

3.5 SOLUTIONS

20. Show that the three groups \mathbf{Z}_6 , \mathbf{Z}_9^\times , and \mathbf{Z}_{18}^\times are isomorphic to each other.

Solution: First, we have $|\mathbf{Z}_9^\times| = 6$, and $|\mathbf{Z}_{18}^\times| = 6$. In \mathbf{Z}_9^\times , $2^2 = 4$, $2^3 = 8 \not\equiv 1$, and so $[2]$ must have order 6, showing that \mathbf{Z}_9^\times is cyclic of order 6. Our theorems tell us that $\mathbf{Z}_9^\times \cong \mathbf{Z}_6$. In \mathbf{Z}_{18}^\times , $5^2 \equiv 7$, $5^3 \equiv 17 \not\equiv 1$, and so $[5]$ must have order 6, showing that \mathbf{Z}_{18}^\times is cyclic of order 6. Our theorems tell us that $\mathbf{Z}_{18}^\times \cong \mathbf{Z}_6$. Thus all three groups are isomorphic.

21. Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$?

Solution: It follows from Theorem 3.5.4 that $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$, and that $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. It then follows from Problem 3.4.23 that $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$, and $\mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. Finally, it is possible to show that the obvious mapping from $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ onto $\mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$ is an isomorphism. Therefore $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_{20}$.

22. Is $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{10}$?

Solution: As in Problem 21, $\mathbf{Z}_4 \times \mathbf{Z}_{15} \cong \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5$, and $\mathbf{Z}_6 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_5$. The two groups are not isomorphic since the first has an element of order 4, while the second has none.

23. Give the lattice diagram of subgroups of \mathbf{Z}_{100} .

Solution: The subgroups correspond to the divisors of 100, and are given in Figure 3.0.1. Note that $n\mathbf{Z}_{100}$ is used to mean all multiples of n in \mathbf{Z}_{100} .

24. Find all generators of the cyclic group \mathbf{Z}_{28} .

Solution: By Proposition 3.5.3 (b), the generators correspond to the numbers less than 28 and relatively prime to 28. The Euler φ -function allows us to compute how many there are: $\varphi(28) = \frac{1}{2} \cdot \frac{6}{7} \cdot 28 = 12$. The list of generators is $\{\pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13\}$.

25. In \mathbf{Z}_{30} , find the order of the subgroup $\langle [18]_{30} \rangle$; find the order of $\langle [24]_{30} \rangle$.

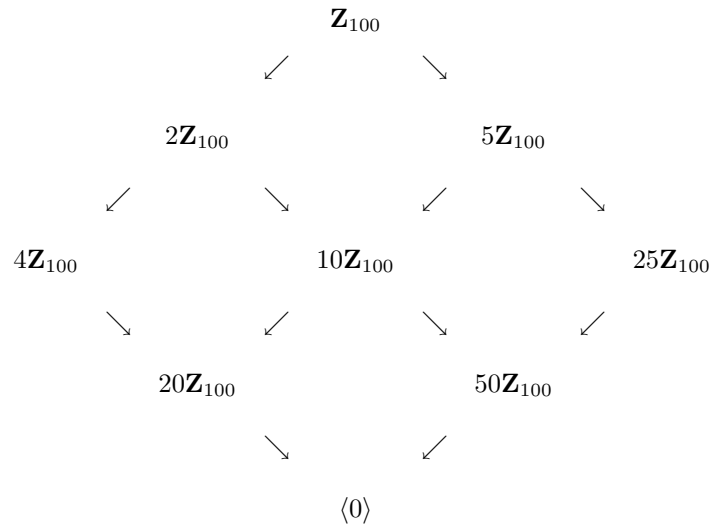
Solution: Using Proposition 3.5.3 (a), we first find $\gcd(18, 30) = 6$. Then $\langle [18]_{30} \rangle = \langle [6]_{30} \rangle$, and so the subgroup has $30/6 = 5$ elements.

Similarly, $\langle [24]_{30} \rangle = \langle [6]_{30} \rangle$, and so we actually have $\langle [24]_{30} \rangle = \langle [18]_{30} \rangle$.

26. Prove that if G_1 and G_2 are groups of order 7 and 11, respectively, then the direct product $G_1 \times G_2$ is a cyclic group.

Solution: Since 7 and 11 are primes, the groups are cyclic. If a has order 7 in G_1 and b has order 11 in G_2 , then (a, b) has order $\text{lcm}[7, 11] = 77$ in $G_1 \times G_2$. Thus $G_1 \times G_2$ is cyclic since it has an element whose order is equal to the order of the group.

Figure 3.0.1 for Problem 23



27. Show that any cyclic group of even order has exactly one element of order 2.

Solution: If G is cyclic of order $2n$, for some positive integer n , then it follows from Theorem 3.5.2 that G is isomorphic to \mathbf{Z}_{2n} . Since isomorphisms preserve orders of elements, we only need to answer the question in \mathbf{Z}_{2n} . In that group, the elements of order 2 are the nonzero solutions to the congruence $2x \equiv 0 \pmod{2n}$, and since the congruence can be rewritten as $x \equiv 0 \pmod{n}$, we see that $[n]_{2n}$ is the only element of order 2 in \mathbf{Z}_{2n} .

28. Use the the result in Problem 27 to show that the multiplicative groups \mathbf{Z}_{15}^\times and \mathbf{Z}_{21}^\times are not cyclic groups.

Solution: In \mathbf{Z}_{15}^\times , both $[-1]_{15}$ and $[4]_{15}$ are easily checked to have order 2.

In \mathbf{Z}_{21}^\times , we have $[8]_{21}^2 = [64]_{21} = [1]_{21}$, and so $[8]_{21}$ and $[-1]_{21}$ have order 2.

29. Find all cyclic subgroups of the quaternion group. Use this information to show that the quaternion group cannot be isomorphic to the subgroup of \mathcal{S}_4 generated by $(1, 2, 3, 4)$ and $(1, 3)$.

Solution: The quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is defined in Example 3.3.7 of the text (see page 108). The elements satisfy the following identities: $i^2 = j^2 = k^2 = -1$ and $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$. The cyclic subgroups $\langle -1 \rangle = \{\pm 1\}$, $\langle \pm i \rangle = \{\pm 1, \pm i\}$, $\langle \pm j \rangle = \{\pm 1, \pm j\}$, and $\langle \pm k \rangle = \{\pm 1, \pm k\}$ can be found by using the given identities. For example, $i^2 = -1, i^3 = i^2i = -i$, and $i^4 = i^2i^2 = (-1)^2 = 1$.

In \mathcal{S}_4 , let $(1, 2, 3, 4) = a$ and $(1, 3) = b$. Since a is a cycle of length 4, it has order 4, with $a^2 = (1, 3)(2, 4)$ and $a^3 = a^{-1} = (1, 4, 3, 2)$. To find the subgroup generated by a and b , we have $ab = (1, 2, 3, 4)(1, 3) = (1, 4)(2, 3)$, $a^2b = (1, 3)(2, 4)(1, 3) = (2, 4)$, and $a^3b = (1, 4, 3, 2)(1, 3) = (1, 2)(3, 4)$. On the other side, we have $ba = (1, 3)(1, 2, 3, 4) = (1, 2)(3, 4) = a^3b$, $ba^2 = (1, 3)(1, 3)(2, 4) = (2, 4) = a^2b$, and $ba^3 = (1, 3)(1, 4, 3, 2) = (1, 4)(2, 3) = ab$. This shows that the subgroup generated by a and b consists of the 8 elements $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Furthermore, from the cycle structures of the elements we can see that the only cyclic subgroup of order 4 is the one generated by a (and a^3). In any isomorphism, cyclic subgroups would correspond to cyclic subgroups, and so it is impossible for this group to be isomorphic to the quaternion group, which has 3 cyclic subgroups of order 4.

30. Prove that if p and q are different odd primes, then \mathbf{Z}_{pq}^\times is not a cyclic group.

Solution: We know that $[-1]_{pq}$ has order 2, so by Problem 27 it is enough to find one other element of order 2. The Chinese remainder theorem (Theorem 1.3.6) states that the system of congruences $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{q}$ has a solution $[a]_{pq}$, since p and q are relatively prime. Because q is an odd prime, $[-1]_{pq}$ is not a solution, so $[a]_{pq} \neq [-1]_{pq}$. But $a^2 \equiv 1 \pmod{p}$ and $a^2 \equiv 1 \pmod{q}$, so $a^2 \equiv 1 \pmod{pq}$ since p and q are relatively prime, and thus $[a]_{pq}$ has order 2.