MATH 343 · Group Theory

Chapter 6 Assigned Problems

Exercises 2, 4, 6, 7, 8, 12, 17, 31, and 41

Solutions based on Gallian, Contemporary Abstract Algebra, 10th edition

Exercise 2: Question

Question

Find $\mathrm{Aut}(\mathbb{Z})$ and $\mathrm{Aut}(\mathbb{Z}_6)$.

Aut(G) is the set of all automorphisms of G: the isomorphisms from G onto itself.

Exercise 2: Solution (1 of 3)

Aut(ℤ): first find what an automorphism of ℤ must look like.

An automorphism of ℤ is fixed by α(1)

Let α ∈ Aut(ℤ) and put m = α(1). Every integer k is k · 1, so by Theorem 6.1(2), written additively,

$$\alpha(k) = k\,\alpha(1) = km \qquad \text{for all } k \in \mathbb{Z}$$

Only m = 1 and m = −1 are possible

α is onto, so 1 = α(k) = km for some integer k. A product of two integers equals 1 only when both are 1 or both are −1. So m = 1 or m = −1, and α is one of

$$\alpha_1(x) = x \qquad \text{or} \qquad \alpha_{-1}(x) = -x$$

Equivalently: an automorphism carries the generator 1 to a generator (Theorem 6.1(4)), and the generators of ℤ are 1 and −1.

Exercise 2: Solution (2 of 3)

Both candidates are automorphisms of $\mathbb{Z}$.

α_1 is the identity map, which is an automorphism. For the other candidate, define

$$\alpha_{-1}: \mathbb{Z} \to \mathbb{Z}, \qquad \alpha_{-1}(x) = -x$$

Step 1 (well defined) $\quad$ for each $x \in \mathbb{Z}$, $-x$ is one integer

Step 2 (one-to-one) $\quad -x = -y \Rightarrow x = y$

Step 3 (onto) $\quad y \in \mathbb{Z}$: $\alpha_{-1}(-y) = y$

Step 4 (operation-preserving) $\quad \alpha_{-1}(x+y) = -(x+y) = (-x) + (-y) = \alpha_{-1}(x) + \alpha_{-1}(y)$

Aut($\mathbb{Z}$) = {α_1, α_{-1}}: a group with two elements.

Exercise 2: Solution (3 of 3)

Aut($\mathbb{Z}_6$): the same idea in a finite cyclic group.

For $\alpha \in \mathrm{Aut}(\mathbb{Z}_6)$, $\alpha(k) = k\alpha(1) \bmod 6$ as before, and $\alpha(1)$ must have order $|1| = 6$ (Theorem 6.1(5)): $\alpha(1) = 1$ or $\alpha(1) = 5$. So

$$\alpha_1(x) = x \qquad \text{or} \qquad \alpha_5(x) = 5x \bmod 6$$

x	0	1	2	3	4	5
$\alpha_5(x)$	0	5	4	3	2	1

α_5 is an automorphism

Since $5 \cdot 5 = 25 \equiv 1 \pmod 6$, $\alpha_5(\alpha_5(x)) = x$: α_5 undoes itself, so it is one-to-one and onto. It also preserves addition in $\mathbb{Z}_6$:

$$\alpha_5(x + y) = 5(x + y) \bmod 6 = \alpha_5(x) + \alpha_5(y)$$

Aut($\mathbb{Z}_6$) = {α_1, α_5}, again a group with two elements.

Exercise 4: Question

Question

Show that U(8) is not isomorphic to U(10).

Show that U(8) is isomorphic to U(12).

Exercise 4: Solution (1 of 3)

U(8) ≇ U(10): both have four elements, so compare the orders of their elements.

x in U(8)	1	3	5	7
|x|	1	2	2	2

$$3^2 = 9 \equiv 1, \qquad 5^2 = 25 \equiv 1, \qquad 7^2 = 49 \equiv 1 \pmod 8$$

x in U(10)	1	3	7	9
|x|	1	4	4	2

$$3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 27 \equiv 7, \quad 3^4 = 81 \equiv 1 \pmod{10}$$

Proof by contradiction

Suppose ϕ: U(8) → U(10) is an isomorphism. ϕ is onto, so 3 = ϕ(a) for some a ∈ U(8), and Theorem 6.1(5) gives |a| = |ϕ(a)| = |3| = 4. But U(8) has no element of order 4.

So U(8) ≇ U(10).

Exercise 4: Solution (2 of 3)

U(8) ≅ U(12): name the map, then check the four steps.

In U(12) = {1, 5, 7, 11} every element other than 1 has order 2, just as in U(8):

$$5^2 = 25 \equiv 1, \qquad 7^2 = 49 \equiv 1, \qquad 11^2 = 121 \equiv 1 \pmod{12}$$

Define ϕ by listing the images:

$$\varphi: U(8) \to U(12), \qquad \varphi(1) = 1, \quad \varphi(3) = 5, \quad \varphi(5) = 7, \quad \varphi(7) = 11$$

Steps 1–3 (well defined, one-to-one, onto)

ϕ is given by a list: each element of U(8) has exactly one image, and the four images 1, 5, 7, 11 are different and fill U(12).

Step 4 is on the next slide.

Exercise 4: Solution (3 of 3)

Step 4 (operation-preserving): $\phi(ab) = \phi(a)\phi(b)$ for all a, b in $U(8)$.

Both groups are Abelian, so $ab = ba$ and it is enough to check unordered pairs.

$a = 1$: $\phi(1 \cdot b) = \phi(b) = 1 \cdot \phi(b) = \phi(1)\phi(b)$.

$a = b \neq 1$: $a^2 = 1$ in $U(8)$ and $\phi(a)^2 = 1$ in $U(12)$, so $\phi(a^2) = \phi(1) = 1 = \phi(a)^2$.

$a \neq b$, both $\neq 1$: three pairs.

a, b	ab in $U(8)$	$\phi(ab)$	$\phi(a)\phi(b)$ in $U(12)$
3, 5	$15 \equiv 7$	11	$5 \cdot 7 = 35 \equiv 11$
3, 7	$21 \equiv 5$	7	$5 \cdot 11 = 55 \equiv 7$
5, 7	$35 \equiv 3$	5	$7 \cdot 11 = 77 \equiv 5$

So ϕ is an isomorphism, and $U(8) \cong U(12)$.

Exercise 6: Question

Question

Prove that isomorphism is an equivalence relation. That is, for any groups G, H, and K:

$$G \cong G$$

$$G \cong H \text{ implies } H \cong G$$

$$G \cong H \text{ and } H \cong K \text{ imply } G \cong K$$

Gallian writes ≈ where these slides write ≅.

Exercise 6: Solution (1 of 2)

Reflexive and symmetric.

Reflexive: G ≅ G

Define ε: G → G by ε(x) = x. Steps 1–3: ε is the identity map, so it is well defined, one-to-one and onto.
Step 4:

$$\varepsilon(ab) = ab = \varepsilon(a)\,\varepsilon(b) \qquad \text{for all } a, b \in G$$

So ε is an isomorphism, and G ≅ G.

Symmetric: G ≅ H implies H ≅ G

Let ϕ: G → H be an isomorphism. By Theorem 6.2(1), proved in the lecture slides, the inverse map ϕ^{-1}: H → G is also an isomorphism.

So H ≅ G.

Exercise 6: Solution (2 of 2)

Transitive: $G \cong H$ and $H \cong K$ imply $G \cong K$.

Let ϕ: G → H and ψ: H → K be isomorphisms, and define the composite

$$\theta: G \to K, \qquad \theta(x) = \psi\big(\varphi(x)\big)$$

Step 1 (well defined) $\varphi(x) \in H$, so $\psi\big(\varphi(x)\big)$ is one element of K

Step 2 (one-to-one) $\psi\big(\varphi(a)\big) = \psi\big(\varphi(b)\big) \Rightarrow \varphi(a) = \varphi(b) \Rightarrow a = b$

Step 3 (onto) $z \in K$: $z = \psi(y)$, $y = \varphi(x) \Rightarrow \theta(x) = z$

Step 4 (operation-preserving) $\theta(ab) = \psi\big(\varphi(a)\varphi(b)\big) = \psi\big(\varphi(a)\big)\,\psi\big(\varphi(b)\big) = \theta(a)\,\theta(b)$

Step 2 uses that ψ and then ϕ are one-to-one; Step 3 that ψ and then ϕ are onto; Step 4 that ϕ and then ψ preserve the operation.

So θ is an isomorphism, and G ≅ K.

Exercise 7: Question

Question

Give three reasons why S_4 is not isomorphic to D_{12}.

Exercise 7: Solution

$|S_4| = 4! = 24 = |D_{12}|$, so the orders of the groups do not separate them. Count element orders.

Order	1	2	3	4	6	12
S_4	1	9	8	6	0	0
D_{12}	1	13	2	2	2	4

An isomorphism keeps the order of every element (Theorem 6.1(5)) and the number of elements of each order (Theorem 6.1(7)). So each line below is enough on its own:

Reason 1. D_{12} has an element of order 12, the rotation R_{30}; S_4 has none.

Reason 2. D_{12} has an element of order 6, the rotation R_{60}; S_4 has none.

Reason 3. D_{12} has 13 elements of order 2 (12 reflections and R_{180}); S_4 has 9.

So $S_4 \ncong D_{12}$.

A fourth reason: the centre $Z(D_{12}) = \{R_0, R_{180}\}$ has two elements and $Z(S_4)$ has one (Theorem 6.2(6)).

Exercise 8: Question

Question

Show that the mapping $a \to \log_{10} a$ is an isomorphism from $\mathbb{R}^+$ under multiplication to $\mathbb{R}$ under addition.

Exercise 8: Solution

$\mathbb{R}^+$ under multiplication, $\mathbb{R}$ under addition: define ϕ, then check the four steps.

$$\varphi: \mathbb{R}^+ \to \mathbb{R}, \qquad \varphi(a) = \log_{10} a$$

Step 1 (well defined) $\quad$ for each $a > 0$, $\log_{10} a$ is one real number

Step 2 (one-to-one) $\quad \log_{10} a = \log_{10} b \;\Rightarrow\; a = 10^{\log_{10} a} = 10^{\log_{10} b} = b$

Step 3 (onto) $\quad y \in \mathbb{R}: \;\; 10^y > 0 \;\text{ and }\; \varphi(10^y) = y$

Step 4 (operation-preserving) $\quad \varphi(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b = \varphi(a) + \varphi(b)$

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

In Step 4 each group keeps its own operation: the product ab is taken in $\mathbb{R}^+$, the sum $\phi(a) + \phi(b)$ in $\mathbb{R}$.

Exercise 12: Question

Question

Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.

Exercise 12: Solution (1 of 2)

α: G → G, α(g) = g^{-1}. Steps 1–3 hold in every group; everything depends on Step 4.

Step 1 (well defined) each $g \in G$ has exactly one inverse (Theorem 2.3)

Step 2 (one-to-one) $$g^{-1} = h^{-1} \Rightarrow g = \left(g^{-1}\right)^{-1} = \left(h^{-1}\right)^{-1} = h$$

Step 3 (onto) $$y \in G: \ \alpha\left(y^{-1}\right) = \left(y^{-1}\right)^{-1} = y$$

Step 4 is the only real condition

Step 4 asks that α(gh) = α(g)α(h), that is, $(gh)^{-1} = g^{-1}h^{-1}$, for all g, h ∈ G. By the Socks–Shoes Property (Theorem 2.4), $(gh)^{-1} = h^{-1}g^{-1}$. So

$$\alpha \text{ is an automorphism} \Leftrightarrow h^{-1}g^{-1} = g^{-1}h^{-1} \text{ for all } g, h \in G$$

Exercise 12: Solution (2 of 2)

α is an automorphism $\Leftrightarrow h^{-1}g^{-1} = g^{-1}h^{-1}$ for all $g, h \in G$.

If G is Abelian, α is an automorphism

Any two elements of G commute, in particular g^{-1} and h^{-1}. So the condition holds.

If α is an automorphism, G is Abelian

Let $x, y \in G$. Apply the condition to $g = x^{-1}$ and $h = y^{-1}$. Since $g^{-1} = x$ and $h^{-1} = y$, it reads

$$yx = xy$$

So any two elements of G commute.

$\alpha(g) = g^{-1}$ is an automorphism of G if and only if G is Abelian.

Example: in S_3, $\alpha((12)(13)) = (132)^{-1} = (123)$, but $\alpha((12))\alpha((13)) = (12)(13) = (132)$. S_3 is not Abelian, and Step 4 fails.

Exercise 17: Question

Question

If G is a group, prove that Aut(G) and Inn(G) are groups.

The operation is composition of functions. $\text{Inn}(G) = \{\phi_a \mid a \in G\}$, where $\phi_a(x) = axa^{-1}$.

This is Theorem 6.3 of the lecture slides.

Exercise 17: Solution (1 of 2)

Aut(G), the set of all automorphisms of G, is a group under composition.

Closure

Let $\alpha, \beta \in \mathrm{Aut}(G)$. The composite $\alpha\beta$, $(\alpha\beta)(x) = \alpha(\beta(x))$, is an isomorphism from G to G: this is the transitive part of Exercise 6 with $G = H = K$. So $\alpha\beta \in \mathrm{Aut}(G)$.

Associativity

Composition of functions is associative (Theorem 0.8): $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

Identity

$\varepsilon(x) = x$ is an automorphism (the reflexive part of Exercise 6), and $\varepsilon\alpha = \alpha\varepsilon = \alpha$.

Inverses

If $\alpha \in \mathrm{Aut}(G)$, its inverse map α^{-1} is an automorphism by Theorem 6.2(1), and $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \varepsilon$.

So Aut(G) is a group under composition.

Exercise 17: Solution (2 of 2)

Inn(G) = $\{\phi_a \mid a \in G\}$ is a subgroup of Aut(G), so it is a group.

Each ϕ_a is an automorphism (lecture slides), so Inn(G) $\subseteq$ Aut(G). Also $\phi_e(x) = exe^{-1} = x$, so $\varepsilon = \phi_e \in$ Inn(G).

The key identity $\phi_a\phi_b = \phi_{ab}$, using $(ab)^{-1} = b^{-1}a^{-1}$ (Theorem 2.4)

$$(\varphi_a\varphi_b)(x) = \varphi_a\left(bxb^{-1}\right) = a\left(bxb^{-1}\right)a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x)$$

Inverses

$$\varphi_a\varphi_{a^{-1}} = \varphi_{aa^{-1}} = \varphi_e = \varepsilon = \varphi_{a^{-1}a} = \varphi_{a^{-1}}\varphi_a, \qquad \text{so} \quad (\varphi_a)^{-1} = \varphi_{a^{-1}}$$

One-Step Subgroup Test (Theorem 3.1)

$$\varphi_a(\varphi_b)^{-1} = \varphi_a\varphi_{b^{-1}} = \varphi_{ab^{-1}} \in \mathrm{Inn}(G)$$

So Inn(G) is a subgroup of Aut(G), and hence a group.

Exercise 31: Question

Question

Let $r \in U(n)$. Prove that the mapping $\alpha: \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\alpha(s) = sr \bmod n$ for all s in $\mathbb{Z}_n$ is an automorphism of $\mathbb{Z}_n$.

The lecture slides prove the case $n = 10$. The argument below works for every n.

Exercise 31: Solution (1 of 2)

$a(s) = sr \bmod n$ on $\mathbb{Z}_n$, with $r \in U(n)$: Steps 1 and 2.

The tool: an inverse of r modulo n

U(n) is a group under multiplication modulo n (Chapter 2, Example 12), so r has an inverse t in U(n):

$$rt \bmod n = 1$$

Step 1 (well defined) $sr \bmod n$ is one element of $\{0,1, \ldots, n-1\} = \mathbb{Z}_n$

Step 2 (one-to-one) $s_1 r \equiv s_2 r \Rightarrow s_1 rt \equiv s_2 rt \Rightarrow s_1 \equiv s_2 \pmod{n}$

In Step 2, s_1 and s_2 both lie in {0, 1, …, n − 1}, so $s_1 \equiv s_2 \pmod{n}$ means $s_1 = s_2$.

Exercise 31: Solution (2 of 2)

$\alpha(s) = sr \bmod n$ on $\mathbb{Z}_n$, with $r \in U(n)$: Steps 3 and 4.

Step 3 (onto)

$$y \in \mathbb{Z}_n: \ \alpha(yt \bmod n) = ytr \bmod n = y$$

Step 4 (operation-preserving)

$$\alpha(s_1 + s_2) = (s_1 + s_2)r \bmod n = \alpha(s_1) + \alpha(s_2)$$

Addition in $\mathbb{Z}_n$ is addition mod n, and reducing mod n before or after adding or multiplying gives the same result (Chapter 0, Exercise 11).

So α is an automorphism of $\mathbb{Z}_n$.

Example: n = 8, r = 3, with t = 3 since 3 · 3 = 9 ≡ 1 (mod 8)

s	0	1	2	3	4	5	6	7
α(s)	0	3	6	1	4	7	2	5

r must be in U(n): for n = 12 and r = 3, α(4) = 12 mod 12 = 0 = α(0), so α is not one-to-one.

Exercise 41: Question

Question

Prove that $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.

Exercise 41: Solution

Suppose there is an isomorphism $\phi: \mathbb{Z} \to \mathbb{Q}$, and reach a contradiction.

Let $\phi: \mathbb{Z} \to \mathbb{Q}$ be an isomorphism and put $r = \phi(1)$. Since $\phi(0) = 0$ (Theorem 6.1(1)) and ϕ is one-to-one, $r \neq 0$. Every integer k is $k \cdot 1$, so by Theorem 6.1(2), written additively,

$$\varphi(k) = k\,\varphi(1) = kr \qquad \text{for all } k \in \mathbb{Z}$$

Now $r/2$ is in $\mathbb{Q}$ and ϕ is onto, so $r/2 = \phi(k) = kr$ for some integer k. Divide by $r \neq 0$:

$$k = \frac{1}{2}, \qquad \text{which is not an integer.}$$

This contradiction shows that no isomorphism from $\mathbb{Z}$ onto $\mathbb{Q}$ exists.

So $\mathbb{Z} \ncong \mathbb{Q}$ (both under addition).

In other words: $\mathbb{Z} = \langle 1 \rangle$ is cyclic, the argument shows that $\mathbb{Q} = \langle r \rangle$ is impossible, and isomorphic groups are both cyclic or both not (Theorem 6.2(3)).