Introduction to Abstract Algebra I: Homework 3

Due on October 22, 2025 at 23:59

Victor Ostrik

Hashem A. Damrah
UO ID: 952102243

Exercise 2.44. Prove that if $f : G_1 \to G_2$ is a group isomorphism from the group $\langle G_1, *_1 \rangle$ to the group $\langle G_2, *_2 \rangle$, then $f^{-1} : G_2 \to G_1$ is a group isomorphism from $\langle G_2, *_2 \rangle$ to $\langle G_1, *_1 \rangle$.

Solution. Given two groups $\langle G_1, *_1 \rangle$ and $\langle G_2, *_2 \rangle$, assume we have an isomorphism $f : G_1 \to G_2$. By definition of isomorphism, f is a bijection and satisfies the homomorphism property, i.e., for every $a, b \in G_1$, we have

$$f(a *_1 b) = f(a) *_2 f(b).$$

Since f is a bijection, it has an inverse function $f^{-1} : G_2 \to G_1$. We need to show that f^{-1} is also a homomorphism. For any $x, y \in G_2$, let $a = f^{-1}(x)$ and $b = f^{-1}(y)$. Then we have

$$f^{-1}(x *_2 y) = f^{-1}(f(a) *_2 f(b)) = f^{-1}(f(a *_1 b)) = a *_1 b = f^{-1}(x) *_1 f^{-1}(y).$$

Thus, f^{-1} satisfies the homomorphism property. Since f^{-1} is also a bijection, we conclude that f^{-1} is an isomorphism from $\langle G_2, *_2 \rangle$ to $\langle G_1, *_1 \rangle$. □

Exercise 3.30. Find *all* solutions x of the given equation: $x +_{2\pi} \pi = \pi/2$ in $\mathbb{R}_{2\pi}$.

Solution. Re-writing the equation, we have $x + \pi \equiv \pi/2 \pmod{2\pi}$. Subtracting π from both sides, we have $x \equiv \pi/2 - \pi$, which simplifies to $x \equiv -\pi/2$. Since we are working in $\mathbb{R}_{2\pi}$, we can add 2π to $-\pi/2$ to find the equivalent positive solution. Thus, we have

$$x \equiv -\pi/2 + 2\pi \pmod{2\pi} \Rightarrow x \equiv 3\pi/2 \pmod{2\pi}.$$

Therefore, the only solution to the equation $x +_{2\pi} \pi = \pi/2$ in $\mathbb{R}_{2\pi}$ is $3\pi/2$. □

Exercise 3.32. Find *all* solutions x of the given equation: $x +_{13} x +_{13} x = 5$ in $\mathbb{Z}_{13}$.

Solution. Re-writing the equation, we have $3x \equiv 5 \pmod{13}$. To solve for x, we need to find the multiplicative inverse of 3 module 13, which is 9, since $3 \times 9 = 27$ and $27 \equiv 1 \pmod{13}$. Multiplying both sides of the equation by 9, we get

$$9 \cdot 3x \equiv 9 \cdot 5 \pmod{13} \Rightarrow x \equiv 45 \pmod{13}.$$

Reducing 45 modulo 13, we find $45 \equiv 6 \pmod{13}$. Therefore, the only solution to the equation $x +_{13} x +_{13} x = 5$ in $\mathbb{Z}_{13}$ is $x \equiv 6$. □

Exercise 3.35. Prove or give a counterexample to the statement that for any $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}_n$, the equation $x +_n x = a$ has at most two solutions in $\mathbb{Z}_n$.

Solution. By definition of $x +_n x$, we have

$$x +_n x = \begin{cases} 2x, & \text{if } 0 \leq 2x < n \\ 2x - n, & \text{if } n \leq 2x \geq n \end{cases}.$$

We will consider two cases based on the value of a.

If $0 \leq a < n/2$, then in this case, we have $2x \equiv a \pmod{n}$. Since $0 \leq a < n/2$, we can solve for x as follows:

$$2x = a + kn \Rightarrow x = \frac{a + kn}{2}.$$

For $k = 0$, we have $x = a/2$. For $k = 1$, we have $x = (a + n)/2$. Since $a < n/2$, we have $(a + n)/2 < n$. Thus, both $a/2$ and $(a + n)/2$ are valid solutions in $\mathbb{Z}_n$. □

Exercise 3.38. There is an isomorphism of U_7 with $\mathbb{Z}_7$ in which $\zeta = e^{i(2\pi/7)} \leftrightarrow 4$. Find the element in $\mathbb{Z}_7$ to which ζ^m must correspond for $m = 0, 2, 3, 4, 5$ and 6.

Solution. Let $f : U_7 \to \mathbb{Z}_7$ be an isomorphism such that $f(\zeta) = 4$, where $\zeta = e^{i(2\pi/7)}$. Since f is a group isomorphism, it preserves the group operation. The operation in U_7 is multiplication, while in $\mathbb{Z}_7$ it is addition modulo 7. Therefore, for any integer m, we have

$$f(\zeta^m) = f(\underbrace{\zeta \cdot \zeta \cdots \zeta}_{m \text{ times}}) = \underbrace{f(\zeta) +_7 f(\zeta) +_7 \cdots +_7 f(\zeta)}_{m \text{ times}} \equiv 4m \pmod 7.$$

Because isomorphisms map identity to identity, we also have $f(\zeta^0) = f(1) = 0$. We can now compute $f(\zeta^m)$ for each given value of m:

$$\begin{aligned}
f(\zeta^0) &= 4(0) \equiv 0 \pmod 7 \\
f(\zeta^2) &= 4(2) \equiv 8 \equiv 1 \pmod 7 \\
f(\zeta^3) &= 4(3) \equiv 12 \equiv 5 \pmod 7 \\
f(\zeta^4) &= 4(4) \equiv 16 \equiv 2 \pmod 7 \\
f(\zeta^5) &= 4(5) \equiv 20 \equiv 6 \pmod 7 \\
f(\zeta^6) &= 4(6) \equiv 24 \equiv 3 \pmod 7.
\end{aligned}$$

Hence, under this isomorphism,

ζ^m	$1 = \zeta^0$	ζ	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6
$f(\zeta^m)$	0	4	1	5	2	6	3

Therefore, each power of ζ corresponds to a unique element of $\mathbb{Z}_7$ given by $f(\zeta^m) \equiv 4m \pmod 7$. □

Exercise 4.10. Convert the permutations σ, τ, and μ defined prior to Exercise 1 to disjoint cycle notation.

Solution. We have the following permutations defined in two-line notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}, \qquad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}.$$

Tracking the orbits for σ, we find $1 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 6 \mapsto 2 \mapsto 1$. Thus, in disjoint cycle notation, we have $\sigma = (1\,3\,4\,5\,6\,2)$. For τ, tracking the orbits, we find $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$ and $5 \mapsto 6 \mapsto 5$. Thus, in disjoint cycle notation, we have $\tau = (1\,2\,4\,3)(5\,6)$. For μ, tracking the orbits, we find $1 \mapsto 5 \mapsto 1$, $3 \mapsto 4 \mapsto 3$, and 2 and 6 are fixed points. Thus, in disjoint cycle notation, we have $\mu = (1\,5)(3\,4)$. Therefore, the permutations in disjoint cycle notation are

$$\sigma = (1\,3\,4\,5\,6\,2), \quad \tau = (1\,2\,4\,3)(5\,6), \quad \mu = (1\,5)(3\,4).$$ □

Exercise 4.12. Compute the permutation products.

(i) $(1, 5, 2, 4)(1, 5, 2, 3)$.

(ii) $(1, 5, 3)(1, 2, 3, 4, 5, 6)(1, 5, 3)^{-1}$.

(iii) $[(1, 6, 7, 2)^2(4, 5, 2, 6)^{-1}(1, 7, 3)]^{-1}$.

(iv) $(1, 6)(1, 5)(1, 4)(1, 3)(1, 2)$.

Solution to (i). Let $\alpha = (1\,5\,2\,4)$ and $\beta = (1\,5\,2\,3)$. Computing $\alpha\beta$ on the points $1, \cdots, 5$, we get

$$\alpha\beta(1) = \alpha(\beta(1)) = \alpha(5) = 2$$

$$\alpha\beta(2) = \alpha(\beta(2)) = \alpha(3) = 3$$
$$\alpha\beta(3) = \alpha(\beta(3)) = \alpha(1) = 5$$
$$\alpha\beta(5) = \alpha(\beta(5)) = \alpha(2) = 4$$
$$\alpha\beta(4) = \alpha(\beta(4)) = \alpha(4) = 1.$$

Tracing the orbit of 1 yields $1 \mapsto 2 \mapsto 3 \mapsto 5 \mapsto 4 \mapsto 1$, so in disjoint cycle notation $\alpha\beta = (1\,2\,3\,5\,4)$. □

Solution to (ii). Let $\alpha = (1\,5\,3)$ and $\beta = (1\,2\,3\,4\,5\,6)$. Computing $\delta := \alpha\beta\alpha^{-1}$ on the points $1, \cdots, 6$, we get

$$\delta(1) = \alpha(\beta(\alpha^{-1}(1))) = \alpha(\beta(3)) = \alpha(4) = 4$$
$$\delta(2) = \alpha(\beta(\alpha^{-1}(2))) = \alpha(\beta(2)) = \alpha(3) = 1$$
$$\delta(3) = \alpha(\beta(\alpha^{-1}(3))) = \alpha(\beta(5)) = \alpha(6) = 6$$
$$\delta(4) = \alpha(\beta(\alpha^{-1}(4))) = \alpha(\beta(4)) = \alpha(5) = 3$$
$$\delta(5) = \alpha(\beta(\alpha^{-1}(5))) = \alpha(\beta(1)) = \alpha(2) = 2$$
$$\delta(6) = \alpha(\beta(\alpha^{-1}(6))) = \alpha(\beta(6)) = \alpha(1) = 5.$$

Tracing the orbit of 1, we find $1 \mapsto 4 \mapsto 3 \mapsto 6 \mapsto 5 \mapsto 2$. Thus, in disjoint cycle notation, we have $\alpha\beta\alpha^{-1} = (1\,4\,3\,6\,5\,2)$. □

Solution to (iii). Let $\alpha = (1\,6\,7\,2)$, $\beta = (4\,5\,2\,6)$, and $\gamma = (1\,7\,3)$. Then $\alpha^2 = (1\,7)(6\,2)$ and $\beta^{-1} = (6\,2\,5\,4)$. Computing $\delta := \alpha^2\beta^{-1}\gamma$ on the points $1, \cdots, 7$, we get

$$\delta(1) = \alpha^2(\beta^{-1}(\gamma(1))) = \alpha^2(\beta^{-1}(7)) = \alpha^2(7) = 1$$
$$\delta(2) = \alpha^2(\beta^{-1}(\gamma(2))) = \alpha^2(\beta^{-1}(2)) = \alpha^2(5) = 5$$
$$\delta(3) = \alpha^2(\beta^{-1}(\gamma(3))) = \alpha^2(\beta^{-1}(1)) = \alpha^2(1) = 7$$
$$\delta(4) = \alpha^2(\beta^{-1}(\gamma(4))) = \alpha^2(\beta^{-1}(4)) = \alpha^2(6) = 2$$
$$\delta(5) = \alpha^2(\beta^{-1}(\gamma(5))) = \alpha^2(\beta^{-1}(5)) = \alpha^2(4) = 4$$
$$\delta(6) = \alpha^2(\beta^{-1}(\gamma(6))) = \alpha^2(\beta^{-1}(6)) = \alpha^2(2) = 6$$
$$\delta(7) = \alpha^2(\beta^{-1}(\gamma(7))) = \alpha^2(\beta^{-1}(3)) = \alpha^2(3) = 3.$$

Thus the nontrivial orbits are $2 \mapsto 5 \mapsto 4 \mapsto 2$ and $3 \mapsto 7 \mapsto 3$, and 1 and 6 are fixed points. Hence, we have

$$\delta = (2\,5\,4)(3\,7).$$

Taking inverses (reverse each cycle), we get $\delta^{-1} = (4\,5\,2)(7\,3)$. □

Solution to (iv). Let $\alpha = (1\,6)$, $\beta = (1\,5)$, $\gamma = (1\,4)$, $\delta = (1\,3)$, and $\varepsilon = (1\,2)$. Computing the product $\zeta := \alpha\beta\gamma\delta\varepsilon$ on the points $1, \cdots, 6$, we get

$$\zeta(1) = \alpha(\beta(\gamma(\delta(\varepsilon(1))))) = \alpha(\beta(\gamma(\delta(2)))) = \alpha(\beta(\gamma(2))) = \alpha(\beta(2)) = \alpha(2) = 2$$
$$\zeta(2) = \alpha(\beta(\gamma(\delta(\varepsilon(2))))) = \alpha(\beta(\gamma(\delta(1)))) = \alpha(\beta(\gamma(3))) = \alpha(\beta(3)) = \alpha(3) = 3$$
$$\zeta(3) = \alpha(\beta(\gamma(\delta(\varepsilon(3))))) = \alpha(\beta(\gamma(\delta(3)))) = \alpha(\beta(\gamma(1))) = \alpha(\beta(4)) = \alpha(4) = 4$$
$$\zeta(4) = \alpha(\beta(\gamma(\delta(\varepsilon(4))))) = \alpha(\beta(\gamma(\delta(4)))) = \alpha(\beta(\gamma(4))) = \alpha(\beta(1)) = \alpha(5) = 5$$
$$\zeta(5) = \alpha(\beta(\gamma(\delta(\varepsilon(5))))) = \alpha(\beta(\gamma(\delta(5)))) = \alpha(\beta(\gamma(5))) = \alpha(\beta(5)) = \alpha(1) = 6$$
$$\zeta(6) = \alpha(\beta(\gamma(\delta(\varepsilon(6))))) = \alpha(\beta(\gamma(\delta(6)))) = \alpha(\beta(\gamma(6))) = \alpha(\beta(6)) = \alpha(6) = 1.$$

Thus, tracing the orbit of 1, we find $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 6 \mapsto 1$. Hence, we have $\zeta = (1\,2\,3\,4\,5\,6)$. □

Exercise 4.14. Write the group table for D_3. Compare the group tables for D_3 and S_3. Are the groups isomorphic?

Solution. Writing out the group table for D_3, we have

D_3	e	r	r^2	s	sr	sr^2
e	e	r	r^2	s	sr	sr^2
r	r	r^2	rr^2	rs	$r(sr)$	$r(sr^2)$
r^2	r^2	r^2r	r^2r^2	r^2s	$r^2(sr)$	$r^2(sr^2)$
s	s	sr	sr^2	ss	$s(sr)$	$s(sr^2)$
sr	sr	$(sr)r$	$(sr)r^2$	$(sr)s$	$(sr)(sr)$	$(sr)(sr^2)$
sr^2	sr^2	$(sr^2)r$	$(sr^2)r^2$	$(sr^2)s$	$(sr^2)(sr)$	$(sr^2)(sr^2)$

Since $D_n = \langle r, s \mid r^n = e = s^2 \text{ and } rs = sr^{n-1} \rangle$, we can fill in the rest of the table using these relations.

Firstly, let's show, with induction that $r^m s = sr^{n-m}$ for all integers $0 \leq m \leq n$. For the base case, when $m = 0$, we have $r^0 s = s = sr^n$ since $r^n = e$. Now, assume that for some k with $0 \leq k < n$, we have $r^k s = sr^{n-k}$. Then, for $m = k + 1$, we have

$$r^{k+1}s = r(r^k s) = r(sr^{n-k}) = (rs)r^{n-k}.$$

Using the relation $rs = sr^{n-1}$, we get

$$(rs)r^{n-k} = (sr^{n-1})r^{n-k} = sr^{(n-1)+(n-k)} = sr^{2n-(k+1)} \equiv sr^{n-(k+1)} \pmod{n}.$$

Thus, by induction, we have $r^m s = sr^{n-m}$ for all integers $0 \leq m \leq n$.

Now, using that relation, we can simplify the entries in the group table. Notice that $rr^2 = e = r^2 r$ and $ss = e = s^2$. Also, $(sr)(sr) = s(rs)r = ssr^2 r = ee = e$. A similar computation shows that $(sr^2)(sr^2) = e$. Continuing, we have $(sr)(sr^2) = s(rs)r^2 = ssr^2 r^2 = r$ and $(sr^2)(sr) = s(r^2 s)r = ssrr = r^2$. For $(sr^2)s = s(r^2 s) = ssr = r$. Similarly, $(sr)s = s(rs) = ssr^2 = r^2$ and $(sr^2)s = s(r^2 s) = ssr = r$. Finally, $r(sr) = (rs)r = (sr^2)r = s = s$ and $r(sr^2) = (rs)r^2 = (sr^2)r^2 = sr^4 = sr$.

Filling in these values, we get the completed group table for D_3:

D_3	e	r	r^2	s	sr	sr^2
e	e	r	r^2	s	sr	sr^2
r	r	r^2	e	sr^2	s	sr
r^2	r^2	e	r	$r^2 s$	sr^2	s
s	s	sr	sr^2	e	r	r^2
sr	sr	sr^2	s	r^2	e	r
sr^2	sr^2	s	sr	r	r^2	e

The symmetric group S_3 has elements, namely, e, (1 2), (1 3), (2 3), (1 2 3), and (1 3 2) Define a map $\varphi : D_3 \to S_3$ by

$$\varphi(e) = e, \quad \varphi(r) = (1\ 2\ 3), \quad \varphi(r^2) = (1\ 3\ 2)$$
$$\varphi(s) = (2\ 3), \quad \varphi(sr) = (1\ 3), \quad \varphi(sr^2) = (1\ 2).$$

Clearly, φ is a bijection between the elements of D_3 and S_3 (both groups have six elements and φ is injective on generators). To show that φ is a homomorphism, we need to verify that $\varphi(xy) = \varphi(x)\varphi(y)$ for all

$x, y \in D_3$. This can be checked by comparing the group tables of D_3 and S_3. For example, consider the product $r \cdot s$ in D_3. From the group table, we have $r \cdot s = sr^2$. Applying φ, we get

$$\varphi(r \cdot s) = \varphi(sr) = (1\ 3).$$

On the other hand, we have

$$\varphi(r) \cdot \varphi(s) = (1\ 2\ 3) \cdot (2\ 3) = (1\ 3).$$

Since $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$, the homomorphism property holds for this pair. Similar checks can be performed for all other pairs of elements in D_3. Since φ is a bijection and satisfies the homomorphism property, it is an isomorphism. Therefore, $D_3 \cong S_3$. □

Exercise 4.32. Strengthening Exercise 31, show that if $n \geq 3$, then the only element of σ of S_n satisfying $\sigma\gamma = \gamma\sigma$ for all $y \in S_n$ is $\sigma = \iota$, the identity permutation.

Solution. Suppose, for contradiction, that $\sigma \in S_n$ commutes with every $\gamma \in S_n$ but $\sigma \neq \iota$. Then there exists at least one element $a \in \{1, \ldots, n\}$ with $\sigma(a) \neq a$. Set $b := \sigma(a)$. Since $n \geq 3$ we can choose $c \in \{1, \ldots, n\}$ distinct from both a and b. Let $\tau = (bc)$ be the transposition swapping b and c (and fixing all other points). By hypothesis σ commutes with τ, so $\sigma\tau = \tau\sigma$. Apply both sides to the element a. Because $a \neq b, c$ we have $\tau(a) = a$, hence $(\sigma tau)(a) = \sigma(\tau(a)) = \sigma(a) = b$. On the other hand, $(\tau sigma)(a) = \tau(\sigma(a)) = \tau(b) = c$. Thus $b = (\sigma\tau)(a) = (\tau\sigma)(a) = c$, contradicting the choice $b \neq c$.

This contradiction shows our assumption $\sigma \neq \iota$ was false. Therefore the only permutation that commutes with every element of S_n is the identity ι. □

Exercise 4.36. Prove that for any integer $n \geq 2$, there are at least two non-isomorphic groups with exactly $2n$ elements.

Solution. Let $C_{2n} = \langle x \mid x^{2n} = e \rangle$ be the cyclic group generated by x. Clearly $|C_{2n}| = 2n$, and C_{2n} contains an element (namely x) of order $2n$.

Let $D_n = \langle r, s \mid r^n = e = s^2, rs = sr^{n-1} \rangle$ be the dihedral group of the regular n-gon. Clearly, $|D_n| = 2n$. The elements split into two types: the powers r^k (the rotations) each have order dividing n and the elements sr^k (the reflections) each have order 2.

In particular no element of D_n can have order $2n$ (since every element has order $\leq n$ or equal to 2).

Suppose, for contradiction, there were an isomorphism $\varphi: C_{2n} \to D_n$. An isomorphism preserves element orders, so D_n would contain an element of order $2n$ (the image of the generator of C_{2n}), contradicting the fact that every element of D_n has order dividing n or equal to 2. Hence no such isomorphism exists.

Therefore C_{2n} and D_n are two groups of order $2n$ which are not isomorphic. □