Introduction to Abstract Algebra I: Homework 4

Due on October 29, 2025 at 23:59

Victor Ostrik

Hashem A. Damrah
UO ID: 952102243

Exercise 5.30. Find the order of the cyclic subgroup $\mathbb{Z}_{16}$ generated by 12.

Solution. Notice that the cyclic subgroup of $\mathbb{Z}_{16}$ generated by 12 is given by

$$\langle 12 \rangle = \{12 \cdot n \pmod{16} \mid n \in \mathbb{Z}\} = \{0, 4, 8, 12\}.$$

Thus, the order of the cyclic subgroup is 4. □

Exercise 5.32. Find the order of the cyclic subgroup S_8 generated by $(2, 4, 6, 9)(3, 5, 7)$.

Solution. Notice that the permutation $(2, 4, 6, 9)(3, 5, 7)$ is the product of two disjoint cycles: a 4-cycle $(2, 4, 6, 9)$ and a 3-cycle $(3, 5, 7)$. The order of a permutation is the least common multiple (LCM) of the lengths of its disjoint cycles. Therefore, the order of the permutation is

$$\operatorname{lcm}(4, 3) = 12.$$

Thus, the order of the cyclic subgroup generated by $(2, 4, 6, 9)(3, 5, 7)$ is 12. □

Exercise 5.40. Show by means of an example that it is possible for the quadratic equation $x^2 = e$ have more than two solutions in some group with identity e.

Solution. Take the algebraic group $\langle V_4, * \rangle$, where V_4 is the Klein four-group defined as $V_4 = \{e, a, b, c\}$ with the operation $*$ defined by the following Cayley table:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

In this group, we can see that:

$$a * a = e, \quad b * b = e, \quad c * c = e.$$

Thus, the equation $x^2 = e$ has four solutions: e, a, b, and c. This shows that it is possible for the quadratic equation $x^2 = e$ to have more than two solutions in a group. □

Exercise 5.41. Let B be a subset of A, and let b be a particular element of B. Determine whether the subset, $\{\sigma \in S_A \mid \sigma(b) = b\}$, of the symmetric group S_A is a subgroup of S_A under the induced operation.

Solution. Define the set $B_S = \{\sigma \in S_A \mid \sigma(b) = b\}$. It's clearly non-empty, since the identity permutation e is in B_S, as $e(b) = b$. Notice that, for any two permutations $\sigma_1, \sigma_2 \in B_S$, we have

$$(\sigma_1 \circ \sigma_2)(b) = \sigma_1(\sigma_2(b)) = \sigma_1(b) = b.$$

Thus, the composition $\sigma_1 \circ \sigma_2$ is also in B_S, showing closure under the group operation. Finally, if $\sigma \in B_S$, then $\sigma \in S_A$. Since S_A is a group, the inverse permutation σ^{-1} also exists in S_A. Moreover, $\sigma^{-1}(b) = b$. Thus, $\sigma^{-1} \in B_S$. Since B_S is closed under the group operation, contains the identity element, and contains inverses, we conclude that B_S is a subgroup of S_A under the induced operation. □

Exercise 5.42. Let B be a subset of A, and let b be a particular element of B. Determine whether the subset, $\{\sigma \in S_A \mid \sigma(b) = B\}$, of the symmetric group S_A is a subgroup of S_A under the induced operation.

Solution. Define the set $B_S = \{\sigma \in S_A \mid \sigma(b) = B\}$. Again, it's clearly non-empty, since the identity permutation e is in B_S, as $e(b) = b \in B$. However, consider two permutations $\sigma_1, \sigma_2 \in B_S$. We have

$$(\sigma_1 \circ \sigma_2)(b) = \sigma_1(\sigma_2(b)) = \sigma_1(B),$$

which may not equal B unless σ_1 maps all elements of B back to B. Thus, the composition $\sigma_1 \circ \sigma_2$ may not be in B_S, showing that B_S is not closed under the group operation. Therefore, we conclude that B_S is not a subgroup of S_A under the induced operation. $\square$

Exercise 5.45. Let $\Phi : G \to G'$ be an isomorphism of a group $\langle G, * \rangle$ with a group $\langle G', *' \rangle$. Prove that if H is a subgroup of G, then $\Phi[H] = \{\Phi(h) \mid h \in H\}$ is a subgroup of G'. That is, an isomorphism carries subgroups into subgroups

Solution. Let H be a subgroup of G. Since H is a subgroup of G, it contains the identity element e. Therefore, $\Phi(e_G) = e'$ is in $\Phi[H]$, so $\Phi[H]$ is non-empty.

Let $\Phi(h_1), \Phi(h_2) \in \Phi[H]$ for some $h_1, h_2 \in H$. Since Φ is an isomorphism, we have

$$\Phi(h_1 * h_2) = \Phi(h_1) *' \Phi(h_2).$$

We have $h_1 * h_2 \in H$ because H is a subgroup of G. Thus, $\Phi(h_1 * h_2) \in \Phi[H]$. Therefore, $\Phi[H]$ is closed under the operation $*'$.

Let $\Phi(h) \in \Phi[H]$ for some $h \in H$. Since Φ is an isomorphism, we have

$$\Phi(h^{-1}) = (\Phi(h))^{-1}.$$

Since H is a subgroup, $h^{-1} \in H$. Thus, $\Phi(h^{-1}) \in \Phi[H]$. Therefore, $\Phi[H]$ contains inverses.

Hence, $\Phi[H]$ is non-empty, closed under the operation $*'$, and contains inverses. Thus, $\Phi[H]$ is a subgroup of G'. $\square$

Exercise 5.46. Let $\Phi : G \to G'$ be an isomorphism of a group $\langle G, * \rangle$ with a group $\langle G', *' \rangle$. Prove that if there is an $a \in G$ such that $\langle a \rangle = G$, then G' is cyclic.

Solution. Since $\langle a \rangle = G$, every element $g \in G$ can be expressed as $g = a^n$ for some integer n. Consider the element $\Phi(a) \in G'$. We will show that $\langle \Phi(a) \rangle = G'$.

Let $g' \in G'$. Since Φ is an isomorphism, there exists a unique $g \in G$ such that $\Phi(g) = g'$. Since $g \in G$, we can write $g = a^n$ for some integer n. Therefore,

$$g' = \Phi(g) = \Phi(a^n) = (\Phi(a))^n.$$

This shows that every element $g' \in G'$ can be expressed as a power of $\Phi(a)$.

Thus, $\langle \Phi(a) \rangle = G'$, and hence G' is cyclic. $\square$

Exercise 5.48. Find an example of a group G and two subgroups H and K such that the set in Exercise 47 is not a subgroup of G.

Solution. Let $G = S_3$, the symmetric group on $\{1, 2, 3\}$. Define two subgroups

$$H = \langle (1\ 2) \rangle = \{e, (1\ 2)\} \text{ and } K = \langle (1\ 3) \rangle = \{e, (1\ 3)\}.$$

Both H and K are subgroups of S_3 of order 2.

Consider the set $HK = \{hk \mid h \in H,\, k \in K\}$. Its elements consist of $\{e, (1\ 2), (1\ 3), (1\ 3\ 2)\}$.

This set has 4 elements. By Lagrange's theorem, any subgroup of S_3 must have an order dividing $|S_3|= 6$. Since there is no subgroup of order 4 in S_3, it follows that HK is *not* a subgroup of G. $\square$

Exercise 5.53. Prove that if G is an abelian group, written multiplicatively, with identity element e, then all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G.

Solution. Let $H = \{x \in G \mid x^2 = e\}$. The identity element e of G satisfies $e^2 = e$, so $e \in H$. Thus, H is non-empty. Let $x, y \in H$. Then $x^2 = e$ and $y^2 = e$. We have

$$(xy)^2 = xyxy = x(yx)y = x(xy)y = (xx)(yy) = e \cdot e = e.$$

Thus, $xy \in H$. Let $x \in H$. We have

$$(x^{-1})^2 = x^{-1}x^{-1} = (xx)^{-1} = e^{-1} = e.$$

Thus, $x^{-1} \in H$.

Since H is non-empty, closed under the group operation, and contains inverses, we conclude that H is a subgroup of G. □

Exercise 5.55. Find a counterexample to Exercise 53 if the assumption of abelian is dropped.

Solution. Consider the non-abelian group $G = S_3$, the symmetric group on $\{1, 2, 3\}$. The elements of S_3 are

$$S_3 = \{e,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}.$$

The elements satisfying $x^2 = e$ are exactly the identity and the transpositions, so

$$H = \{x \in S_3 \mid x^2 = e\} = \{e, (1\ 2), (1\ 3), (2\ 3)\}.$$

To see that H is not a subgroup, note that it is not closed under the group operation. For instance,

$$(1\ 2)(1\ 3) = (1\ 3\ 2) \notin H,$$

because $(1\ 3\ 2)^2 = (1\ 2\ 3) \neq e$. Thus H fails to be closed, so it is not a subgroup of S_3. □