAMPLE (CONTINUED). The table of $U(12)$ and the table of its left regular representation $\overline{U(12)}$ differ only in notation: $\varphi(x) = T_x$ renames each entry.

U(12)	1	5	7	11	Ū(12)	T_1	T_5	T_7	T_{11}
1	1	5	7	11	T_1	T_1	T_5	T_7	T_{11}
5	5	1	11	7	T_5	T_5	T_1	T_{11}	T_7
7	7	11	1	5	T_7	T_7	T_{11}	T_1	T_5
11	11	7	5	1	T_{11}	T_{11}	T_7	T_5	T_1

The Left Regular Representation of D_4

EXAMPLE. In D_4, $T_{R_{270}}(x) = R_{270}x$ permutes the eight elements in two 4-cycles, drawn below. Likewise $T_H(x) = Hx$ gives $T_H = (R_0\ H)(R_{90}\ D)(R_{180}\ V)(R_{270}\ D')$.



$x \mapsto R_{270}x$: $(R_0\ R_{270}\ R_{180}\ R_{90})(H\ D\ V\ D')$. Every element moves, and every cycle has length $|R_{270}| = 4$.

Why Cayley's Theorem Matters

- Every abstract group can be studied as a concrete group of permutations
- It shows the axioms of Chapter 2 are the right abstraction: an abstract group is a group of permutations seen from a different viewpoint
- Not every isomorphism is easy to find. As groups, $\mathbb{R}$ and $\mathbb{C}$ under addition are isomorphic, and so are $\mathbb{C}^*$ and the unit circle $\{z \in \mathbb{C}: |z| = 1\}$ under multiplication — the proofs are beyond this course
- Chapter 24 generalises Cayley's construction

What to Take Away

- An isomorphism is a map $\varphi: G \to \overline{G}$ that is one-to-one, onto and operation-preserving: $\varphi(ab) = \varphi(a)\varphi(b)$
- To prove $G \cong \overline{G}$: define φ by a formula, then check Steps 1–4
- Isomorphisms preserve orders, generators, commuting, subgroups and centers — so one differing invariant proves "not isomorphic"
- Cyclic groups of the same order are isomorphic: $\langle a \rangle \cong \mathbb{Z}$ or $\mathbb{Z}_n$
- Inner automorphisms are $\varphi_a(x) = axa^{-1}$; and $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$
- Cayley: every group is isomorphic to a group of permutations