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. An automorphism has to map a generator to a generator. The generators of $\mathbb{Z}_8$ are the elements that are coprime to 8. The integers coprime to 8 in the range from 0 to 7 are 1, 3, 5, and 7. Therefore, there are 4 generators in $\mathbb{Z}_8$. Take the automorphism that maps $\varphi_1(1) = 3$ and another that maps $\varphi_2(3)1$, then notice that $\varphi_2 = \varphi_1^{-1}$. Similarly, we have $\varphi_3(1) = 5$ and its inverse $\varphi_4(5) = 1$. Thus, we have 4 automorphisms in total. □

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. Computing the powers of the element

$$\begin{aligned}
x^0 &= 1 \\
x^1 &= \frac{1+i}{\sqrt{2}} \\
x^2 &= \left(\frac{1+i}{\sqrt{2}}\right)^2 = \frac{1+2i+i^2}{2} = \frac{2i}{2} = i \\
x^3 &= x^2 \cdot x^1 = i \cdot \frac{1+i}{\sqrt{2}} = \frac{i+i^2}{\sqrt{2}} = \frac{i-1}{\sqrt{2}} \\
x^4 &= x^2 \cdot x^2 = i \cdot i = i^2 = -1 \\
x^5 &= x^4 \cdot x^1 = -1 \cdot \frac{1+i}{\sqrt{2}} = \frac{-1-i}{\sqrt{2}} \\
x^6 &= x^4 \cdot x^2 = -1 \cdot i = -i \\
x^7 &= x^6 \cdot x^1 = -i \cdot \frac{1+i}{\sqrt{2}} = \frac{-i-i^2}{\sqrt{2}} = \frac{-i+1}{\sqrt{2}} \\
x^8 &= x^4 \cdot x^4 = -1 \cdot -1 = 1 \\
x^9 &= x^8 \cdot x^1 = 1 \cdot \frac{1+i}{\sqrt{2}} = \frac{1+i}{\sqrt{2}} = x^1.
\end{aligned}$$

Thus, the powers of x start repeating after x^8. We also have the inverse powers

$$x^{-1} = x^7, \quad x^{-2} = x^6, \quad x^{-3} = x^5, \quad x^{-4} = x^4, \quad x^{-5} = x^3, \quad x^{-6} = x^2, \quad x^{-7} = x^1, \quad x^{-8} = x^0.$$

Therefore, the cyclic subgroup generated by x has 8 elements.

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

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

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

$$\frac{24}{\gcd(24, 10)} = \frac{24}{2} = 12.$$

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

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

Solution. To find the maximum possible order of an element in the symmetric group S_8, we need to consider the cycle decomposition of permutations. The order of a permutation is the least common multiple (LCM) of the lengths of its disjoint cycles. For $n = 8$, we can consider different cycle structures and calculate their orders:

(i) A single 8-cycle: $(a_1a_2a_3a_4a_5a_6a_7a_8)$ has order 8.

(ii) A 7-cycle and a 1-cycle: $(a_1a_2a_3a_4a_5a_6a_7)(a_8)$ has order 7.

(iii) A 6-cycle and a 2-cycle: $(a_1a_2a_3a_4a_5a_6)(a_7a_8)$ has order $\text{lcm}(6, 2) = 6$.

(iv) A 5-cycle and a 3-cycle: $(a_1a_2a_3a_4a_5)(a_6a_7a_8)$ has order $\text{lcm}(5, 3) = 15$.

(v) A 4-cycle and a 4-cycle: $(a_1a_2a_3a_4)(a_5a_6a_7a_8)$ has order $\text{lcm}(4, 4) = 4$.

(vi) A 4-cycle, a 3-cycle, and a 1-cycle: $(a_1a_2a_3a_4)(a_5a_6a_7)(a_8)$ has order $\text{lcm}(4, 3, 1) = 12$.

(vii) A 3-cycle, a 3-cycle, and a 2-cycle: $(a_1a_2a_3)(a_4a_5a_6)(a_7a_8)$ has order $\text{lcm}(3, 3, 2) = 6$.

(viii) Two 2-cycles and a 4-cycle: $(a_1a_2)(a_3a_4)(a_5a_6a_7a_8)$ has order $\text{lcm}(2, 2, 4) = 4$.

(ix) Four 2-cycles: $(a_1a_2)(a_3a_4)(a_5a_6)(a_7a_8)$ has order $\text{lcm}(2, 2, 2, 2) = 2$.

After evaluating these structures, we find that the maximum order is achieved with the cycle structure of a 5-cycle and a 3-cycle, which gives us an order of 15. Therefore, the maximum possible order for an element of S_8 is 15 □

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

Solution. By Lagrange's theorem, the order of any subgroup of a finite group must divide the order of the group. The group $\mathbb{Z}_{12}$ has order 12. The divisors of 12 are 1, 2, 3, 4, 6, and 12. Therefore, the possible orders of subgroups of $\mathbb{Z}_{12}$ are just these divisors. □

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 is the Euler's totient function. To have exactly four generators, we need to find an integer n such that $\varphi(n) = 4$. The values of n for which $\varphi(n) = 4$ are: $n = 5$, $n = 8$, and $n = 10$, since $\varphi(5) = 4$, $\varphi(8) = 4$, and $\varphi(10) = 4$.

Therefore, examples of cyclic groups having four generators include $\mathbb{Z}_5$, $\mathbb{Z}_8$, and $\mathbb{Z}_{10}$. □

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 the formula

$$e^{2\pi ik/n} \quad \text{for } k = 0, 1, 2, \ldots, n-1.$$

For $n = 12$, the 12th roots of unity are:

$$e^{2\pi ik/12} \quad \text{for } k = 0, 1, 2, \ldots, 11.$$

The primitive nth roots of unity are those roots for which k is coprime to n. The integers coprime to 12 in the range from 0 to 11 are 1, 5, 7, and 11. Therefore, the primitive 12th roots of unity are:

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

Simplifying these expressions, we get:

$$e^{\pi i/6}, \quad e^{5\pi i/6}, \quad e^{7\pi i/6}, \quad e^{11\pi i/6}.$$

Thus, the primitive 12th roots of unity are:

$$\cos(\pi/6) + i\sin(\pi/6), \quad \cos(5\pi/6) + i\sin(5\pi/6), \quad \cos(7\pi/6) + i\sin(7\pi/6), \quad \cos(11\pi/6) + i\sin(11\pi/6).$$ □

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 a cyclic group generated by a, every element $x \in G$ can be expressed as $x = a^k$ for some integer k. Now, consider the two isomorphisms $\varphi : G \to G'$ and $\psi : G \to G'$ such that $\varphi(a) = \psi(a)$.

We want to show that $\varphi(x) = \psi(x)$ for all $x \in G$. Let $x = a^k$ for some integer k. Then we have:

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

Similarly,

$$\psi(x) = \psi(a^k) = (\psi(a))^k.$$

Since we are given that $\varphi(a) = \psi(a)$, it follows that:

$$(\varphi(a))^k = (\psi(a))^k.$$

Therefore, we have:

$$\varphi(x) = \psi(x).$$

This shows that for every element $x \in G$, the value of $\varphi(x)$ is completely determined by the value of $\varphi(a)$, and thus $\varphi(x) = \psi(x)$ for all $x \in G$. □

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. Let the order of the element ab be n. This means that

$$(ab)^n = e.$$

We want to show that $(ba)^n = e$ as well. We can compute $(ba)^n$ as follows:

$$\begin{aligned} (ba)^n &= b(ab)^{n-1}a \\ &= bea \quad (\text{since } (ab)^n = e) \\ &= ba. \end{aligned}$$

However, this does not directly show that $(ba)^n = e$. Instead, we can use the fact that conjugation preserves order. Specifically, we can write:

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

Thus, we have shown that $(ba)^n = e$, which means that the order of ba is also n. □