Group Theory Exercises 7

Jason Sass

June 25, 2023

Isomorphisms

Exercise 1. Show that $f : \mathbb{R}^* \to \mathbb{R}^*$ defined by $f(x) = x^3$ for all $x \in \mathbb{R}^*$ is a group isomorphism.

Proof. Clearly, f is a function.

To prove f is bijective, we prove f is invertible.
Let $g : \mathbb{R}^* \to \mathbb{R}^*$ be defined by $g(x) = \sqrt[3]{x}$ for all $x \in \mathbb{R}^*$.
Let $x \in \mathbb{R}^*$.
Observe that $(g \circ f)(x) = g(f(x)) = g(x^3) = \sqrt[3]{x^3} = x$.
Hence, $g \circ f = id$.
Observe that $(f \circ g)(x) = f(g(x)) = f(\sqrt[3]{x}) = (\sqrt[3]{x})^3 = x$.
Hence, $f \circ g = id$.
Therefore, g is an inverse function of f, so f is invertible.
Since f is invertible iff f is bijective, then f is bijective.

We prove f is a homomorphism.
Let $a, b \in \mathbb{R}^*$.
Observe that $\mathbb{R}^*$ is an abelian group and

$$\begin{array}{rcl} f(ab) & = & (ab)^3 \\ & = & a^3b^3 \\ & = & f(a)f(b). \end{array}$$

Therefore, f is a homomorphism.
Since f is a bijective homomorphism, then f is an isomorphism. □

Exercise 2. For $n \neq 0, (\mathbb{Z}, +) \cong (n\mathbb{Z}, +)$.

Solution. Let $n \in \mathbb{Z}$.

If $n = 0$, then $n\mathbb{Z} = 0\mathbb{Z} = \{0\}$ which is the trivial group, so $\mathbb{Z} \ncong n\mathbb{Z}$ if $n = 0$. Thus, we restrict n to nonzero integers. We can use the definition of isomorphism to show there exists an explicit isomorphism. However, we can also use existing theorems. In fact, we see that $n\mathbb{Z} < \mathbb{Z}$. We also observe that $n\mathbb{Z} = \langle n \rangle$, the cyclic subgroup of $\mathbb{Z}$ generated by n. We know that every cyclic group of infinite order is isomorphic to $\mathbb{Z}$. □

Proof. Let n be a nonzero integer.

Observe that $n\mathbb{Z} < \mathbb{Z}$ and $n\mathbb{Z} = \langle n \rangle$.

Hence, $n\mathbb{Z}$ is the cyclic subgroup of $\mathbb{Z}$ generated by n.

Every cyclic group of infinite order is isomorphic to $\mathbb{Z}$.

Since $n \neq 0$, then $n\mathbb{Z}$ is of infinite order.

Hence, $n\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.

Therefore, $n\mathbb{Z} \cong \mathbb{Z}$, so $\mathbb{Z} \cong n\mathbb{Z}$. □

Exercise 3. $(\mathbb{Z}_6, +) \ncong (S_3, \circ)$.

Solution. We know that $|\mathbb{Z}_6| = 6$ and $|S_3| = 3! = 6$, but $\mathbb{Z}_6$ is abelian group, while S_3 is nonabelian.

Thus, we conjecture that there does not exist an isomorphism.

To prove this, let's suppose there does exist an isomorphism and derive a contradiction. □

Proof. Suppose $\mathbb{Z}_6$ is isomorphic to S_3.

Then there exists an isomorphism between $\mathbb{Z}_6$ and S_3.

Let $\phi : \mathbb{Z}_6 \mapsto S_3$ be some isomorphism.

Then ϕ is a bijective homomorphism.

Since ϕ is a homomorphism, then for every $[a], [b] \in \mathbb{Z}_6$, $\phi([a] + [b]) = \phi([a])\phi([b])$.

Since S_3 is non abelian, then $\circ$ is not commutative.

Therefore, there exist $\sigma, \tau \in S_3$ such that $\sigma\tau \neq \tau\sigma$.

Since $\mathbb{Z}_6$ is abelian, then for every $[a], [b] \in \mathbb{Z}_6$, $[a] + [b] = [b] + [a]$.

Since ϕ is bijective, then ϕ is surjective.

Therefore, since $\sigma \in S_3$, then there exists $[a] \in \mathbb{Z}_6$ such that $\phi([a]) = \sigma$.

Similarly, since $\tau \in S_3$, then there exists $[b] \in \mathbb{Z}_6$ such that $\phi([b]) = \tau$.

Observe that $\sigma\tau = \phi([a])\phi([b]) = \phi([a] + [b]) = \phi([b] + [a]) = \phi([b])\phi([a]) = \tau\sigma$.

Hence, we have $\sigma\tau = \tau\sigma$ and $\sigma\tau \neq \tau\sigma$, a contradiction.

Therefore, there is no isomorphism ϕ.

Since no isomorphism exists between $\mathbb{Z}_6$ and S_3, then $\mathbb{Z}_6$ is not isomorphic to S_3. □

Exercise 4. $(\mathbb{Z}_8^*, \cdot) \ncong (\mathbb{Z}_4, +)$.

Solution. We know that $|\mathbb{Z}_8^*| = \phi(8) = 4$ and $|\mathbb{Z}_4| = 4$, but $\mathbb{Z}_8^*$ is not cyclic, while $\mathbb{Z}_4$ is cyclic. Thus, intuitively, it appears these are not isomorphic groups. To formally prove this observation, we suppose there exists an isomorphism and derive a contradiction(ie, use proof by contradiction). In fact, since there are only 2 groups of order 4 up to isomorphism, the cyclic group of order 4 and the Klein 4 group, then $\mathbb{Z}_8^*$ is isomorphic to the Klein 4 group which is isomorphic to the symmetries of a rectangle, D_2. □

Proof. Suppose $\mathbb{Z}_8^* \cong \mathbb{Z}_4$. Then $\mathbb{Z}_4 \cong \mathbb{Z}_8^*$. Thus, if $\mathbb{Z}_4$ is cyclic, then $\mathbb{Z}_8^*$ is cyclic. Since $\mathbb{Z}_4$ is cyclic, then $\mathbb{Z}_8^*$ is cyclic. Hence, there exists a generator $g \in \mathbb{Z}_8^*$ such that $\langle g \rangle = \mathbb{Z}_8^*$. Thus, $|\langle g \rangle| = |\mathbb{Z}_8^*| = 4$.

The order of an element is the order of the cyclic subgroup generated by that element. Thus, the order of g is 4. Hence, there exists an element of $\mathbb{Z}_8^*$ that has order 4. Each element of $\mathbb{Z}_8^*$ is its own inverse. Thus, $x = x^{-1}$ for all $x \in \mathbb{Z}_8^*$. Hence, $x^2 = 1$ for all $x \in \mathbb{Z}_8^*$. This implies the order of each element is at most 2. Thus, there is no element in $\mathbb{Z}_8^*$ of order 4. Hence, there is an element of $\mathbb{Z}_8^*$ of order 4 and there is not an element of $\mathbb{Z}_8^*$ of order 4, a contradiction. Therefore, $\mathbb{Z}_8^* \ncong \mathbb{Z}_4$. □

Exercise 5. $(\mathbb{Z}_5^*, \cdot) \cong (\mathbb{Z}_{10}^*, \cdot)$, but $(\mathbb{Z}_{12}^*, \cdot) \ncong (\mathbb{Z}_{10}^*, \cdot)$.

Solution. We draw out the Cayley multiplication tables and see that $\mathbb{Z}_5^* \cong \mathbb{Z}_4$ because $\mathbb{Z}_5^*$ is cyclic.

Similarly, $\mathbb{Z}_{10}^* \cong \mathbb{Z}_4$ because $\mathbb{Z}_{10}^*$ is cyclic.

However, $\mathbb{Z}_{12}^* \cong$ Kelin 4 group which is not cyclic, so $\mathbb{Z}_{12}^*$ is not cyclic. □

Proof. Observe that $|\mathbb{Z}_5^*| = |\mathbb{Z}_{10}^*| = |\mathbb{Z}_{12}^*| = 4$, so each group of units is a group of order 4. Since $\langle 2 \rangle = \mathbb{Z}_5^*$, then $\mathbb{Z}_5^*$ is cyclic. Every cyclic group of finite order n is isomorphic to $(\mathbb{Z}_n, +)$, so $\mathbb{Z}_5^*$ is isomorphic to $\mathbb{Z}_4$. Hence, $\mathbb{Z}_5^* \cong \mathbb{Z}_4$.

Since $\langle 3 \rangle = \mathbb{Z}_{10}^*$, then $\mathbb{Z}_{10}^*$ is cyclic. Hence, $\mathbb{Z}_{10}^* \cong \mathbb{Z}_4$, so $\mathbb{Z}_4 \cong \mathbb{Z}_{10}^*$. Since $\mathbb{Z}_5^* \cong \mathbb{Z}_4$ and $\mathbb{Z}_4 \cong \mathbb{Z}_{10}^*$, then $\mathbb{Z}_5^* \cong \mathbb{Z}_{10}^*$.

Suppose $\mathbb{Z}_{12}^* \cong \mathbb{Z}_{10}^*$. Since $\mathbb{Z}_4 \cong \mathbb{Z}_{10}^*$, then $\mathbb{Z}_{10}^* \cong \mathbb{Z}_4$. Thus, $\mathbb{Z}_{12}^* \cong \mathbb{Z}_4$, so $\mathbb{Z}_4 \cong \mathbb{Z}_{12}^*$. Since $\mathbb{Z}_4$ is cyclic, then $\mathbb{Z}_{12}^*$ is cyclic. Hence, there exists $g \in \mathbb{Z}_{12}^*$ such that $\langle g \rangle = \mathbb{Z}_{12}^*$. Thus, $|\langle g \rangle| = |\mathbb{Z}_{12}^*| = 4$. The order of an element is the order of the cyclic subgroup generated by that element. Hence, the order of g is 4, so $|g| = 4$.

Observe that $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ and $1 * 1 = 1$ and $5 * 5 = 5$ and $7 * 7 = 1$ and $11 * 11 = 1$. Hence, $x^2 = 1$ for each $x \in \mathbb{Z}_{12}^*$. Thus, the order of each $x \in \mathbb{Z}_{12}^*$ is at most 2. Therefore, $|x| \leq 2$ for all $x \in \mathbb{Z}_{12}^*$. In particular, $|g| \leq 2$, so $|g| \neq 4$. Thus, we have $|g| = 4$ and $|g| \neq 4$, a contradiction. Therefore, $\mathbb{Z}_{12}^* \ncong \mathbb{Z}_{10}^*$. □

Exercise 6. The cyclic subgroup of $\mathbb{Z}_{12}$ generated by $[3]_{12}$ is isomorphic to $\mathbb{Z}_4$.

Solution. Let G be the cyclic subgroup of $\mathbb{Z}_{12}$ generated by $[3]_{12}$.

Then $G = \{k[3]_{12} : k \in \mathbb{Z}\} = \{[0], [3], [6], [9]\}$.

Since $\mathbb{Z}_4$ is a cyclic group of order 4, then $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$.

Let $\phi : \mathbb{Z}_4 \to G$ be defined by $\phi([x]_4) = [3x]_{12}$ for all $[x]_4 \in \mathbb{Z}_4$.

We prove ϕ is a group isomorphism.

We must first prove ϕ is well defined.

Let $[a]_4, [b]_4 \in \mathbb{Z}_4$ such that $[a]_4 = [b]_4$.

Then $a \equiv b \pmod{4}$, so $4 | a - b$.

Thus, $3 * 4 | 3(a - b)$, so $12 | 3a - 3b$.

Hence, $3a \equiv 3b \pmod{12}$, so $[3a]_{12} = [3b]_{12}$.

Therefore, $\phi([a]_4) = \phi([b]_4)$.

Since $[a]_4 = [b]_4$ implies $\phi([a]_4) = \phi([b]_4)$, then ϕ is well defined.

Thus, ϕ is a function.

We prove ϕ is a group isomorphism.

Let $[a]_4, [b]_4 \in \mathbb{Z}_4$.
Then

$$\begin{aligned}\phi([a]_4 + [b]_4) &= \phi([a+b]_4)\\ &= [3(a+b)]_{12}\\ &= [3a+3b]_{12}\\ &= [3a]_{12} + [3b]_{12}\\ &= \phi([a]_4) + \phi([b]_4).\end{aligned}$$

Thus, ϕ is a homomorphism.

We prove ϕ is injective.
Let $[a]_4, [b]_4 \in \mathbb{Z}_4$ such that $\phi([a]_4) = \phi([b]_4)$.
Then $[3a]_{12} = [3b]_{12}$, so $3a \equiv 3b \pmod{12}$.
Hence, $12|3a - 3b$, so $3 * 4|3(a - b)$.
Thus, $4|a - b$, so $a \equiv b \pmod 4$.
Therefore, $[a]_4 = [b]_4$.
Hence, $\phi([a]_4) = \phi([b]_4)$ implies $[a]_4 = [b]_4$, so ϕ is injective.

We prove ϕ is surjective.
Let y be an arbitrary element of G.
Then there exists an integer k such that $y = k[3]_{12}$.
Thus, $[k]_4 \in \mathbb{Z}_4$ and $\phi([k]_4) = [3k]_{12} = [k * 3]_{12} = k[3]_{12} = y$.
Hence, there exists $[k]_4 \in \mathbb{Z}_4$ such that $\phi([k]_4) = y$, so ϕ is surjective.
Therefore, ϕ is bijective, so ϕ is a bijective homomorphism.
Thus, ϕ is an isomorphism, so $\mathbb{Z}_4 \cong G$.
Hence, $G \cong \mathbb{Z}_4$. □

Exercise 7. $(\mathbb{Z}_2 \times \mathbb{Z}_3, +) \cong (\mathbb{Z}_6, +)$.

Solution. We make some observations about each group.

We know that $|\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_2||\mathbb{Z}_3| = 2 * 3 = 6$ and $|\mathbb{Z}_6| = 6$, so both groups are finite of order 6.

We also know that identity of $\mathbb{Z}_6$ is 0 and identity of $\mathbb{Z}_2 \times \mathbb{Z}_3$ is $(0, 0)$ (because we can draw out the Cayley table for $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Also, $\mathbb{Z}_6$ is a cyclic group with generators 1 and 5.

Likewise $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic with generators $(1, 1)$ and $(1, 2)$.

We know that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ since $\gcd(2, 3) = 1$.

Since both groups are cyclic, then we can express each element as a multiple of its generators.

Thus, $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1, 1) \rangle = \{k(1, 1) : k \in \mathbb{Z}\} = \{(k, k) : k \in \mathbb{Z}\}$.

Hence, one possible isomorphism is $f : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ given by $f([a]_6) = ([a]_2, [a]_3)$, so

$$\begin{array}{rcl} f(0) & = & (0,0) \\ f(1) & = & (1,1) \\ f(2) & = & (0,2) \\ f(3) & = & (1,0) \\ f(4) & = & (0,1) \\ f(5) & = & (1,2). \end{array}$$

Also, $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,2) \rangle = \{k(1,2) : k \in \mathbb{Z}\} = \{(k, 2k) : k \in \mathbb{Z}\}$.

Hence, another isomorphism is $g : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ given by $g([b]_6) = ([b]_2, [2b]_3)$, so

$$\begin{array}{rcl} g(0) & = & (0,0) \\ g(1) & = & (1,2) \\ g(2) & = & (0,1) \\ g(3) & = & (1,0) \\ g(4) & = & (0,2) \\ g(5) & = & (1,1). \end{array}$$

Thus, there are at least 2 isomorphisms.

So, how many actual isomorphisms exist?

Can there exist more than 2 isomorphisms? Suppose there are more than 2 isomorphisms. Then there exist at least 3 isomorphisms. Since f and g are distinct isomorphisms, let $h : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ be a third distinct isomorphism. Then $h \neq f$ and $h \neq g$.

Since isomorphisms preserve identity, then $h(0) = (0,0)$.

Since isomorphisms preserve finite order of an element and $|3| = 2$ and $(1,0)$ is the only element in $\mathbb{Z}_2 \times \mathbb{Z}_3$ that has order 2, then $h(3) = (1,0)$.

Since $|1| = 6$ and $|(1,1)| = |(1,2)| = 6$, then either $h(1) = (1,1)$ or $h(1) = (1,2)$.

We consider these cases separately.

Suppose $h(1) = (1,1)$. Since isomorphisms preserve inverses, then $h(-1) = -(h1) = -(1,1) = (-1,-1) = (-1+2, -1+3) = (1,2)$. Thus, $h(-1) = h(-1+6) = h(5) = (1,2)$. Since h is a homomorphism, then $h(3+5) = h(3) + h(5)$. Hence, $h(8) = (1,0) + (1,2) = (2,2) = (2-2,2) = (0,2)$. Thus, $(0,2) = h(8) = h(8-6) = h(2)$, so $h(2) = (0,2)$. Therefore, $h(-2) = -h(2) = -(0,2) = (0,-2) = (0,-2+3) = (0,1)$. Hence, $(0,1) = h(-2) = h(-2+6) = h(4)$, so $h(4) = (0,1)$.

Thus, we have

$$\begin{aligned} h(0) &= (0,0) \\ h(1) &= (1,1) \\ h(2) &= (0,2) \\ h(3) &= (1,0) \\ h(4) &= (0,1) \\ h(5) &= (1,2). \end{aligned}$$

Therefore, $h = f$. Hence, $h = f$ and $h \neq f$, a contradiction. Therefore, $h(1) \neq (1,1)$.

Suppose $h(1) = (1,2)$.

In a similar fashion, we can show that $h(1) \neq (1,2)$.

Therefore, h does not exist, so there are not more than 2 isomorphisms. Hence, there are at most 2 isomorphisms. Since there are at least 2 isomorphisms (namely, f and g) and there are at most 2 isomorphisms, then there are exactly 2 isomorphisms. □

Proof. The direct product group $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ has finite order 6 since $|\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_2||\mathbb{Z}_3| = 2 * 3 = 6$ The order of 1 in $\mathbb{Z}_2$ is 2 since $[2][1] = [2] = [0]_2$. The order of 1 in $\mathbb{Z}_3$ is 3 since $[3][1] = [3] = [0]_3$. Therefore, the order of $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ is the least common multiple of 2 and 3. Hence, $|(1,1)| = 6$. The order of the element $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ is the order of the cyclic subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_3$ generated by $(1,1)$.

Let G be the cyclic subgroup generated by $(1,1)$. Then $G \subset \mathbb{Z}_2 \times \mathbb{Z}_3$ and $|G| = 6 = |\mathbb{Z}_2 \times \mathbb{Z}_3|$.

If S is a finite set and T is a subset of S such that $|T| = |S|$, then $T = S$. Since $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a finite set and $G \subset \mathbb{Z}_2 \times \mathbb{Z}_3$ and $|G| = |\mathbb{Z}_2 \times \mathbb{Z}_3|$, then $G = \mathbb{Z}_2 \times \mathbb{Z}_3$. Therefore, the element $(1,1)$ is a generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$, so the group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. Hence, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group of order 6. Every cyclic group of finite order n is isomorphic to $(\mathbb{Z}_n, +)$. Hence, every cyclic group of finite order 6 is isomorphic to $(\mathbb{Z}_6, +)$. Thus, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $(\mathbb{Z}_6, +)$.

We exhibit an isomorphism explicitly and prove it is an isomorphism.

Let $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ be defined by $\phi([x]_6) = ([x]_2, [2x]_3)$ for all $[x]_6 \in \mathbb{Z}_6$.

We must prove ϕ is well defined and then prove ϕ is a group isomorphism.

Let $[a], [b] \in \mathbb{Z}_6$ such that $[a] = [b]$. Then $[a]_6 = [b]_6$, so $a \equiv b \pmod 6$. Thus, $6|a-b$, so $a - b = 6k = 2(3k) = 3(2k)$ for some integer k. Since $3k$ is an integer, then $2|a-b$. Since $2k$ is an integer, then $3|a-b$. Thus, $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$. Hence, $[a]_2 = [b]_2$ and $[a]_3 = [b]_3$. Thus, $[2]_3[a]_3 = [2]_3[b]_3$, so $[2a]_3 = [2b]_3$. Hence, $([a]_2, [2a]_3) = ([b]_2, [2b]_3)$, so $\phi([a]_3) = \phi([b]_3)$. Therefore, $[a]_6 = [b]_6$ implies $\phi([a]_3) = \phi([b]_3)$, so ϕ is well defined. Hence, ϕ is a function.

Let $[a], [b] \in \mathbb{Z}_6$.

Then

$$\begin{aligned}\phi([a]_6 + [b]_6) &= \phi([a+b]_6) \\ &= ([a+b]_2, [2(a+b)]_3) \\ &= ([a+b]_2, [2a+2b]_3) \\ &= ([a]_2 + [b]_2, [2a]_3 + [2b]_3) \\ &= ([a]_2, [2a]_3) + ([b]_2, [2b]_3) \\ &= \phi([a]_6) + \phi([b]_6).\end{aligned}$$

Hence, ϕ is a group homomorphism.

We prove ϕ is injective.

Let $[x]_6 \in \ker(\phi)$. Then $[x]_6 \in \mathbb{Z}_6$ and $\phi([x]_6) = ([0]_2, [0]_3)$. Hence, $0 \leq x < 6$ and $([x]_2, [2x]_3) = ([0]_2, [0]_3)$. Thus, $[x]_2 = [0]_2$ and $[2x]_3 = [0]_3$. Hence, $x \equiv 0 \pmod 2$ and $2x \equiv 0 \pmod 3$. Since $x \equiv 0 \pmod 2$, then either $x = 0$ or $x = 2$ or $x = 4$. Since $2x \equiv 0 \pmod 3$, then $x = 0$ or $x = 3$. Thus, $x = 0$, so $[x]_6 \in \{[0]_6\}$. Hence, $[x]_6 \in \ker(\phi)$ implies $[x]_6 \in \{[0]_6\}$, so $\ker(\phi) \subset \{[0]_6\}$. Since ϕ is a group homomorphism, then $[0]_6 \in \ker(\phi)$, so $\{[0]_6\} \subset \ker(\phi)$. Therefore, $\ker(\phi) \subset \{[0]_6\}$ and $\{[0]_6\} \subset \ker(\phi)$, so $\ker(\phi) = \{[0]_6\}$. Hence, ϕ is injective.

Since $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ are finite sets and $|\mathbb{Z}_6| = 6 = |\mathbb{Z}_2 \times \mathbb{Z}_3|$ and ϕ is a function, then ϕ is injective iff ϕ is surjective.

Since ϕ is injective, then this implies ϕ is surjective.

Therefore, ϕ is a bijective homomorphism, so ϕ is an isomorphism.

Hence, $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, so $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. □

Exercise 8. $(S_n, \circ) \cong (A_{n+2}, \circ)$.

Proof. Let $n \in \mathbb{Z}^+$.

Let S_n be the symmetric group on n symbols.

Let A_{n+2} be the alternating group on $n+2$ symbols.

Let $\sigma \in S_n$.

We first exhibit a left representation of σ.

Let $(n+1, n+2)$ be a transposition in A_{n+2}.

Let $\lambda_\sigma = \sigma$ if σ is even and $\lambda_\sigma = \sigma(n+1, n+2)$ if σ is odd.

We prove $\lambda_\sigma \in A_{n+2}$.

Either σ is even or odd.

We consider these cases separately.

Case 1: Suppose σ is even.

Then $\lambda_\sigma = \sigma$, so λ_σ is even.

Every even permutation in S_n is contained in S_{n+2}.

Since $\lambda_\sigma \in S_{n+2}$ and λ_σ is even, then $\lambda_\sigma \in A_{n+2}$.

Case 2: Suppose σ is odd.

Then $\lambda_\sigma = \sigma(n+1, n+2)$.

Since σ is odd and $(n+1, n+2)$ is odd, then λ_σ is a product of permutations of the same parity.

Hence, λ_σ is even.

Since $\lambda_\sigma \in S_{n+2}$ and λ_σ is even, then $\lambda_\sigma \in A_{n+2}$.

Thus, in all cases, $\lambda_\sigma \in A_{n+2}$.

Hence, $\lambda_\sigma \in A_{n+2}$ for all $\sigma \in S_n$.

Let $H = \{\lambda_\sigma : \sigma \in S_n\}$.

We prove $H < A_{n+2}$ by the subgroup test.

Let $\lambda_\sigma \in H$. Then $\sigma \in S_n$. Thus, $\lambda_\sigma \in A_{n+2}$. Hence, $\lambda_\sigma \in H$ implies $\lambda_\sigma \in A_{n+2}$, so $H \subset A_{n+2}$.

Let (1) be the identity of A_{n+2}. Then (1) is the identity permutation and $(1) \in S_n$. Since (1) is even, then $\lambda_{(1)} = (1)$. Hence, $(1) \in H$. Therefore, the identity of A_{n+2} is in H.

We prove H is closed under permutation multiplication.

Let $\lambda_\alpha, \lambda_\beta \in H$.

Then $\alpha, \beta \in S_n$.

We prove $\lambda_\alpha \lambda_\beta \in H$.

A permutation is either even or odd, so there are 4 cases to consider.

Case 1: Suppose α and β are even.

Then $\alpha\beta$ is even and $\lambda_\alpha = \alpha$ and $\lambda_\beta = \beta$.

Observe that $\lambda_\alpha \lambda_\beta = \alpha\beta = \lambda_{\alpha\beta}$.

Since $\alpha\beta \in S_n$, then $\lambda_{\alpha\beta} \in H$, so $\lambda_\alpha \lambda_\beta \in H$.

Case 2: Suppose α is even and β is odd.

Then

Let $\phi : S_n \to A_{n+2}$ be defined by $\phi(\sigma) = \lambda_\sigma$ for all $\sigma \in S_n$.

We prove ϕ is an isomorphism. □

Exercise 9. Show that $\mathbb{Z}_{17}^* \cong \mathbb{Z}_{16}$.

Solution. We know that the order of both groups is 16.

Since $[3]_{17}$ has order 16, then $\mathbb{Z}_{17}^*$ is cyclic and $\mathbb{Z}_{17}^* = \langle [3]^k : k \in \mathbb{Z}\} = \{[3], [3]^2, [3]^3, ..., [3]^{16}\}$.

Any cyclic group of order 16 is isomorphic to $\mathbb{Z}_{16}$, so $\mathbb{Z}_{17}^* \cong \mathbb{Z}_{16}$.

Now, to devise an actual isomorphism, let $\phi : \mathbb{Z}_{16} \to \mathbb{Z}_{17}^*$ be defined by $\phi([k]_{16}) = [3]_{17}^k$ for all $[k] \in \mathbb{Z}_{16}$.

Clearly, ϕ is a binary relation from $\mathbb{Z}_{16}$ to $\mathbb{Z}_{17}^*$.

Let $[a], [b] \in \mathbb{Z}_{16}$ such that $[a] = [b]$. Then $a, b \in \mathbb{Z}$ and $0 \leq a, b < 16$ and $a \equiv b \pmod{16}$. Since $|[3]| = 16$ in $\mathbb{Z}_{17}^*$, then $3^a = 3^b$ iff $a \equiv b \pmod{16}$. Thus, $3^a = 3^b$, so $\phi([a]) = \phi([b])$. Hence, ϕ is well defined, so ϕ is a function.

Observe that

$$\begin{aligned}\phi([a]_{16}+[b]_{16}) &= \phi([a+b]_{16}) \\ &= [3]_{17}^{a+b} \\ &= [3]^a[3]^b \\ &= \phi([a])\phi([b]).\end{aligned}$$

Therefore, ϕ is a homomorphism.

Suppose $\phi([a]) = \phi([b]$.
Then $[3]^a = [3]^b$.
Since $|[3]| = 16$ in $\mathbb{Z}_{17}^*$, then $[3]^a = [3]^b$ iff $a \equiv b \pmod{16}$.
Thus, $a \equiv b \pmod{16}$.
Since $0 \leq a, b < 16$, then this implies $a = b$.
Therefore, ϕ is injective.

s To prove ϕ is surjective, assume $[3]_{17}^a \in \mathbb{Z}_{17}^*$.
Then $a \in \mathbb{Z}$, so $[a]_{16} \in \mathbb{Z}_{16}$.
Observe that $\phi([a]_{16}) = [3]_{17}^a$.
Hence, there exists $[a]_{16} \in \mathbb{Z}_{16}$ such that $\phi([a]_{16}) = [3]_{17}^a$.
Therefore ϕ is surjective.
Hence, ϕ is a bijective homomorphism, so ϕ is an isomorphism. □

Exercise 10. $(\mathbb{Z}_5^*, *) \cong (\mathbb{Z}_4, +)$.

Solution. We can write out the multiplication tables for each group. □

Proof. Observe that $\mathbb{Z}_5^* = \{[1], [2], [3], [4]\}$.
Observe that $|\mathbb{Z}_5^*| = \phi(5) = 5 - 1 = 4$.

We prove $[2] \in \mathbb{Z}_5^*$ has order 4.
Observe that $[2]^1 = [2] \neq [1]_5$.
Observe that $[2]^2 = [4] \neq [1]_5$.
Observe that $[2]^3 = [8] = [3] \neq [1]_5$.
Observe that $[2]^4 = [16] = [1]_5$.
Hence, the order of $[2]$ is 4.
The order of $[2]$ is the order of the cyclic subgroup generated by $[2]$.
Let H be the cyclic subgroup of $\mathbb{Z}_5^*$ generated by $[2]$.
Then $H < \mathbb{Z}_5^*$ and $|H| = 4$.
Since $H \subset \mathbb{Z}_5^*$ and $|H| = 4 = |\mathbb{Z}_5^*|$ and $\mathbb{Z}_5^*$ is finite, then $H = \mathbb{Z}_5^*$.
Hence, $\mathbb{Z}_5^*$ is cyclic.
Every cyclic group of finite order n is isomorphic to $\mathbb{Z}_n$, so every cyclic group of finite order 4 is isomorphic to $\mathbb{Z}_4$.
In particular, $\mathbb{Z}_5^*$ is isomorphic to $\mathbb{Z}_4$. □

Exercise 11. For prime p, $(\mathbb{Z}_p^*, *) \cong (\mathbb{Z}_{p-1}, +)$.

Solution. We can try some examples like the group of units $\mathbb{Z}_5^*$ and verify computationally via Cayley table or construct an explicit isomorphism to show that it is isomorphic to the cyclic group $\mathbb{Z}_4$.

We can then generalize this argument.

To do this, we need to show in general why these groups are isomorphic.

After thinking about this, we can use Euler's theorem to show that there exists an element $a \in \mathbb{Z}_p^*$ such that $|a| = p-1$ which shows that there exists a cyclic subgroup of $\mathbb{Z}_p^*$ that is isomorphic to $\mathbb{Z}_{p-1}$.

Since $\mathbb{Z}_p^*$ is a finite group and there exists a subgroup that has the same number of elements, then this subgroup must equal the group itself.

So, we essentially must show that $\mathbb{Z}_p^*$ is a cyclic group because every cyclic group of finite order $p-1$ must be isomorphic to $\mathbb{Z}_{p-1}$. □

Proof. Let p be prime. Then $p > 1$. Let $(\mathbb{Z}_p^*, *)$ be the group of units of $\mathbb{Z}_p$. Let $(\mathbb{Z}_{p-1}, +)$ be the cyclic group of integers modulo $p-1$.

Observe that $\mathbb{Z}_p^* = \{[1], [2], ..., [p-1]\}$.

Observe that $|\mathbb{Z}_p^*| = \phi(p) = p - 1 = |\mathbb{Z}_{p-1}|$. Hence, both groups have finite order $p-1$.

We prove $\mathbb{Z}_p^*$ is cyclic. Thus, we shall prove there exists an element $[a] \in \mathbb{Z}_p^*$ such that $\mathbb{Z}_p^* = \langle [a] \rangle$.

Let $[a]$ be some element of $\mathbb{Z}_p^*$ such that $|[a]| = k$. The order of an element in a finite group is finite and so $1 \leq k \leq p-1$, since the order of $\mathbb{Z}_p^*$ is $p-1$. Then k is the least positive integer such that $[a]^k = [1]_p$. Since $\mathbb{Z}_p^*$ is a finite group of order $p-1$, then by a corollary to Lagrange's theorem, $[x]^{p-1} = [1]_p$ for all $[x] \in \mathbb{Z}_p^*$. In particular, $[a]^{p-1} = [1]_p$. Since the order of $[a]_p$ is k, then $[a]^{p-1} = [1]_p$ iff $k|p-1$. Hence, $k|p-1$.

We prove $k = p - 1$.

Let H be the cyclic

Either $p = 2$ or $p > 2$. □

Exercise 12. Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$ be group isomorphisms.

Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by $\phi(x_1, x_2) = (\theta_1(x_1), \theta_2(x_2))$ for all $(x_1, x_2) \in G_1 \times G_2$.

Then ϕ is a group isomorphism.

Proof. Let $(x_1, x_2) \in G_1 \times G_2$.

Then $\theta_1(x_1) \in H_1$ and $\theta_2(x_2) \in H_2$.

Therefore, $(\theta_1(x_1), \theta_2(x_2)) \in H_1 \times H_2$.

Hence, ϕ is a function.

Let (x_1, x_2) and (x_3, x_4) be arbitrary elements of $G_1 \times G_2$.

Then

$$\begin{aligned}\phi((x_1,x_2)(x_3,x_4)) &= \phi(x_1x_3,x_2x_4)\\ &= (\theta_1(x_1x_3),\theta_2(x_2x_4))\\ &= (\theta_1(x_1)\theta_1(x_3),\theta_2(x_2)\theta_2(x_4))\\ &= (\theta_1(x_1),\theta_2(x_2))(\theta_1(x_3),\theta_2(x_4))\\ &= \phi(x_1,x_2)\phi(x_3,x_4).\end{aligned}$$

Therefore, ϕ is a group homomorphism.

Suppose $\phi(x_1,x_2) = \phi(x_3,x_4)$.
Then $(\theta_1(x_1),\theta_2(x_2)) = (\theta_1(x_3),\theta_2(x_4))$.
Thus, $\theta_1(x_1) = \theta_1(x_3)$ and $\theta_2(x_2) = \theta_2(x_4)$.
Since θ_1 is injective, then $x_1 = x_3$.
Since θ_2 is injective, then $x_2 = x_4$.
Hence, $(x_1,x_2) = (x_3,x_4)$.
Therefore, ϕ is injective.

Let $(h_1,h_2) \in H_1 \times H_2$.
Then $h_1 \in H_1$ and $h_2 \in H_2$.
Since θ_1 is surjective, then there exists $g_1 \in G_1$ such that $\theta_1(g_1) = h_1$.
Since θ_2 is surjective, then there exists $g_2 \in G_1$ such that $\theta_2(g_2) = h_2$.
Hence, there exists $(g_1,g_2) \in G_1 \times G_2$ such that $\phi(g_1,g_2) = (\theta_1(g_1),\theta_2(g_2)) = (h_1,h_2)$.
Therefore, ϕ is surjective.

Thus, ϕ is bijective, so ϕ is a bijective homomorphism.
Therefore, ϕ is an isomorphism. □

Exercise 13. Prove $\mathbb{Z}_6 \times \mathbb{Z}_{10} \cong \mathbb{Z}_7^* \times \mathbb{Z}_{11}^*$.

Solution. Both groups are direct products of order 60 and are not cyclic.

Observe that $\mathbb{Z}_6$ is a cyclic group of order 6 with generator $[1]_6$. Hence, $\mathbb{Z}_6$ is abelian.

Observe that $\mathbb{Z}_{10}$ is a cyclic group of order 10 with generator $[1]_{10}$. Hence, $\mathbb{Z}_{10}$ is abelian.

Thus, the direct product $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ is abelian.

Observe that $\mathbb{Z}_6 \times \mathbb{Z}_{10} = \{([a],[b]) : [a] \in \mathbb{Z}_6, [b] \in \mathbb{Z}_{10}\} = \{([a],[b]) : 0 \leq a < 6, 0 \leq b < 10\}$.

Observe that $|\mathbb{Z}_7^*| = \phi(7) = 6$. The group $\mathbb{Z}_7^*$ has element $[3]_7$ of order 6, so $[3]$ is a generator of $\mathbb{Z}_7^*$. Hence, $\mathbb{Z}_7^*$ is cyclic and $\mathbb{Z}_7^* = \langle [3] \rangle = \{[3]^k : k \in \mathbb{Z}\} = \{[3]^k : 0 \leq k < 6\}$. Thus, $\mathbb{Z}_7^*$ is abelian and $\mathbb{Z}_7^* \cong \mathbb{Z}_6$.

Observe that $|\mathbb{Z}_{11}^*| = \phi(11) = 10$. The group $\mathbb{Z}_{11}^*$ has element $[2]_{11}$ of order 10, so $[2]$ is a generator of $\mathbb{Z}_{11}^*$. Hence, $\mathbb{Z}_{11}^*$ is cyclic and $\mathbb{Z}_{11}^* = \langle [2] \rangle = \{[2]^m : m \in \mathbb{Z}\} = \{[2]^m : 0 \leq m < 10\}$. Thus, $\mathbb{Z}_{11}^*$ is abelian and $\mathbb{Z}_{11}^* \cong \mathbb{Z}_{10}$.

Since $\mathbb{Z}_7^*$ and $\mathbb{Z}_{11}^*$ are abelian, then $\mathbb{Z}_7^* \times \mathbb{Z}_{11}^*$ is abelian.

Observe that $\mathbb{Z}_7^* \times \mathbb{Z}_{11}^* = \{([a],[b]) : [a] \in \mathbb{Z}_7^*, [b] \in \mathbb{Z}_{11}^*\} = \{([3]^k,[2]^m) : 0 \leq k < 6, 0 \leq m < 10\}$. □

Proof. Define $\theta_1 : \mathbb{Z}_6 \to \mathbb{Z}_7^*$ by $\theta_1([a]) = [3]^a$ for all $[a] \in \mathbb{Z}_6$.

Define $\theta_2 : \mathbb{Z}_{10} \to \mathbb{Z}_{11}^*$ by $\theta_2([b]) = [2]^b$ for all $[b] \in \mathbb{Z}_{10}$.

Define $\phi : \mathbb{Z}_6 \times \mathbb{Z}_{10} \to \mathbb{Z}_7^* \times \mathbb{Z}_{11}^*$ by $\phi([a],[b]) = ([3]^a,[2]^b)$ for all $([a],[b]) \in \mathbb{Z}_6 \times \mathbb{Z}_{10}$.

To prove ϕ is an isomorphism, we must prove θ_1 and θ_2 are group isomorphisms.

We first prove θ_1 is a group isomorphism.

Clearly, θ_1 is a binary relation from $\mathbb{Z}_6$ to $\mathbb{Z}_7^*$.

Let $[a]_6, [b]_6 \in \mathbb{Z}_6$ such that $[a] = [b]$. Then $a \equiv b \pmod 6$. Since the order of $[3]_7$ is 6, then $[3]^a = [3]^b$ iff $a \equiv b \pmod 6$. Thus, $[3]^a = [3]^b$, so $\theta_1([a]) = \theta_1([b])$. Hence, θ_1 is well defined, so θ_1 is a function.

Let $[a]_6, [b]_6 \in \mathbb{Z}_6$.

Then

$$\begin{aligned} \theta_1([a]_6 + [b]_6) &= \theta_1([a+b]_6) \\ &= [3]_7^{a+b} \\ &= [3]^a[3]^b \\ &= \theta_1([a]_6)\theta_1([b]_6). \end{aligned}$$

Therefore, θ_1 is a homomorphism.

Suppose $\theta_1([a]) = \theta_1([b])$.

Then $[3]^a = [3]^b$.

Since the order of $[3]_7$ is 6, then $[3]^a = [3]^b$ iff $a \equiv b \pmod 6$.

Thus, $[a] \equiv [b] \pmod 6$.

Since $0 \leq a, b < 6$, then this implies $a = b$.

Therefore, θ_1 is injective.

Suppose $[3]^k$ is an element of $\mathbb{Z}_7^*$.

Then k is an integer, so $[k] \in \mathbb{Z}_6$.

Observe that $\theta_1([k]) = [3]^k$.

Therefore, θ_1 is surjective.

Hence, θ_1 is a bijective homomorphism, so θ_1 is an isomorphism.

We next prove θ_2 is a group isomorphism.

Clearly, θ_2 is a binary relation from $\mathbb{Z}_{10}$ to $\mathbb{Z}_{11}^*$.

Let $[a]_{10}, [b]_{10} \in \mathbb{Z}_{10}$ such that $[a] = [b]$. Then $a \equiv b \pmod{10}$. Since the order of $[2]_{11}$ is 10, then $[2]^a = [2]^b$ iff $a \equiv b \pmod{10}$. Thus, $[2]^a = [2]^b$, so $\theta_2([a]) = \theta_2([b])$. Hence, θ_2 is well defined, so θ_2 is a function.

Let $[a]_{10}, [b]_{10} \in \mathbb{Z}_{10}$.

Then

$$\begin{aligned}\theta_2([a]_{10}+[b]_{10}) &= \theta_2([a+b]_{10}) \\ &= [2]_{11}^{a+b} \\ &= [2]^a[2]^b \\ &= \theta_2([a]_{10})\theta_2([b]_{10}).\end{aligned}$$

Therefore, θ_2 is a homomorphism.

Suppose $\theta_2([a]) = \theta_2([b])$.
Then $[2]^a = [2]^b$.
Since the order of $[2]_{11}$ is 10, then $[2]^a = [2]^b$ iff $a \equiv b \pmod{10}$.
Thus, $a \equiv b \pmod{10}$.
Since $0 \leq a, b < 10$, then this implies $a = b$.
Therefore, θ_2 is injective.

Suppose $[2]^k$ is an element of $\mathbb{Z}_{11}^*$.
Then k is an integer, so $[k] \in \mathbb{Z}_{10}$.
Observe that $\theta_2([k]) = [2]^k$.
Therefore, θ_2 is surjective.
Hence, θ_2 is a bijective homomorphism, so θ_2 is an isomorphism.
Since θ_1 and θ_2 are isomorphisms, then ϕ is an isomorphism. □

Exercise 14. Define $\phi : \mathbb{Z}_{30} \times \mathbb{Z}_2 \to \mathbb{Z}_{10} \times \mathbb{Z}_6$ by $\phi([x],[y]) = ([x],[4x+3y])$.
Prove ϕ is well defined and then prove ϕ is a group isomorphism.

Proof. Let $([a_1],[b_1])$ and $([a_2],[b_2])$ be arbitrary elements of $\mathbb{Z}_{30} \times \mathbb{Z}_2$ such that $([a_1],[b_1]) = ([a_2],[b_2])$.

Then $[a_1]_{30} = [a_2]_{30}$ and $[b_1]_2 = [b_2]_2$.

Since $[a_1]_{30} = [a_2]_{30}$, then $a_1 \equiv a_2 \pmod{30}$, so $30|(a_1 - a_2)$. Hence, there exists an integer k such that $a_1 - a_2 = 30k$. Since $[b_1]_2 = [b_2]_2$, then $b_1 \equiv b_2 \pmod{2}$, so $2|(b_1 - b_2)$. Hence, there exists an integer m such that $b_1 - b_2 = 2m$.

Thus,

$$\begin{aligned}(4a_1+3b_1)-(4a_2+3b_2) &= (4a_1-4a_2)+(3b_1-3b_2) \\ &= 4(a_1-a_2)+3(b_1-b_2) \\ &= 4(30k)+3(2m) \\ &= 120k+6m \\ &= 6(20k+m).\end{aligned}$$

Hence, 6 divides $(4a_1+3b_1)-(4a_2+3b_2)$, so $4a_1+3b_1 \equiv 4a_2+3b_2 \pmod{6}$.

Thus, $[4a_1+3b_1]_6 = [4a_2+3b_2]_6$.

Since $a_1 - a_2 = 30k = 10(3k)$, then 10 divides $a_1 - a_2$. Hence, $a_1 \equiv a_2 \pmod{10}$, so $[a_1]_{10} = [a_2]_{10}$.

Thus, $([a_1]_{10}, [4a_1 + 3b_1]_6) = ([a_2]_{10}, [4a_2 + 3b_2]_6)$. Hence, $\phi([a_1]_{30}, [b_1]_2) = \phi([a_2]_{30}, [b_2]_2)$. Therefore, ϕ is well defined, so ϕ is a function.

Let $([a_1], [b_1])$ and $([a_2], [b_2]])$ be arbitrary elements of $\mathbb{Z}_{30} \times \mathbb{Z}_2$.

Then

$$\begin{aligned}
\phi(([a_1], [b_1]) + ([a_2], [b_2])) &= \phi(([a_1] + [a_2], [b_1] + [b_2])) \\
&= \phi([a_1 + a_2], [b_1 + b_2]) \\
&= ([a_1 + a_2], [4(a_1 + a_2) + 3(b_1 + b_2)]) \\
&= ([a_1 + a_2], [(4a_1 + 3b_1) + (4a_2 + 3b_2)]) \\
&= ([a_1] + [a_2], [4a_1 + 3b_1] + [4a_2 + 3b_2]) \\
&= ([a_1], [4a_1 + 3b_1]) + ([a_2], [4a_2 + 3b_2]) \\
&= \phi([a_1], [b_1]) + \phi([a_2], [b_2]).
\end{aligned}$$

Therefore, ϕ is a homomorphism.

Suppose $\phi([a_1]_{30}, [b_1]_2) = \phi([a_2]_{30}, [b_2]_2)$. Then $([a_1]_{10}, [4a_1+3b_1]_6) = ([a_2]_{10}, [4a_2+3b_2]_6)$. Thus, $[a_1]_{10} = [a_2]_{10}$ and $[4a_1 + 3b_1]_6 = [4a_2 + 3b_2]_6$. Hence, $a_1 \equiv a_2 \pmod{10}$ and $4a_1+3b_1 \equiv 4a_2+3b_2 \pmod{6}$. Thus, $10|a_1-a_2$ and $(4a_1+3b_1)-(4a_2+3b_2) = 6m$ for some integer m. Therefore, $a_1 - a_2 = 10k$ for some integer k and $4(a_1 - a_2) + 3(b_1 - b_2) = 6m$.

Substituting, we obtain $4(10k)+3(b_1-b_2) = 6m$, so $3(b_1-b_2) = 6m-40k = 2(3m-20k)$. Since $3m-20k$ is an integer, then this implies $2|3(b_1-b_2)$. Since $\gcd(2, 3) = 1$, then this implies $2|b_1 - b_2$. Hence, $b_1 - b_2 = 2n$ for some integer n. Thus, we have $4(a_1-a_2)+3(2n) = 6m$, so $4(a_1-a_2) = 6m-6n = 6(m-n)$. Hence, $2(a_1 - a_2) = 3(m - n)$. Since $m - n$ is an integer, then this implies $3|2(a_1 - a_2)$. Since $\gcd(3, 2) = 1$, then $3|a_1 - a_2$.

Since $3|a_1 - a_2$ and $10|a_1-a_2$ and $\gcd(3, 10) = 1$, then $3*10$ divides a_1-a_2. Therefore, $30|a_1 - a_2$, so $a_1 \equiv a_2 \pmod{30}$. Hence, $[a_1]_{30} = [a_2]_{30}$.

Since $2|b_1 - b_2$, then $b_1 \equiv b_2 \pmod{2}$, so $[b_1]_2 = [b_2]_2$.

Thus, $([a_1]_{30}, [b_1]_2) = ([a_2]_{30}, [b_2]_2)$.

Hence, $\phi([a_1]_{30}, [b_1]_2) = \phi([a_2]_{30}, [b_2]_2)$ implies $([a_1]_{30}, [b_1]_2) = ([a_2]_{30}, [b_2]_2)$, so ϕ is injective.

Since $\mathbb{Z}_{30} \times \mathbb{Z}_2$ and $\mathbb{Z}_{10} \times \mathbb{Z}_6$ are finite and $|\mathbb{Z}_{30} \times \mathbb{Z}_2| = 60 = |\mathbb{Z}_{10} \times \mathbb{Z}_6|$ and ϕ is injective, then ϕ is surjective.

Thus, ϕ is a bijective homomorphism, so ϕ is an isomorphism. □

Proof. An alternate proof that ϕ is injective is to prove $\ker(\phi) = \{e\}$.

Since ϕ is a group homomorphism, let $\ker(\phi)$ be the kernel of ϕ.

Suppose $([x], [y]) \in \ker(\phi)$. Then $([x]_{30}, [y]_2) \in \mathbb{Z}_{30} \times \mathbb{Z}_2$ and $\phi([x]_{30}, [y]_2) = ([0]_{10}, [0]_6)$. Thus, $([x]_{10}, [4x + 3y]_6) = ([0]_{10}, [0]_6)$. Hence, $[x]_{10} = [0]_{10}$ and $[4x+3y]_6 = [0]_6$. Thus, $x \equiv 0 \pmod{10}$ and $4x+3y \equiv 0 \pmod{6}$. Hence, $10|x$ and $6|4x + 3y$. Therefore, $x = 10k$ for some integer k and $4x + 3y = 6m$ for some integer m.

Substituting, we obtain $4(10k)+3y = 6m$, so $3y = 6m-40k = 2(3m-20k)$. Since $3m - 20k$ is an integer, then this implies $2|3y$. Since $\gcd(2, 3) = 1$, then $2|y$. Hence, $y = 2n$ for some integer n.

Substituting, we obtain $4x + 3(2n) = 6m$, so $4x = 6m - 6n = 6(m - n)$. Thus, $2x = 3(m - n)$. Since $m - n$ is an integer, then $3|2x$. Since $\gcd(3, 2) = 1$, then $3|x$.

Since $3|x$ and $10|x$ and $\gcd(3, 10) = 1$, then this implies $3 * 10$ divides x. Hence, $30|x$, so $x \equiv 0 \pmod{30}$. Therefore, $[x]_{30} = [0]_{30}$.

Since $2|y$, then $y \equiv 0 \pmod 2$, so $[y]_2 = [0]_2$. Thus, $([x]_{30}, [y]_2) = ([0]_{30}, [0]_2)$.

Hence, $([x], [y]) \in \ker(\phi)$ implies $([x], [y]) \in \{([0]_{30}, [0]_2)\}$, so $\ker(\phi) \subset \{([0]_{30}, [0]_2)\}$. Since ϕ is a group homomorphism, then $([0]_{30}, [0]_2) \in \ker(\phi)$, so $\{([0]_{30}, [0]_2)\} \subset \ker(\phi)$.

Therefore, $\ker(\phi) \subset \{([0]_{30}, [0]_2)\}$ and $\{([0]_{30}, [0]_2)\} \subset \ker(\phi)$, so $\ker(\phi) = \{([0]_{30}, [0]_2)\}$. Since $\ker(\phi) = \{([0]_{30}, [0]_2)\}$ iff ϕ is injective, then ϕ is injective. □

Exercise 15. Let $(\mathbb{Z}, +)$ the additive group of integers.

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = -n$ for all $n \in \mathbb{Z}$ is an automorphism.

Proof. Let $a, b \in \mathbb{Z}$ such that $f(a) = f(b)$.

Then $-a = f(a) = f(b) = -b$, so $-a = -b$.

Therefore, $a = b$, so f is injective.

Let $n \in \mathbb{Z}$.

Then $-n \in \mathbb{Z}$ and $f(-n) = -(-n) = n$.

Since $-n \in \mathbb{Z}$ and $f(-n) = n$, then f is surjective.

Since f is injective and surjective, then f is bijective.

Let $r, s \in \mathbb{Z}$.

Then $f(r + s) = -(r + s) = -r - s = f(r) - s = f(r) + (-s) = f(r) + f(s)$, so f is a homomorphism.

Since f is bijective and f is a homomorphism, then f is an isomorphism.

Therefore, $f : \mathbb{Z} \to \mathbb{Z}$ is an automorphism. □

Exercise 16. The map $(a, b) \to (b, a)$ on the group $(\mathbb{R}^2, +)$ is an automorphism.

Proof. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be defined by $f(a, b) = (b, a)$ for all $(a, b) \in \mathbb{R}^2$.

Let $(a, b) \in \mathbb{R}^2$ and $(c, d) \in \mathbb{R}^2$ such that $f(a, b) = f(c, d)$.

Then $(b, a) = f(a, b) = f(c, d) = (d, c)$, so $b = d$ and $a = c$.

Therefore, $(a, b) = (c, d)$, so f is injective.

Let $(x, y) \in \mathbb{R}^2$.

Then $x \in \mathbb{R}$ and $y \in \mathbb{R}$, so $(y, x) \in \mathbb{R}^2$ and $f(y, x) = (x, y)$.

Since there is some $(y, x) \in \mathbb{R}^2$ such that $f(y, x) = (x, y)$, then f is surjective.

Since f is injective and surjective, then f is bijective.

Let $(a,b) \in \mathbb{R}^2$ and $(c,d) \in \mathbb{R}^2$.

Observe that

$$\begin{aligned} f((a,b)+(c,d)) &= f(a+c, b+d) \\ &= (b+d, a+c) \\ &= (b,a)+(d,c) \\ &= f(a,b)+f(c,d). \end{aligned}$$

Therefore, f is a homomorphism.

Since f is bijective and f is a homomorphism, then f is an isomorphism, so $f : \mathbb{R}^2 \to \mathbb{R}^2$ is an automorphism. □

Exercise 17. $A \mapsto BAB^{-1}$ is an automorphism of $SL_2(\mathbb{R})$ for all $B \in GL_2(\mathbb{R})$.

Solution. Let B be an arbitrary element of $GL_2(\mathbb{R})$.

Let $\phi : SL_2(\mathbb{R}) \to SL_2(\mathbb{R})$ be defined by $\phi(A) = BAB^{-1}$ for all $A \in SL_2(\mathbb{R})$.

To prove ϕ is an automorphism of $SL_2(\mathbb{R})$, we must prove ϕ is an isomorphism.

Thus, we must prove:

1. ϕ is a bijective.

2. ϕ is a homomorphism. □

Proof. Let B be an arbitrary element of $GL_2(\mathbb{R})$.

Let $\phi : SL_2(\mathbb{R}) \to SL_2(\mathbb{R})$ be defined by $\phi(A) = BAB^{-1}$ for all $A \in SL_2(\mathbb{R})$.

Let $A \in SL_2(\mathbb{R})$.

Then $A \in GL_2(\mathbb{R})$ and $\det(A) = 1$ and $\phi(A) = BAB^{-1}$.

Since matrix multiplication is a binary operation on $GL_2(\mathbb{R})$, then $BAB^{-1} \in GL_2(\mathbb{R})$ and is unique.

Observe that

$$\begin{aligned} \det(BAB^{-1}) &= \det(B)\det(A)\det(B^{-1}) \\ &= \det(B) * 1 * \det(B^{-1}) \\ &= \det(B) * \det(B^{-1}) \\ &= \det(BB^{-1}) \\ &= \det(I) \\ &= 1. \end{aligned}$$

Since $BAB^{-1} \in GL_2(\mathbb{R})$ and $\det(BAB^{-1}) = 1$, then $BAB^{-1} \in SL_2(\mathbb{R})$.

Since $BAB^{-1} \in SL_2(\mathbb{R})$ and is unique, then ϕ is a function.

Let $X, Y \in SL_2(\mathbb{R})$.

Then

$$\begin{aligned}\phi(XY) &= B(XY)B^{-1}\\ &= (BX)(YB^{-1})\\ &= (BX)(B^{-1}B)(YB^{-1})\\ &= (BXB^{-1})(BYB^{-1})\\ &= \phi(X)\phi(Y).\end{aligned}$$

Thus, ϕ is a homomorphism.

Suppose $\phi(X) = \phi(Y)$.
Then $BXB^{-1} = BYB^{-1}$.
By the right cancellation law, we have $BX = BY$.
By the left cancellation law, we have $X = Y$.
Therefore, $\phi(X) = \phi(Y)$ implies $X = Y$, so ϕ is injective.

Let Y be an arbitrary element of $SL_2(\mathbb{R})$.
Then $Y \in GL_2(\mathbb{R})$ and $\det(Y) = 1$.
Let $X = B^{-1}YB$.
By closure of $GL_2(\mathbb{R})$, $X \in GL_2(\mathbb{R})$.
Observe that

$$\begin{aligned}\det(X) &= \det(B^{-1}YB)\\ &= \det(B^{-1})\det(Y)\det(B)\\ &= \det(B^{-1}) * 1 * \det(B)\\ &= \det(B^{-1})\det(B)\\ &= \det(B^{-1}B)\\ &= \det(I)\\ &= 1.\end{aligned}$$

Since $X \in GL_2(\mathbb{R})$ and $\det(X) = 1$, then $X \in SL_2(\mathbb{R})$
Observe that

$$\begin{aligned}\phi(X) &= \phi(B^{-1}YB)\\ &= B(B^{-1}YB)B^{-1}\\ &= (BB^{-1})Y(BB^{-1})\\ &= Y.\end{aligned}$$

Thus, there exists $X \in SL_2(\mathbb{R})$ such that $\phi(X) = Y$.
Hence, ϕ is surjective.

Thus, ϕ is a bijective homomorphism, so $\phi : SL_2(\mathbb{R}) \to SL_2(\mathbb{R})$ is an isomorphism.

Therefore, ϕ is an automorphism of $SL_2(\mathbb{R})$. □

Exercise 18. Let α be a fixed element of S_n.

Let $\phi_\alpha : S_n \to S_n$ be defined by $\phi_\alpha(\sigma) = \alpha\sigma\alpha^{-1}$ for all $\sigma \in S_n$.

Then ϕ is an automorphism of S_n.

Proof. Clearly, ϕ_α is a function.

Let $\sigma, \tau \in S_n$ such that $\phi_\alpha(\sigma) = \phi_\alpha(\tau)$.

Then $\alpha\sigma\alpha^{-1} = \alpha\tau\alpha^{-1}$.

By left cancellation law, $\sigma\alpha^{-1} = \tau\alpha^{-1}$.

By right cancellation law, $\sigma = \tau$.

Hence, $\phi_\alpha(\sigma) = \phi_\alpha(\tau)$ implies $\sigma = \tau$, so ϕ_α is injective.

Let $\gamma \in S_n$.

Let $\sigma = \alpha^{-1}\gamma\alpha$.

Then by closure of $S_n, \sigma \in S_n$.

Observe that

$$\begin{aligned}\phi_\alpha(\sigma) &= \alpha\sigma\alpha^{-1} \\ &= \alpha(\alpha^{-1}\gamma\alpha)\alpha^{-1} \\ &= (\alpha\alpha^{-1})\gamma(\alpha\alpha^{-1}) \\ &= \gamma.\end{aligned}$$

Hence, there exists $\sigma \in S_n$ such that $\phi_\alpha(\sigma) = \gamma$, so ϕ_α is surjective.

Thus, ϕ_α is bijective.

Let $\sigma, \tau \in S_n$.

Observe that

$$\begin{aligned}\phi_\alpha(\sigma\tau) &= \alpha(\sigma\tau)\alpha^{-1} \\ &= (\alpha\sigma)(\tau\alpha^{-1}) \\ &= (\alpha\sigma)(\alpha^{-1}\alpha)(\tau\alpha^{-1}) \\ &= (\alpha\sigma\alpha^{-1})(\alpha\tau\alpha^{-1}) \\ &= \phi_\alpha(\sigma)\phi_\alpha(\tau).\end{aligned}$$

Hence, ϕ_α is a homomorphism.

Thus, ϕ_α is a bijective homomorphism, so ϕ_α is an isomorphism.

Hence, ϕ_α is an automorphism of S_n. □

Exercise 19. Let $\phi : \mathbb{Z}_{17^*} \to \mathbb{Z}_{17^*}$ be defined by $\phi(x) = x^{-1}$.

Then ϕ is an automorphism of $\mathbb{Z}_{17^*}$.

Proof. Since $\mathbb{Z}_{17^*}$ is an abelian group, then ϕ is a group homomorphism.

Observe that $\phi(\phi(x)) = \phi(x^{-1}) = (x^{-1})^{-1} = x$ for all $x \in \mathbb{Z}_{17^*}$.

Thus, $\phi\phi = id$, where id is the identity function.

Hence, $\phi^{-1} = \phi$, so ϕ is bijective.

Therefore, ϕ is a bijective homomorphism, so $\phi : \mathbb{Z}_{17^*} \to \mathbb{Z}_{17^*}$ is an isomorphism.

Thus, ϕ is an automorphism of $\mathbb{Z}_{17^*}$. □

Direct Products

Exercise 20. Show that $\mathbb{Z}_5 \times \mathbb{Z}_3$ is a cyclic group and list all of its generators.

Solution. A direct product of groups is a group. Since $\mathbb{Z}_5$ and $\mathbb{Z}_3$ are groups, then $\mathbb{Z}_5 \times \mathbb{Z}_3$ is a group. The order of $\mathbb{Z}_5 \times \mathbb{Z}_3$ is $|\mathbb{Z}_5 \times \mathbb{Z}_3| = |\mathbb{Z}_5| * |\mathbb{Z}_3| = 5 * 3 = 15$. Since $\gcd(5, 3) = 1$ and $\mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$ iff $\gcd(5, 3) = 1$, then $\mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$. Hence, $\mathbb{Z}_5 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_{15}$. Since $\mathbb{Z}_{15}$ is a cyclic group and isomorphisms preserve cyclic property of groups, then $\mathbb{Z}_5 \times \mathbb{Z}_3$ is cyclic. Hence, $\mathbb{Z}_5 \times \mathbb{Z}_3$ has at least one generator.

Let $(a, b) \in \mathbb{Z}_5 \times \mathbb{Z}_3$ be a generator of $\mathbb{Z}_5 \times \mathbb{Z}_3$. Then $a \in \mathbb{Z}_5$ and $b \in \mathbb{Z}_3$ and $15 = |(a, b)| = lcm(|a|, |b|)$. Since $\mathbb{Z}_5$ is a group of prime order, then any non identity element of $\mathbb{Z}_5$ is a generator of $\mathbb{Z}_5$ and has order 5. Thus, $a \in \{1, 2, 3, 4\}$.

Since $\mathbb{Z}_3$ is a group of prime order, then any non identity element of $\mathbb{Z}_3$ is a generator of $\mathbb{Z}_3$ and has order 3.

Thus, $b \in \{1, 2\}$.

Therefore, the generators of $\mathbb{Z}_5 \times \mathbb{Z}_3$ are :

$\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2), (4, 1), (4, 2)\}$.

Hence, there are $4 * 2 = 8$ generators of $\mathbb{Z}_5 \times \mathbb{Z}_3$. □