Homework 7 Solution

Chapter 7.

1. Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4.

   Because $|A_4| = 12$ and $|H| = 4$, there are exactly $12/4 = 3$ distinct cosets of H.

$$H = \{e, (12)(34), (13)(24), (14)(23)\}$$

$$\begin{aligned}(123)H &= \{(123)e, (123)(12)(34), (123)(13)(24), (123)(14)(23)\}\\ &= \{(123), (134), (243), (142)\}\end{aligned}$$

$$\begin{aligned}(124)H &= \{(124)e, (124)(12)(34), (124)(13)(24), (124)(14)(23)\}\\ &= \{(124), (143), (132), (234)\}\end{aligned}$$

   So they are all of them. Indeed, $H = (12)(34)H = (13)(24)H = (14)(23)H$, $(123)H = (134)H = (243)H = (142)H$, $(124)H = (143)H = (132)H = (234)H$.

6. Let n be a positive integer. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \cdots\}$. Find all left cosets of H in $\mathbb{Z}$. How many are there?

   Note that $H = \langle n \rangle$. We claim that $H, 1 + H, 2 + H, \cdots, (n-1) + H$ are all distinct cosets of H.

   Step 1. They are distinct.

   If $a + H = b + H$ for $0 \le a, b \le n - 1$, then $a \in b + H = \{b, b \pm n, b \pm 2n, \cdots\}$. Because b is the only positive integer in $b + H$ less than n, $a = b$. Therefore they are distinct.

   Step 2. They are all of them.

   If $c + H$ is a coset containing $c \in \mathbb{Z}$, then by division algorithm, there are q and r such that $c = qn + r$ and $0 \le r < n$. Then $c \in r + H$ and $c + H = r + H$.

   In summary, there are n distinct cosets.

7. Find all of the left cosets of $\{1, 11\}$ in $U(30)$.

   Note that $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$. So there are 4 distinct cosets. Let $H = \{1, 11\}$. Then

$$H, 7H = \{7 \cdot 1, 7 \cdot 11\} = \{7, 17\},$$

$$13H = \{13 \cdot 1, 13 \cdot 11\} = \{13, 23\}, 19H = \{19 \cdot 1, 19 \cdot 11\} = \{19, 29\}$$

   are distinct cosets.

8. Suppose that a has order 15. Find all of the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.

   Because $|\langle a \rangle : \langle a^5 \rangle| = 15/3 = 5$, there are 5 distinct cosets. Let $H = \langle a^5 \rangle$. We claim that H, aH, a^2H, a^3H, a^4H are all cosets. They are distinct, because the smallest positive n such that a^n is in the coset is $5, 1, 2, 3$, and 4 respectively.

12. Let a and b be nonidentity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.

    Let H be a non-trivial subgroup of G containing both a and b. By Lagrange's theorem, $|H| = 5, 31$, or 155. If $|H| = 5$, then it is cyclic and all non-identity elements have the same order 5. Similarly, if $|H| = 31$, all non-identity elements are of order 31. Therefore $|H| = 155$ and $H = G$.

18. Recall that, for any integer n greater than 1, $\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)} \bmod n = 1$.

    Let $a \bmod n = b$. Because a is relatively prime to n, $b \in U(n)$. Because $|U(n)| = \phi(n)$, $b^{\phi(n)} = b^{|U(n)|} = 1 \bmod n$. Therefore $a^{\phi(n)} = b^{\phi(n)} = 1 \bmod n$.

20. Use Corollary 2 of Lagrange's Theorem (Theorem 7.1) to prove that the order of $U(n)$ is even when $n > 2$.

    Because $\gcd(n-1, n) = 1$, $n - 1 \in U(n)$. If $n > 2$, then $n - 1 \neq 1$. Now $(n-1)^2 = n^2 - 2n + 1 = 1 \bmod n$. Therefore $|n-1| = 2$. Because $2 = |n-1| \,|\, |U(n)|$, $|U(n)|$ is even.

21. Suppose G is a finite group of order n and m is relatively prime to n. If $g \in G$ and $g^m = e$, prove that $g = e$.

    Because $g^m = e$, $|g| \,|\, m$. Also $|g| \,|\, |G| = n$. Therefore $|g|$ is a common divisor of m and n, which is 1. Therefore $|g| = 1$ and $g = e$.

27. Let $|G| = 15$. If G has only one subgroup of order 3 and only one of order 5, prove that G is cyclic. Generalize to $|G| = pq$, where p and q are prime.

    Note that for a non-identity element $a \in G$, $|a| = 3, 5$, or 15. Let $A = \{a \in G \mid |a| = 3\}$ and $B = \{a \in G \mid |a| = 5\}$. For $b \in A$, $\langle b \rangle = \{e, b, b^2\}$ is a subgroup of order 3. Because there is only one subgroup of order 3, $A = \{b, b^2\}$ and $|A| = 2$. Similarly, for $c \in B$, $\langle c \rangle = \{e, c, c^2, c^3, c^4\}$ is the unique subgroup of order 5 and $B = \{c, c^2, c^3, c^4\}$. Therefore $|B| = 4$. This implies that there are $15 - 2 - 4 - 1 = 8$ elements of order 15 (The one is for the identity). Hence G is cyclic.

    The argument can be generalized in a straightforward way. If we define $S_p = \{a \in G \mid |a| = p\}$ and $S_q = \{a \in G \mid |a| = q\}$, then $|S_p| = p - 1$ and $|S_q| = q - 1$. Because $(p-1)(q-1) > 0$, $|G| = pq > p - 1 + q - 1 + 1 = p + q - 1$. Thus there is an element of order pq and G is cyclic.

30. Let $|G| = 8$. Show that G must have an element of order 2.

For a non-identity $a \in G$, $|a| = 2, 4$, or 8. If $|a| = 2$, a is what we want. If $|a| = 4$, then $|a^2| = 4/2$. If $|a| = 8$, $|a^4| = 8/4 = 2$. Thus in any cases, we can find an order two element.

42. Let G be a group of order n and k be any integer relatively prime to n. Show that the mapping from G to G given by $g \to g^k$ is one-to-one. If G is also Abelian, show that the mapping given by $g \to g^k$ is an automorphism of G.

    Let $\phi : G \to G$ is defined by $\phi(g) = g^k$. Because n and k are relatively prime, there are two integers a, b such that $an + bk = 1$. If $\phi(g) = \phi(h)$, then $g^k = h^k$. So

    $$g = g^{an+bk} = (g^n)^a(g^k)^b = (g^k)^b = (h^k)^b = (h^n)^a(h^k)^b = h^{an+bk} = h.$$

    Therefore G is one-to-one.

    Now suppose that G is Abelian. Then ϕ is one-to-one as above. Moreover, ϕ is onto because an one-to-one map between two finite sets with the same number of elements is onto as well. Finally, because G is Abelian,

    $$\phi(gh) = (gh)^k = g^k h^k = \phi(g)\phi(k).$$

    Therefore ϕ is an automorphism.

45. Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$.

    (a) Find the stabilizer of 1 and the orbit of 1.

    $$\mathrm{stab}_G(1) = \{(1), (24)(56)\},\ \mathrm{orb}_G(1) = \{1, 2, 3, 4\}$$

    (b) Find the stabilizer of 3 and the orbit of 3.

    $$\mathrm{stab}_G(3) = \{(1), (24)(56)\},\ \mathrm{orb}_G(3) = \{3, 4, 1, 2\}$$

    (c) Find the stabilizer of 5 and the orbit of 5.

    $$\mathrm{stab}_G(5) = \{(1), (12)(34), (13)(24), (14)(23)\},\ \mathrm{orb}_G(5) = \{5, 6\}$$

57. Let $G = GL(2, \mathbb{R})$ and $H = SL(2, \mathbb{R})$. Let $A \in G$ and suppose that $\det A = 2$. Prove that AH is the set of all 2×2 matrices in G that have determinant 2.

    Let $D = \{A \in GL(2, \mathbb{R}) \mid \det A = 2\}$.

    If $B \in AH$, then $B = AC$ where $C \in H = SL(2, \mathbb{R})$. So $\det B = \det AC = \det A \det C = 2 \cdot 1 = 2$. Therefore $B \in D$ and $AH \subset D$.

    On the other hand, if $B \in D$, then $B = AA^{-1}B$ and $\det A^{-1}B = \det A^{-1} \det B = 1/2 \cdot 2 = 1$. Therefore $A^{-1}B \in SL(2, \mathbb{R}) = H$ and $B \in AH$. Hence $D \subset AH$ and $D = AH$.