CHAPTER 6

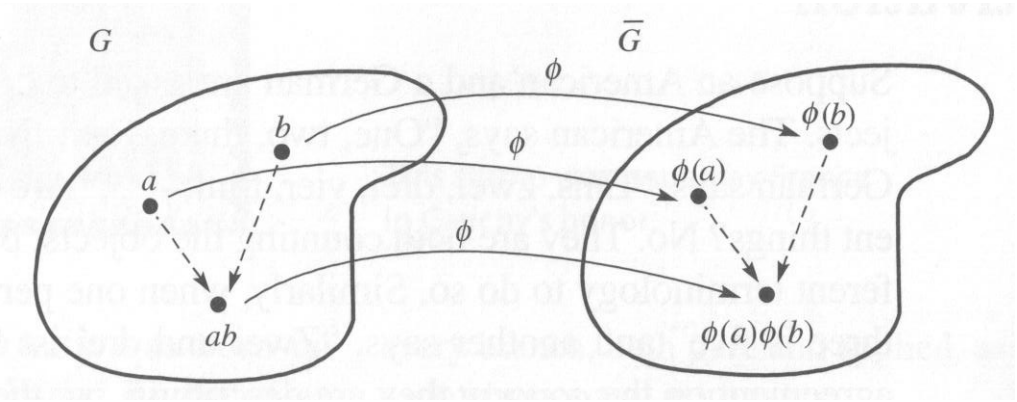
Isomorphisms

A while back, we saw that $\langle a \rangle$ with $|\langle a \rangle| = 42$ and $\mathbb{Z}_{42}$ had basically the same structure, and said the groups were "isomorphic," in some sense the same.

DEFINITION (Group Isomorphism). An isomorphism ϕ from a group G to a group $\overline{G}$ is a 1–1 mapping from G onto $\overline{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \quad \forall\ a, b \in G.$$

If there is an isomorphism from G onto $\overline{G}$, we say G and $\overline{G}$ arr isomorphic and write $G \approx \overline{G}$.



NOTE. The operations in G and $\overline{G}$ may be different. The operation to the left of "=" is in G, while that on the right is in $\overline{G}$.

G Operation	$\overline{G}$ Operation	Operation Preservation
$\cdot$	$\cdot$	$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
$\cdot$	$+$	$\phi(a \cdot b) = \phi(a) + \phi(b)$
$+$	$\cdot$	$\phi(a + b) = \phi(a) \cdot \phi(b)$
$+$	$+$	$\phi(a + b) = \phi(a) + \phi(b)$

To establish an isomorphism:

(1) Define $\phi : G \to \overline{G}$.

(2) Show ϕ is 1–1: assuming $\phi(a) = \phi(b)$, show $a = b$.

(3) Show ϕ is onto: $\forall\ \overline{g} \in \overline{G}$. show $\exists\ g \in G \ni \phi(g) = \overline{g}$.

(4) Show $\phi(ab) = \phi(a)\phi(b)\ \forall\ a, b \in G$.

EXAMPLE. With $|a| = 42$, show $\langle a \rangle \approx \mathbb{Z}_{42}$.

PROOF.

Define $\phi : \langle a \rangle \to \mathbb{Z}_{42}$ by $\phi(a^n) = n \bmod 42$.

[Show 1–1.] Suppose $\phi(a^n) = \phi(a^m)$. Then

$$n = m \bmod 42 \Longrightarrow 42 | n - m \Longrightarrow a^n = a^m$$

by Theorem 4.1. Thus ϕ is 1–1.

[Show onto.] For all $n \in \mathbb{Z}_{42}$, $a^n \in \langle a \rangle$ and $\phi(a^n) = n$, so ϕ is onto.

[Show operation preservation.] For all $a^n, a^m \in \langle a \rangle$,

$\phi(a^n a^m) = \phi(a^{n+m}) = n+m \bmod 42 = n \bmod 42 + m \bmod 42 = \phi(a^n) + \phi(a^m)$.

Thus, by definition, $\langle a \rangle \approx \mathbb{Z}_{42}$. □

EXAMPLE. Any finite cyclic group $\langle a \rangle$ with $|\langle a \rangle| = n$ is isomorphic to $\mathbb{Z}_n$ under $\phi(a^k) = k \bmod n$. The proof of this is identical to that of the previous example.

EXAMPLE. Let G be the positive real numbers with multiplication and $\overline{G}$ be the group of real numbers with addition. Show $G \approx \overline{G}$.

PROOF.

Define $\phi : G \to \overline{G}$ by $\phi(x) = \ln(x)$.

[Show 1–1.] Suppose $\phi(x) = \phi(y)$. Then

$$\ln(x) = \ln(y) \Longrightarrow e^{\ln(x)} = e^{\ln(y)} \Longrightarrow x = y,$$

so ϕ is 1–1.

[Show onto] Now suppose $x \in \overline{G}$. $e^x > 0$ and $\phi(e^x) = \ln e^x = x$, so ϕ is onto.

[Show operation preservation.] Finally, for all $x, y \in G$,

$$\phi(xy) = \ln(xy) = \ln x + \ln y = \phi(x) + \phi(y),$$

so $G \approx \overline{G}$.

[Question: is ϕ the only isomorphism?] □

EXAMPLE. Any infinite cyclic group is isomorphic to $\mathbb{Z}$ with addition. Given $\langle a \rangle$ with $|a| = \infty$, define $\phi(a^k) = k$. The map is clearly onto. If $\phi(a^n) = \phi(a^m)$, $n = m \Longrightarrow a^n = a^m$, so ϕ is 1–1. Also,

$$\phi(a^n a^m) = \phi(a^{n+m}) = n + m = \phi(n) + \phi(m),$$

so $\langle a \rangle \approx \mathbb{Z}$.

Consider $\langle 2 \rangle$ under addition, the cyclic group of even integers. The $\langle 2 \rangle \approx \mathbb{Z} = \langle 1 \rangle$ with $\phi : \langle 2 \rangle \to \mathbb{Z}$ defined by $\phi(2n) = n$.

EXAMPLE. Let G be the group of real numbers under addition and $\overline{G}$ be the group of positive numbers under multiplication. Define $\phi(x) = 2^{x-1}$. ϕ is 1–1 and onto but

$$\phi(1+2) = \phi(3) = 4 \neq 2 = 1 \cdot 2 = \phi(1)\phi(2),$$

so ϕ is not an isomorphism.

Can this mapping be adjusted to make it an isomorphism?

Use $\phi(x) = 2^x$.

If $\phi(x) = \phi(y),\ 2^x = 2^y \Longrightarrow \log_2 2^x = \log_2 2^y \Longrightarrow x = y$, so ϕ is 1–1.

Given any positive y, $\phi(\log_2 y) = 2^{\log_2 y} = y$, so ϕ is onto.

Also, for all $x, y \in \mathbb{R}$,$\phi(x+y) = 2^{x+y} = 2^x 2^y = \phi(x)\phi(y)$.

Thus ϕ is an isomorphism.

EXAMPLE. Are $U(8)$ and $U(12)$ isomorphic?

SOLUTION.

$U(8) = \{1, 3, 5, 7\}$ is noncyclic with $|3| = |5| = |7| = 2$.

$U(12) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ is noncyclic with $|5| = |7| = |11| = 2$.

Define $\phi : U(8) \to U(12)$ by $1 \to \overline{(1)},\ 3 \to \overline{5},\ 5 \to \overline{7},\ 7 \to \overline{11}$.

ϕ is clearly 1–1 and onto. Regarding operation preservation:

$\phi(3 \cdot 5) = \phi(7) = \overline{11}$ and $\phi(3)\phi(5) = \overline{5} \cdot \overline{7} = \overline{11}$.

$\phi(3 \cdot 7) = \phi(5) = \overline{7}$ and $\phi(3)\phi(7) = \overline{5} \cdot \overline{11} = \overline{7}$.

$\phi(5 \cdot 7) = \phi(3) = \overline{5}$ and $\phi(5)\phi(7) = \overline{7} \cdot \overline{11} = \overline{5}$.

$\phi(1 \cdot 3) = \phi(3) = \overline{5}$ and $\phi(1)\phi(3) = \overline{1} \cdot \overline{5} = \overline{5}$.

etc.

Since both groups are Abelian, we need only check each pair in a single order. Thus, $U(8) \approx U(12)$. □

This group of order 4, with all non-identity element of order 2, is called the Klein 4 group. Any other group of order 4 must have an element of order 4, so is cyclic and isomorphic to $\mathbb{Z}_4$.

For orders 1, 2, 3, 5, there are only the cyclic groups $\mathbb{Z}_1,\ \mathbb{Z}_2, \mathbb{Z}_3$, and $\mathbb{Z}_5$.

PROBLEM (Page 140 # 36).

Let $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and $H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{Q} \right\}$ Show that G and H are isomorphic under addition. Prove that G and H are closed under multiplication. Does your isomorphism preserve multiplication as well as addition? (G and H are examples of rings — a topic we begin in Chapter 12)

SOLUTION.

Given $a + b\sqrt{2}, c + d\sqrt{2} \in G$.

$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in G$ and

$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in G$

since $(a + c),\ (b + d),\ (ac + 2bd),\ (ad + bc) \in \mathbb{Q}$.

Also, if $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}, \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \in H$,

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix} \text{and}$$

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{bmatrix} \in H$$

since $(a + c),\ (b + d),\ (ac + 2bd),\ ad + bc \in \mathbb{Q}$.

Thus G and H are closed under both addition and multiplication. Also, G and H are groups under addition (you can prove this, if you desire).

Define $\phi : G \to H$ by $\phi(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$.

Suppose $\phi(a + b\sqrt{2}) = \phi(c + d\sqrt{2})$. Then $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \Longrightarrow$

$a = c$ and $b = d \Longrightarrow a + b\sqrt{2} = c + d\sqrt{2} \Longrightarrow \phi$ is 1–1.

For $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \in H$, $a + b\sqrt{2} \in G$ and $\phi(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$, so ϕ is onto.

Now suppose $a + b\sqrt{2},\ c + d\sqrt{2} \in G$. Then

$$\phi\big((a + b\sqrt{2}) + (c + d\sqrt{2})\big) = \phi\big((a + c) + (b + d)\sqrt{2}\big) = \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix} =$$

$$\begin{bmatrix} a + c & 2b + 2d \\ b + d & a + c = \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2}).$$

Thus ϕ is an isomorphism under addition.

Also,

$$\phi\big((a+b\sqrt{2})(c+d\sqrt{2})\big) = \phi\big((ac+2bd)+(ad+bc)\sqrt{2}\big) = \begin{bmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{bmatrix} =$$

$$\begin{bmatrix} ac + 2bd & 2ad + 2bc \\ ad + bc & ac + 2bd \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \big(\phi(a + b\sqrt{2})\big)\big(\phi(c + d\sqrt{2})\big).$$

So ϕ preserves multiplication also. (We will later see that this makes ϕ a ring homomorphism.) $\square$

PROBLEM (Page 141 # 54). Consider $G = \langle m \rangle$ and $H = \langle n \rangle$ where $m, n \in \mathbb{Z}$. These are groups under addition. Show $G \approx H$. Does this isomorphism also preserve multiplication?

SOLUTION.

Define $\phi : G \to H$ by $\phi(x) = \frac{n}{m}x$. Suppose $\phi(x) = \phi(y)$. Then

$\frac{n}{m}x = \frac{n}{m}y \Longrightarrow x = y \Longrightarrow \phi$ is 1–1.

For $x \in H$, $x = rn$ where $r \in \mathbb{Z}$. Then $\frac{m}{n}x = \frac{m}{n}rn = rm \in G$. Then

$\phi\left(\frac{m}{n}x\right) = \frac{n}{m}\left(\frac{m}{n}x\right) = x$, so ϕ is onto. Now, suppose $x, y \in G$. Then

$$\phi(x + y) = \frac{n}{m}(x + y) = \frac{n}{m}x + \frac{n}{m}y = \phi(x) + \phi(y),$$

so addition is preserved and $G \approx H$. But,

$$\phi(xy) = \frac{n}{m}(xy) \neq \left(\frac{n}{m}x\right)\left(\frac{n}{m}y\right) = \phi(x)\phi(y),$$

so multiplication is not preserved by ϕ. □

THEOREM (3). *$\approx$ is an equivalence relation on the set $\mathcal{G}$ of all groups.*

PROOF.

(1) $G \approx G$. Define $\phi : G \to G$ by $\phi(x) = x$. This is clear.

(2) Suppose $G \approx H$. If $\phi : G \to H$ is the isomrphism and, for $g \in G$, $\phi(g) = h$, then $\phi^{-1} : H \to G$ where $\phi^{-1}(h) = g$ is 1–1 and onto.

Suppose $a, b \in H$. Since ϕ is onto, $\exists\ \alpha, \beta \in G \ni \phi(\alpha) = a$ and $\phi(\beta) = b$. Then $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta) = ab$, so

$$\phi^{-1}(ab) = \phi^{-1}\big(\phi(\alpha)\phi(\beta)\big) = \phi^{-1}\big(\phi(\alpha\beta)\big) = \alpha\beta = \phi^{-1}\big(\phi(\alpha)\big)\phi^{-1}\big(\phi(\beta)\big) = \phi^{-1}(a)\phi^{-1}(b).$$

Thus ϕ^{-1} is an isomorphism and $H \approx G$.

(3) Suppose $G \approx H$ and $H \approx K$ with $\phi : G \to H$ and $\psi : H \to K$ the isomorphisms. Then $\psi\phi : G \to K$ is 1–1 and onto.

For all $a, b \in G$,

$$(\psi\phi)(ab) = \psi\big[\phi(ab)\big] = \psi\big[\phi(a)\phi(b)\big] = \psi\big[\phi(a)\big]\psi\big[\phi(b)\big] = \big[(\psi\phi)(a)\big]\big[(\psi\phi)(b)\big].$$

Thus $G \approx K$ and $\approx$ is an equivalence relation on $\mathcal{G}$. □

NOTE. Thus, when two groups are isomorphic, they are in some sense equal. They differ in that their elements are named differently. Knowing of a computation in one group, the isomorphism allows us to perform the analagous computation in the other group.

EXAMPLE (Conjugation by a). Let G be a group, $a \in G$. Define a function $\phi_a : G \to G$ by $\phi_a(x) = axa^{-1}$.

Suppose $\phi_a(x) = \phi_a(y)$. Then $axa^{-1} = aya^{-1} \implies x = y$ by left and right cancellation. Thus ϕ_a is 1–1.

Now suppose $y \in G$. We need to find $x \in G \ni axa^{-1} = y$. But that will be so if $x = a^{-1}ya$, for then

$$\phi_a(x) = \phi_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = (aa^{-1})y(aa^{-1}) = eye = y,$$

so ϕ_a is onto.

Finally, for all $x, y \in G$,

$$\phi_a(xy) = axya^{-1} = axeya^{-1} = axa^{-1}aya^{-1} = \phi_a(x)\phi_a(y).$$

Thus ϕ_a is an isomorphism from G onto G.

Recall $U(8) = \{1, 3, 5, 7\}$. Consider ϕ_7. Since 7 is its own inverse,

$\phi_7(1) = 7 \cdot 1 \cdot 7 = 1,$

$\phi_7(3) = 7 \cdot 3 \cdot 7 = 5 \cdot 7 = 3,$

$\phi_7(5) = 7 \cdot 5 \cdot 7 = 3 \cdot 7 = 5,$

$\phi_7(7) = 7 \cdot 7 \cdot 7 = 1 \cdot 7 = 7.$

Conjugation by 7 turns out to be the identity isomorphism, which is not very interesting.

THEOREM (6.1 — Cayley's Theorem). *Every group is isomorphic to a group of permutations.*

PROOF.

Let G be any group. [We need to find a set A and a permutation on A that forms a group $\overline{G}$ that is isomorphic to G.] We take the set G and define, for each $g \in G$, the function $T_g : G \to G$ by $T_g(x) = gx \ \forall x \in G$.

Now $T_g(x) = T_g(y) \Longrightarrow gx = gy \Longrightarrow x = y$ by left cancellation, so T_g is 1–1.

Given $y \in G$, by Theorem 2 (solutions of equations) $\exists$ a unique solution

$x \in G \ni gx = y$ or $T_g(x) = y$. Thus T_g is onto and so is a permutation on G.

Now define $\overline{G}$ by $\{T_g | g \in G\}$. For any $g, h \in G$,

$$(T_g T_h)(x) = T_g\big(T_h(x)\big) = T_g(hx) = g(hx) = (gh)(x) = T_{gh}(x) \ \forall \ x \in G,$$

so $\overline{G}$ is closed under composition. Then T_e is the identity and $T_g^{-1} = T_{g^{-1}}$. Since composition is associative, $\overline{G}$ is a group.

Now define $\phi : G \to \overline{G}$ by $\phi(g) = T_g \ \forall \ g \in G$.

$$\phi(g) = \phi(h) \Longrightarrow T_g = T_h \Longrightarrow T_g(e) = T_h(e) \Longrightarrow ge = he \Longrightarrow g = h,$$

so ϕ is 1–1. ϕ is clearly onto by construction.

Finally, for $g, h \in G$,

$$\phi(gh) = T_{gh} = T_g T_h = \phi(g)\phi(h),$$

so ϕ is an isomorphism. □

EXAMPLE. $U = \{1, 3, 5, 7\}$.

$$T_1 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 1 & 3 & 5 & 7 \end{bmatrix}, T_3 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 3 & 1 & 7 & 5 \end{bmatrix}, T_5 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 5 & 7 & 1 & 3 \end{bmatrix}, T_7 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 7 & 5 & 3 & 1 \end{bmatrix}.$$

Then $\overline{U(8)} = \{T_1, T_3, T_5, T_7\}$.

$U(8)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\overline{U(8)}$	T_1	T_3	T_5	T_7
T_1	T_1	T_3	T_5	T_7
T_3	T_3	T_1	T_7	T_5
T_5	T_5	T_7	T_1	T_3
T_7	T_7	T_5	T_3	T_1

THEOREM (6.2 — Properties of Elements Acting on Elements). *Suppose ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then*

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

PROOF.

$\phi(e) = \phi(ee) = \phi(e)\phi(e)$. Also, since $\phi(e) \in \overline{G}$, $\phi(e) = \overline{e}\phi(e) \Longrightarrow$ $\overline{e}\phi(e) = \phi(e)\phi(e) \Longrightarrow \overline{e} = \phi(e)$ by right cancellation. □

(2) For all $n \in \mathbb{Z}$ and for all $a \in G$, $\phi(a^n) = \big[\phi(a)\big]^n$.

PROOF.

For $n \in \mathbb{Z}$, $n \geq 0$, $\phi(a^n) = \big[\phi(a)\big]^n$ from the definition of an isomorphism and induction. For $n < 0$, $-n > 0$, so

$$\overline{e} = \phi(e) = \phi(a^n a^{-n}) = \phi(a^n)\phi(a^{-n}) = \phi(a^n)\big[\phi(a)\big]^{-n} \Longrightarrow \big[\phi(a)\big]^n = \phi(a^n).$$

□

(3) For all $a, b \in G$, $ab = ba \iff \phi(a)\phi(b) = \phi(b)\phi(a)$.

PROOF.

$$ab = ba \iff \phi(ab) = \phi(ba) \iff \phi(a)\phi(b) = \phi(b)\phi(a).$$

□

(4) $G = \langle a \rangle \iff \overline{G} = \langle \phi(a) \rangle$.

PROOF.

Let $G = \langle a \rangle$. By closure, $\langle \phi(a) \rangle \subseteq \overline{G}$. Since ϕ is onto, for any element $b \in \overline{G}$, $\exists\ a^k \in G \ni \phi(a^k) = b$. Thus $b = \left[\phi(a)\right]^k \implies b \in \langle \phi(a) \rangle$. Thus $\overline{G} = \langle \phi(a) \rangle$.

Now suppose $\overline{G} = \langle \phi(a) \rangle$. Clearly, $\langle a \rangle \subseteq G$. For all $b \in G$, $\phi(b) \in \langle \phi(a) \rangle$.

Thus $\exists\ k \in \mathbb{Z} \ni \phi(b) = \phi(a)^k = \phi(a^k)$. Since ϕ is 1–1, $b = a^k$. Thus $\langle a \rangle = G$. □

(5) $|a| = |\phi(a)|\ \forall\ a \in G$ *(Isomorphisms preserve order).*

PROOF.

$$a^n = e \iff \phi(a^n) = \phi(e) \iff \left[\phi(a)\right]^n = \overline{e}.$$

Thus a has infinite order $\iff$ $\phi(a)$ has infinite order, and a has finite order $n \iff$ $\phi(a)$ has infinite order n. □

(6) For a fixed integer k *and a fixed* $b \in G$, $x^k = b$ *has the same number of solutions in* G *as does* $x^k = \phi(b)$ *in* $\overline{G}$.

PROOF.

Suppose a is a solution of $x^k = b$ in G, i.e., $a^k = b$. Then

$$\phi(a^k) = \phi(b) \implies \left[\phi(a)\right]^k = \phi(b),$$

so $\phi(a)$ is a solution of $x^k = \phi(b)$ in $\overline{G}$.

Now suppose y is a solution of $x^k = \phi(b)$ in $\overline{G}$. Since ϕ is onto, $\exists\ a \in G \ni \phi(a) = y$. Then

$$\left[\phi(a)\right]^k = \phi(b) \iff \phi(a^k) = \phi(b) \implies a^k = b$$

since ϕ is 1–1. Thus a is a solution of $x^k = b$ in G.

Therefore, there exists a 1–1 correspondence between the sets of solutions. □

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

PROOF. Follows directly from property (5). □

EXAMPLE. Is $\mathbb{C}^* \approx \mathbb{R}^*$ with multiplication the operation of both groups?

SOLUTION.

$x^2 = -1$ has 2 solutions in $\mathbb{C}^*$, but none in $\mathbb{R}^*$, so by Theorem 6.2(6) no isomorphism can exist. □

THEOREM (6.3 — Properties of Isomorphisms Acting on Groups).

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

(1) ϕ^{-1} is an isomorphism from $\overline{G}$ onto G.

PROOF.

The inverse of ϕ is 1–1 since ϕ is. Let $g \in G$. $\phi^{-1}\big(\phi(g)\big) = g \Longrightarrow \phi$ is onto. Now let $x, y \in \overline{G}$. Then

$$\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y) \iff \phi\big(\phi^{-1}(xy)\big) = \phi\big(\phi^{-1}(x)\phi^{-1}(y)\big) \iff$$
$$xy = \phi\big(\phi^{-1}(x)\big)\phi\big(\phi^{-1}(y)\big) = xy.$$

Thus operations are preserved and ϕ^{-1} is an isomorphism. □

(2) G is Abelian $\iff$ $\overline{G}$ is Abelian.

PROOF.

Follows directly from Theorem 6.2(3) since isomorphisms preserve commutivity. □

(3) G is cyclic $\iff$ $\overline{G}$ is cyclic.

PROOF.

Follows directly from Theorem 6.2(4) since isomorphisms preserve order. □

(4) If $K \leq G$, then $\phi(K) = \{\phi(k) \mid k \in K\} \leq \overline{G}$.

PROOF.

Follows directly from Theorem 6.2(4) since isomorphisms preserve order. □

(5) If $\overline{K} \leq \overline{G}$, then $\phi^{-1}(\overline{K}) = \{g \in G \mid \phi(g) \in \overline{K}\} \leq G$.

PROOF.

Follows directly from (1) and (4). □

(6) $\phi\big(Z(G)\big) = Z(\overline{G})$.

PROOF.

Follows directly from Theorem 6.2(3) since isomorphisms preserve commutivity. □

DEFINITION (Automorphism). An isomorphims from a group G onto itself is called an automorphism.

PROBLEM (Psge 140 # 35). Show that the mapping $\phi(a + bi) = a - bi$ is an automorphism of $\mathbb{C}$ under addition. Show that ϕ preserves complex multiplication as well. (This means ϕ is an automorphims of $\mathbb{C}^*$ as well.)

SOLUTION.

ϕ is clearly 1–1 and onto. Suppose $a + bi, c + di \in \mathbb{C}$.

$$\phi\big[(a + bi) + (c + di)\big] = \phi\big[(a + c) + (b + d)i\big] = (a + c) - (b + d)i$$
$$(a - bi) + (c - di) = \phi(a + bi) + \phi(c + di),$$

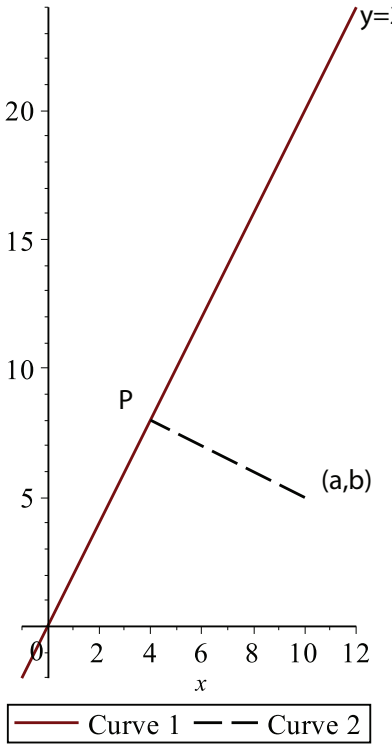
so ϕ is an automorphism of $\mathbb{C}$ under addition.

Now suppose $a + bi, c + di \in \mathbb{C}^*$.

$$\phi\big[(a + bi)(c + di)\big] = \phi\big[(ac - bd) + (ad + bc)i\big] = (ac - bd) - (ad + bc)i =$$
$$(a - bi)(c - di) = \phi(a + bi)\phi(c + di),$$

so ϕ is an automorphism of $\mathbb{C}^*$ under multiplication. □

EXAMPLE (related to Example 10 on Page 135). Consider $\mathbb{R}^2$. Any reflection across a line through the origin or rotation about the origin is an automorphism under componentwise addition. For example, consider the reflection about the line $y = 2x$.



Consider (a, b) not on $y = 2x$. The line through $(a, b) \perp y = 2x$ is

$y - b = -\frac{1}{2}\Big(x - a\Big)$. To find P (using substitution):

$$2x - b = -\frac{1}{2}\Big(x - a\Big) \Longrightarrow \frac{5}{2}x = \frac{1}{2}a + b \Longrightarrow x = \frac{1}{5}a + \frac{2}{5}b \Longrightarrow y = \frac{2}{5}a + \frac{4}{5}b.$$

Thus the direction vector $\mathbf{v} = P - (a, b)$ takes (a, b) to P.

$$\mathbf{v} = \Big(-\frac{4}{5}a + \frac{2}{5}b,\ \frac{2}{5}a - \frac{1}{5}b\Big).$$

Define

$$\phi(a, b) = (b, a).$$

ϕ is clearly 1–1 and onto.

Finally,

$$\phi\big[(a,b)+(c,d)\big] = \phi(a+c, b+d) = \\ (b+d,\ a+c) = (b,a)+(d,c) = \phi(a,b)+\phi(c,d),$$

so ϕ is an isomorphism.

DEFINITION (Inner Automorphism Induced by a).

Let G be a group, $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}\ \forall\, x \in G$ is called the inner automorphism of G induced by a.

EXAMPLE. The action of the inner automorphism of D_4 induced by R_{90} is given in the following table.

x	$\overset{\phi_{R_{90}}}{\rightarrow}$	$R_{90}\, x\, R_{90}^{-1}$
R_0	$\rightarrow$	$R_{90}R_0R_{90}^{-1} = R_0$
R_{90}	$\rightarrow$	$R_{90}R_{90}R_{90}^{-1} = R_{90}$
R_{180}	$\rightarrow$	$R_{90}R_{180}R_{90}^{-1} = R_{180}$
R_{270}	$\rightarrow$	$R_{90}R_{270}R_{90}^{-1} = R_{270}$
H	$\rightarrow$	$R_{90}HR_{90}^{-1} = V$
V	$\rightarrow$	$R_{90}VR_{90}^{-1} = H$
D	$\rightarrow$	$R_{90}DR_{90}^{-1} = D'$
D'	$\rightarrow$	$R_{90}D'R_{90}^{-1} = D$

PROBLEM (Page 145 # 45). Suppose g and h induce the same inner automorphism of a group G. Prove $h^{-1}g \in Z(G)$.

PROOF. Let $x \in G$. Then

$$\phi_g(x) = \phi_h(x) \Longrightarrow gxg^{-1} = hxh^{-1} \Longrightarrow h^{-1}gxg^{-1}h = x \Longrightarrow$$
$$(h^{-1}g)x(h^{-1}g)^{-1}h = x \Longrightarrow (h^{-1}g)x = x(h^{-1}g) \Longrightarrow$$

$h^{-1}g \in Z(G)$ since x is arbitrary. □

DEFINITION.

$\mathrm{Aut}(G) = \{\phi \mid \phi \text{ is an automorphism of } G\}$ and

$\mathrm{Inn}(G) = \{\phi \mid \phi \text{ is an inner automorphism of } G\}$.

THEOREM (6.4 — $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups). *$\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups under function composition.*

PROOF.

From the transitive portion of Theorem 3, compositions of isomorphisms are isomorphisms. Thus $\mathrm{Aut}(G)$ is closed under composition. We know function composition is associative and that the identity map is the identity automorphism.

Suppose $\alpha \in \mathrm{Aut}(G)$. α^{-1} is clearly 1–1 and onto. Now

$$\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y) \iff (\Longleftarrow \text{ by 1–1})$$
$$\alpha\big[\alpha^{-1}(xy)\big] = \alpha\big[\alpha^{-1}(x)\alpha^{-1}(y)\big] \iff xy = \alpha\big[\alpha^{-1}(x)\big]\alpha\big[\alpha^{-1}(y)\big] \iff$$
$$xy = xy.$$

Thus α^{-1} is operation preserving, and $\mathrm{Aut}(G)$ is a group.

Now let $\phi_g, \phi_h \in \text{Inn}(G) \subseteq \text{Aut}(G)$. For all $x \in G$,

$$\phi_g\phi_h(x) = \phi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x),$$

so $\phi_{gh} = \phi_g\phi_h \in \text{Inn}(G)$, and $\text{Inn}(G)$ is closed under composition.

Also, $\phi_g^{-1} = \phi_{g^{-1}}$ since

$$\phi_{g^{-1}}\phi_g(x) = \phi_{g^{-1}}(gxg^{-1}) = g^{-1}gxg^{-1}(g^{-1})^{-1} = g^{-1}gxg^{-1}g = exe = \phi_e(x),$$

and so also $\phi_{gg^{-1}} = \phi_e$. Thus $\text{Inn}(G) \subseteq \text{Aut}(G)$ by the two-step test. □

EXAMPLE. Find $\text{Inn}(\mathbb{Z}_{12})$.

SOLUTION.

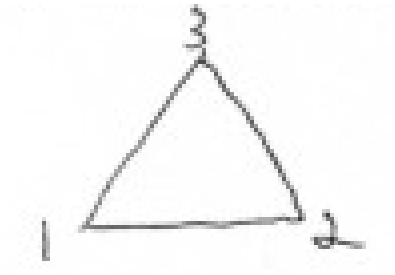
Since $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$, $\text{Inn}(\mathbb{Z}_{12}) = \{\phi_0, \phi_1, \phi_2, \ldots, \phi_{11}\}$, but the second list may have duplicates. That is the case here. For all $n \in \mathbb{Z}_{12}$ and for all $x \in \mathbb{Z}_{12}$,

$$\phi_n(x) = n + x + (-n) = n + (-n) + x = 0 + x = 0 + x + 0 = \phi_0(x),$$

the identity automorphism. Thus $\text{Inn}(\mathbb{Z}_{12}) = \{\phi_0\}$. □

EXAMPLE. Find $\text{Inn}(D_3)$.

SOLUTION.



$D_3 = \{\varepsilon, (1\ 2\ 3), (1\ 3\ 2), (2\ 3), (1\ 3), (1\ 2)\}$ as permutations. Then

$\text{Inn}(D_3) = \{\phi_\varepsilon, \phi_{(1\ 2\ 3)}, \phi_{(1\ 3\ 2)}, \phi_{(2\ 3)}, \phi_{(1\ 3)}, \phi_{(1\ 2)}\}$, but we need to eliminate repetitions.

$\phi_{(1\ 2\ 3)}(1\ 2\ 3) = (1\ 2\ 3)(1\ 2\ 3)(3\ 2\ 1) = (1\ 2\ 3)$.

$\phi_{(1\ 2\ 3)}(1\ 3\ 2) = (1\ 3\ 2)(1\ 2\ 3)(3\ 2\ 1) = (1\ 3\ 2)$.

$\phi_{(1\ 2\ 3)}(2\ 3) = (1\ 3\ 2)(2\ 3)(3\ 2\ 1) = (1\ 3)$.

$\phi_{(1\ 2\ 3)}(1\ 3) = (1\ 3\ 2)(1\ 3)(3\ 2\ 1) = (1\ 2)$.

$\phi_{(1\ 2\ 3)}(1\ 2) = (1\ 3\ 2)(1\ 2)(3\ 2\ 1) = (2\ 3)$. Thus $\phi_{(1\ 2\ 3)}$ is distinct from ϕ_ε.

$\phi_{(1\ 3\ 2)}(2\ 3) = (1\ 3\ 2)(2\ 3)(2\ 3\ 1) = (1\ 2)$. Thus $\phi_{(1\ 3\ 2)}$ is distinct.

$\phi_{(2\ 3)}(2\ 3) = (2\ 3)(2\ 3)(2\ 3) = (2\ 3)$.

$\phi_{(2\ 3)}(1\ 3) = (2\ 3)(1\ 3)(2\ 3) = (1\ 2)$. Thus $\phi_{(2\ 3)}$ is distinct

$\phi_{(1\ 3)}(2\ 3) = (1\ 3)(2\ 3)(1\ 3) = (1\ 2)$.

$\phi_{(1\ 3)}(1\ 3) = (1\ 3)(1\ 3)(1\ 3) = (1\ 3)$.

$\phi_{(1\ 3\ 2)}(1\ 3) = (1\ 3\ 2)(1\ 3)(2\ 3\ 1) = (2\ 3)$. Thus $\phi_{(1\ 3)}$ is distinct.

$\phi_{(1\ 2)}(2\ 3) = (1\ 2)(2\ 3)(1\ 2) = (1\ 3)$.

$\phi_{(1\ 2)}(1\ 3) = (1\ 2)(1\ 3)(1\ 2) = (2\ 3)$. Thus $\phi_{(1\ 2)}$ is distinct.

Therefore, there are no duplicates and

$\text{Inn}(D_3) = \{\phi_\varepsilon, \phi_{(1\ 2\ 3)}, \phi_{(1\ 3\ 2)}, \phi_{(2\ 3)}, \phi_{(1\ 3)}, \phi_{(1\ 2)}\}$. □

THEOREM (6.5 – $\mathrm{Aut}(\mathbb{Z}_n) = U(n)$). *For all* $n \in \mathbb{N}$, $\mathrm{Aut}(\mathbb{Z}_n) = U(n)$.

PROOF.

Let $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$. Then

$$\alpha(k) = \alpha(\underbrace{1+1+\cdots+1}_{k \text{ terms}}) = (\underbrace{\alpha(1)+\alpha(1)+\cdots+\alpha(1)}_{k \text{ terms}}) = k\alpha(1).$$

Now $|1| = n \Longrightarrow |\alpha(1)| = n$, so $\alpha(1)$ is a generator of $\mathbb{Z}_n$ since 1 is also a generator. Now consider

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

Suppose $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}_n)$ and $T(\alpha) = T(\beta)$. Then $\alpha(1) = \beta(1)$, so $\forall\ k \in \mathbb{Z}_n$, $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$. Thus $\alpha = \beta$ and T is 1–1.

[To show T is onto.] Now suppose $r \in U(n)$ and consider $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\alpha(s) = sr \bmod n\ \forall\ s \in \mathbb{Z}_n$.

[To show $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$.] Suppose $\alpha(x) = \alpha(y)$. Then $xr = yr \bmod n$.

But r^{-1} exists modulo $n \Longrightarrow xrr^{-1} = yrr^{-1} \bmod n \Longrightarrow x \cdot 1 = y \cdot 1 \bmod n \Longrightarrow$

$x = y \bmod n$, so α is 1–1.

Suppose $x \in \mathbb{Z}_n$. By Theorem2, $\exists\ s \in \mathbb{Z}_n \ni \alpha(s) = sr = x$, so α is onto.

Now suppose $x, y \in \mathbb{Z}_n$.

$$\alpha(x+y) = (x+y)r \bmod n = (xr+yr) \bmod n =$$
$$xr \bmod n + yr \bmod n = \alpha(x) + \alpha(y),$$

so $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$.

Since $T(\alpha) = \alpha(1) = r$, T is onto.

Finally, let $\alpha, \beta \in \text{Aut}(\mathbb{Z}_n)$. Then

$$T(\alpha\beta) = (\alpha\beta)(1) = \alpha\big[\beta(1)\big] = \alpha(\underbrace{1+1+\cdots+1}_{\beta(1) \text{ terms}})$$

$$\underbrace{\alpha(1)+\alpha(1)+\cdots+\alpha(1)}_{\beta(1) \text{ terms}} = \alpha(1)\beta(1) = T(\alpha)T(\beta),$$

so $\text{Aut}(\mathbb{Z}_n) \approx U(n)$. □

EXAMPLE. $\text{Aut}(\mathbb{Z}_{10}) \approx U(10)$. The multiplication tables for the two groups are given below:

$U(10)$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\text{Aut}(Z_{10})$	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

The isomorphism is clear.