

1. (b) Let G be a group, and let a be an element of G . Define $\phi : G \rightarrow G$ by setting $\phi(x) = axa^{-1}$, for all $x \in G$. Show that ϕ is an isomorphism.

Solution: To show that ϕ is one-to-one, define $\theta : G \rightarrow G$ by $\theta(x) = a^{-1}xa$, for all $x \in G$. Then it is easy to check that θ is an inverse function for ϕ .

Finally, ϕ respects the operation of G since $\phi(xy) = axya^{-1}$ and $\phi(x)\phi(y) = (axa^{-1})(aya^{-1}) = axya^{-1}$.

2. (a) Prove that if $\phi : G_1 \rightarrow G_2$ is a group isomorphism and H is a subgroup of G_1 , then $\phi(H)$ is a subgroup of G_2 .

Solution: Since $e \in H$ and $\phi(e) = e$, we have $e \in \phi(H)$.

If $y_1, y_2 \in \phi(H)$, then $y_1 = \phi(x_1)$ and $y_2 = \phi(x_2)$, for some $x_1, x_2 \in H$. Then $y_1y_2^{-1} = \phi(x_1)(\phi(x_2))^{-1} = \phi(x_1)\phi(x_2^{-1}) = \phi(x_1x_2^{-1}) \in \phi(H)$ since $x_1x_2^{-1} \in H$.

4. Let G be an abelian group, and let H be the subset of G consisting of all elements of G that have finite order.

(a) Prove that H is a subgroup of G .

Solution: The identity e certainly belongs to H , since it has order 1. If a and b have finite order, say $a^n = e$ and $a^k = e$, then for $m = \text{lcm}[n, k]$ we have $(ab)^m = a^mb^m = e$ since G is abelian, so the order of ab is a divisor of m . Finally, if a has order n then so does a^{-1} from a homework problem, so a^{-1} belongs to H .

(b) If $G = \mathbf{R}^\times$, what is H ? If $G = \mathbf{R}$, what is H ?

Solution: If $G = \mathbf{R}^\times$, then $H = \{\pm 1\}$, since $x^n = 1$ forces $|x| = 1$. If $G = \mathbf{R}$, then $H = \{0\}$ since the only solution to the equation $nx = 0$ is $x = 0$.

5. (b) Let G be a group. If $a \in G$ has order 48, list all powers of a that have order 12.

Solution: The element a^4 has order 12, and generates a cyclic subgroup isomorphic to \mathbf{Z}_{12} . The elements of order 12 in \mathbf{Z}_{12} are 1, 5, 7, 11, and so the corresponding element in $\langle a \rangle$ are $a^4, (a^4)^5 = a^{20}, (a^4)^7 = a^{28},$ and $(a^4)^{11} = a^{44}$.

6. (a) Let G be a group of order 4, with identity element e and elements a, b, c . If a, b, c each have order 2, write out the group table for G . Explain why there is only one possible group table.

Solution: See the discussion on page 115, which includes the group tables for a cyclic group of order 4 and for a group of order 4 that is not cyclic. The difference is that if every nontrivial element has order 4, then every entry on the main diagonal of the group has to be e .

(b) Explain why any group of order 4 is isomorphic to either \mathbf{Z}_4 or $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Solution: In a group of order 4 the only possible orders of elements are 1, 2, 4. Therefore either the group has an element of order 4, which makes it cyclic and isomorphic to \mathbf{Z}_4 , or else it has no element of order 4 and therefore has the group table in part (a). This group table is the same as the one for $\mathbf{Z}_2 \times \mathbf{Z}_2$, which is not cyclic. Therefore, in the second case, the group is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$.

7. List the elements of \mathbf{Z}_{30}^\times . Is \mathbf{Z}_{30}^\times a cyclic group?

Solution: $\mathbf{Z}_{30}^\times = \{1, 7, 11, 13, 17, 19, 23, 29\} = \{\pm 1, \pm 7, \pm 11, \pm 13\}$

Since $30 = 2 \cdot 3 \cdot 5$, we have $\mathbf{Z}_{30}^\times \cong \mathbf{Z}_2^\times \times \mathbf{Z}_3^\times \times \mathbf{Z}_5^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_4$ so it has no element of order 8.

The computational proof (not as elegant) goes this way: $(\pm 7)^2 = 49 \equiv -11$, and $(-11)^2 = 121 \equiv 1$. This shows that ± 7 have order 4, while ± 11 have order 2. Next, $(\pm 13)^2 = 169 \equiv -11$, so ± 13 have order 4. Finally, -1 has order 2. Thus there is no element of order 8, and the group is not cyclic.

8. Let $n = pq$, where p and q are different odd primes. Prove that \mathbf{Z}_n^\times is not cyclic.

Solution: We have $\mathbf{Z}_n^\times \cong \mathbf{Z}_p^\times \times \mathbf{Z}_q^\times$. Since \mathbf{Z}_p^\times has $p - 1$ elements and \mathbf{Z}_q^\times has $q - 1$ elements, which are both even numbers, the least common multiple of $p - 1$ and $q - 1$ cannot be equal to their product. This means that \mathbf{Z}_n^\times cannot have an element of order $\varphi(n)$.

As an alternate proof, in the direct product you can see that there is a subgroup of order 4 that is not cyclic: $\{(\pm 1, \pm 1)\}$. Since every subgroup of a cyclic group must be cyclic, this shows that \mathbf{Z}_n^\times is not cyclic.