Introduction to Abstract Algebra I: Homework 5

Due on November 5, 2025 at 23:59

Victor Ostrik

Hashem A. Damrah

UO ID: 952102243

Exercise 6.10. Find the number of generators of a cyclic group having the given order of 24.

Solution. The number of generators of a cyclic group of order n is given by $\varphi(n)$, where φ is the Euler's totient function. For $n = 24$, we have

$$\varphi(24) = 24 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8.$$

Therefore, a cyclic group of order 24 has 8 generators. □

Exercise 6.14. An isomorphism of a group with itself is an automorphism of the group. Find the number of automorphisms of the group $\mathbb{Z}_8$.

Solution. Any automorphism of $\mathbb{Z}_8$ is completely determined by the image of 1, and this image must be a generator of $\mathbb{Z}_8$. The generators of $\mathbb{Z}_8$ are precisely the elements that are coprime to 8, namely $1, 3, 5,$ and 7. Therefore, there are 4 possible choices for $\varphi(1)$, each of which defines a distinct automorphism. Hence,

$$|\mathrm{Aut}(\mathbb{Z}_8)| = \varphi(8) = 4.$$

Equivalently, we have $\mathrm{Aut}(\mathbb{Z}_8) \cong U(8) = \{1, 3, 5, 7\}$ under multiplication mod 8. □

Exercise 6.20. Find the number of elements in the cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 19 generated by $(1 + i)/\sqrt{2}$.

Solution. Let $x = \frac{1+i}{\sqrt{2}}$. Computing successive powers, we obtain

$$x^0 = 1, \quad x^1 = \frac{1 + i}{\sqrt{2}}, \quad x^2 = \left(\frac{1 + i}{\sqrt{2}}\right)^2 = i,$$

$$x^3 = \frac{i - 1}{\sqrt{2}}, \quad x^4 = -1, \quad x^5 = \frac{-1 - i}{\sqrt{2}},$$

$$x^6 = -i, \quad x^7 = \frac{1 - i}{\sqrt{2}}, \quad x^8 = 1.$$

Since $x^8 = 1$ and no smaller positive power equals 1, the element x has order 8. Therefore, the cyclic subgroup generated by x has 8 elements, giving us

$$\langle (1 + i)/\sqrt{2} \rangle = \left\{1, \frac{1 + i}{\sqrt{2}}, i, \frac{i - 1}{\sqrt{2}}, -1, \frac{-1 - i}{\sqrt{2}}, -i, \frac{1 - i}{\sqrt{2}}\right\}.$$

Equivalently, note that $\dfrac{1 + i}{\sqrt{2}} = e^{i\pi/4}$, so this subgroup consists of the eighth roots of unity in $\mathbb{C}^*$. □

Exercise 6.22. Find the number of elements in the cyclic subgroup $\langle r^{10} \rangle$ of D_{24}.

Solution. The dihedral group D_{24} has order 48, and its rotation element r has order 24. The order of the element r^{10} is given by

$$\mathrm{ord}(r^{10}) = \frac{24}{\gcd(24, 10)} = \frac{24}{2} = 12.$$

Therefore, the cyclic subgroup $\langle r^{10} \rangle$ has order 12. □

Exercise 6.28. Find the maximum possible order for an element of S_n for a given value of $n = 8$.

Solution. The order of a permutation in S_n is equal to the least common multiple (LCM) of the lengths of its disjoint cycles. Thus, to find the maximum possible order for an element of S_8, we must determine the partition of 8 whose cycle lengths yield the largest LCM. Considering the possible decompositions, we have:

$$(8) \Rightarrow \text{order } 8$$
$$(7, 1) \Rightarrow \text{order } 7$$
$$(6, 2) \Rightarrow \text{order } \operatorname{lcm}(6, 2) = 6$$
$$(5, 3) \Rightarrow \text{order } \operatorname{lcm}(5, 3) = 15$$
$$(4, 3, 1) \Rightarrow \text{order } \operatorname{lcm}(4, 3, 1) = 12$$
$$(4, 2, 2) \Rightarrow \text{order } \operatorname{lcm}(4, 2, 2) = 4.$$

Among these, the maximum occurs for the cycle structure $(5, 3)$, giving an order of 15. Therefore, the maximum possible order of an element in S_8 is 15. $\qquad\square$

Exercise 6.36. Find all orders of subgroups of the group $\mathbb{Z}_{12}$.

Solution. The group $\mathbb{Z}_{12}$ is cyclic of order 12. By Lagrange's theorem, the order of any subgroup of a finite group must divide the order of the group. Hence, the possible orders of subgroups of $\mathbb{Z}_{12}$ are the positive divisors of 12, namely 1, 2, 3, 4, 6, and 12. Moreover, since $\mathbb{Z}_{12}$ is cyclic, there is exactly one subgroup of each of these orders, namely, $\langle 0 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, $\langle 6 \rangle$, and $\langle 12 \rangle = \mathbb{Z}_{12}$ itself. $\qquad\square$

Exercise 6.46. Either give an example of a cyclic group having four generators, or explain why no example exists.

Solution. A cyclic group of order n has $\varphi(n)$ generators, where φ denotes the Euler totient function. To have exactly four generators, we must find all integers n such that $\varphi(n) = 4$. Computing, we find

$$\varphi(5) = 4, \quad \varphi(8) = 4, \quad \varphi(10) = 4, \text{ and } \varphi(12) = 4.$$

Therefore, examples of cyclic groups with four generators include

$$\mathbb{Z}_5, \quad \mathbb{Z}_8, \quad \mathbb{Z}_{10}, \text{ and } \mathbb{Z}_{12}.$$

Each of these cyclic groups has exactly four generators. $\qquad\square$

Exercise 6.50. The generators of the cyclic multiplicative group U_n of all nth roots of unity in $\mathbb{C}$ are the primitive nth roots of unity. Find the primitive nth roots of unity for the given value of $n = 12$.

Solution. The nth roots of unity are given by $e^{2\pi i k/n}$, where $k = 0, 1, 2, \cdots, n-1$ For $n = 12$, these are

$$e^{2\pi i k/12}.$$

The primitive 12th roots of unity correspond to the integers k that are coprime to 12. Since $\gcd(k, 12) = 1$, for $k = 1, 5, 7, 11$. The primitive 12th roots of unity are

$$e^{2\pi i/12}, \quad e^{10\pi i/12}, \quad e^{14\pi i/12}, \quad e^{22\pi i/12}, .$$

Hence, the primitive 12th roots of unity are

$$\cos\left(\frac{\pi}{6}\right) + i\sin\left(\frac{\pi}{6}\right), \ \cos\left(\frac{5\pi}{6}\right) + i\sin\left(\frac{5\pi}{6}\right), \ \cos\left(\frac{7\pi}{6}\right) + i\sin\left(\frac{7\pi}{6}\right), \ \cos\left(\frac{11\pi}{6}\right) + i\sin\left(\frac{11\pi}{6}\right). \ \square$$

Exercise 6.53. Let G be a cyclic group with generator a, and let G' be a group isomorphic to G. If $\varphi : G \to G'$ is an isomorphism, show that, for every $x \in G$, $\varphi(x)$ is completely determined by the value $\varphi(a)$. That is, if $\varphi : G \to G'$ and $\sigma : G \to G'$ are two isomorphisms such that $\varphi(a) = \psi(a)$, then $\varphi(x) = \psi(x)$ for all $x \in G$.

Solution. Since G is cyclic and generated by a, every element $x \in G$ can be written as $x = a^k$ for some integer k. Let $\varphi, \sigma : G \to G'$ be isomorphisms such that $\varphi(a) = \sigma(a)$. Because isomorphisms preserve the group operation, for all integers k we have

$$\varphi(a^k) = (\varphi(a))^k \text{ and } \sigma(a^k) = (\sigma(a))^k.$$

Hence, for $x = a^k$,

$$\varphi(x) = (\varphi(a))^k = (\sigma(a))^k = \sigma(x).$$

Therefore, $\varphi(x) = \sigma(x)$ for all $x \in G$, showing that $\varphi(x)$ is completely determined by the value of $\varphi(a)$. $\square$

Exercise 6.56. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

Solution. Suppose the element ab has order n, so that $(ab)^n = e$. Notice that $ba = b(ab)b^{-1}$. Thus, ba is conjugate to ab by b. Since conjugate elements in a group have the same order, it follows that $\mathrm{ord}(ba) = \mathrm{ord}(ab) = n$.

For completeness, we can verify this directly. We have

$$(ba)^n = b(ab)^n b^{-1} = beb^{-1} = e.$$

Therefore, ba also has order n. $\square$