

Solution Outlines for Chapter 7

1: Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4 (using table 5.1).

There are three cosets:

$$H = \{(1), (12)(34), (13)(24), (14)(23)\} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$$

$$(123)H = \{(123), (134), (243), (142)\} = \{\alpha_5, \alpha_6, \alpha_7, \alpha_8\}$$

$$(132)H = \{(132), (143), (234), (124)\} = \{\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}\}$$

2: Let H be as in Exercise 1. How many left cosets of H in S_4 are there? (Determine this without listing them.)

Using Corollary 1 of Lagrange's theorem, there are $\frac{|S_4|}{|H|} = \frac{4!}{4} = 6$ left cosets. (Note: this makes sense given that there are three in A_4 and S_4 is twice as large.)

3: Let $H = \{0, \pm 3, \pm 6, \pm 9, \dots\}$. Find all the left cosets of H in \mathbb{Z} .

There are 3: H , $1 + H$, and $2 + H$. (Note: By the division algorithm, we know there are no other cosets.)

5: Let H be as in Exercise 3. Decide whether or not the following cosets of H are the same.

To do this, we use that $aH = bH$ iff $a^{-1}b \in H$, which in additive notation is $(-a) + b \in H$.

a. $11 + H$ and $17 + H$: $-11 + 17 = 6$, and $6 \in H$ so yes, they are the same.

b. $-1 + H$ and $5 + H$: $-(-1) + 5 = 6$, which is still in H so yes, they are the same.

c. $7 + H$ and $23 + H$: $-7 + 23 = 16$ but 16 is not a multiple of 3 so it is not in H . Hence these are different cosets.

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

Notice that $\frac{15}{3} = 5$, so we will have five left cosets. They are: $\langle a^5 \rangle = \{a^5, a^{10}, e\}$, $a \langle a^5 \rangle = \{a^6, a^{11}, a\}$, $a^2 \langle a^5 \rangle = \{a^7, a^{12}, a^2\}$, $a^3 \langle a^5 \rangle = \{a^8, a^{13}, a^3\}$, and $a^4 \langle a^5 \rangle = \{a^9, a^{14}, a^4\}$.

14: Let C^* be the group of nonzero complex numbers under multiplication and let $H = \{a + bi \in \mathbb{C}^* | a^2 + b^2 = 1\}$. Give a geometric description of the coset $(3 + 4i)H$. Give a geometric description of the coset $(c + di)H$.

First, notice that geometrically H is a circle of radius 1 with center $(0, 0)$. Now, the coset $(3 + 4i)H$ is a circle with center $(0, 0)$ as well. However, the $(3 + 4i)$ scales the equation so that 1 becomes $3^2 + 4^2 = 25$. To see this, notice that $(3 + 4i)(a + bi) = (3a - 4b) + (3b + 4a)i$ so the action of $(3 + 4i)$ sends the point (a, b) to the point $(3a - 4b, 3b + 4a)$. Now, this makes the equation $(3a - 4b)^2 + (3b + 4a)^2 = 9a^2 - 24ab + 16b^2 + 9b^2 + 24ab + 16a^2 = 25a^2 + 25b^2 =$

$$25(a^2 + b^2) = 25.$$

In general, the coset $(c + di)H$, by similar computation, is the circle centered at the origin with radius $\sqrt{c^2 + d^2}$.

15: Let G be a group of order 60. What are the possible orders for the subgroups of G ?

The possible orders are the divisors of 60: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

16: Suppose that K is a proper subgroup of H and H is a proper subgroup of G . If $|K| = 42$ and $|G| = 420$, what are the possible orders of H ?

By Lagrange's theorem we know that K a subgroup of H implies that $42 \mid |H|$. Similarly, H a subgroup of G implies $|H| \mid 420$. Thus the possible orders of H are 42, 84, 210, and 420. However, we also know that these subgroups are all proper and so H can not have order 42 (else $H = K$) nor can it have order 420 (else $H = G$). Hence, the possible orders are 84 and 210.

17: Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

Proof. Let G be a group with $|G| = pq$ where p, q are prime. Let H be a proper subgroup of G . By Lagrange's theorem, the order of H is either 1, p , or q (It can not be pq since H is proper). If $|H| = 1$, $H = \{e\} = \langle e \rangle$, and hence it is cyclic. If H is not trivial, then the order of H is either p or q , which are both prime. Hence, H is cyclic (by corollary of Lagrange's theorem). \square

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

Proof. Notice that $n - 1 \in U(n)$ for all n . Further, $(n - 1)^2 = n^2 - 2n + 1 = 1$ so the order of $n - 1$ is 2. Thus we know that $2 \mid |U(n)|$ so its order must be even. \square

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 $g = e$.

Proof. Notice that the order of an element has to divide the order of the group, so the order of g can not be m . We also know that $g^{|G|} = g^n = e$. So the order of g divides both m and n . However, $\gcd(m, n) = 1$ so the order of g is actually 1. Hence, $g = e$. \square

26: Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime.

Proof. Let G be a group with more than element and no proper, nontrivial subgroups. First, suppose $|G|$ is infinite. If G is cyclic, it is generated by some element in G , say x . Then $\langle x^2 \rangle$ is a proper, nontrivial subgroup of G , which is a contradiction. Suppose instead that G is not cyclic. Then let x be any non-identity element of G . The group $\langle x \rangle$ is now a

proper, nontrivial subgroup of G and we again have a contradiction.

Hence, we may now assume $|G|$ is finite. Let x be a non-identity element in G . Since G has no proper, non-trivial subgroups and $\langle x \rangle \subseteq G$, it must be that $G = \langle x \rangle$. Now, by the fundamental theorem of cyclic groups, we know that any divisor of the order of G will result in a corresponding cyclic subgroup. Since there are none, the order of G has to be prime. \square

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.

Proof. Let G have order 15 and be as described above. Since 3 and 5 are prime, the two subgroups are cyclic. Call their generators a and b respectively so $|\langle a \rangle| = 3$ and $|\langle b \rangle| = 5$. Since the intersection of these two groups is just $\{e\}$, $|\langle a \rangle \cup \langle b \rangle| = 7$. Therefore G has some elements not in $\langle a \rangle \cup \langle b \rangle$. Choose one, say d . Then the order of d is either 3, 5, or 15. Since $d \notin \langle a \rangle$, the order of d can not be 3 (otherwise $\langle d \rangle$ would be a new subgroup of order 3). Similarly, the order of d can not be 5. Hence, the order of d is 15 and $G = \langle d \rangle$. \square

The proof generalizes to any group of order pq where p and q are prime. In this case $|H \cup K| = p + q - 1 < pq$. Just as above, any element not in $H \cup K$ would necessarily have order pq , making it a generator of G .

28: Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G . Generalize to any group of order p^2 where p is prime. Does your proof work for this generalization?

Proof. Let G be a group of order 25. Assume G is not cyclic. Hence no element of G has order 25. But $|g|$ must divide $|G| = 25$ for all $g \in G$, so the order of g must be 5 for all elements. Hence, $g^5 = e$ for all $g \in G$. \square

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

Let $|G| = 8$. Let g be any non-identity element of G . Its order is 2, 4 or 8 (consequence of Lagrange's theorem). If g has order 2, we are done. Assume g has order 4. Then $(g^2)^2 = e$ and $g^2 \neq e$. So g^2 is an element of order 2. Now, assume g has order 8, making G is cyclic. Then $(g^4)^2 = e$ so the element g^4 has order 2.

33: Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $|G : H| = |G : K||K : H|$.

Viewing K as a subgroup of G , we see $\frac{|G|}{|K|} = |G : K|$. Next, we can view H as a subgroup of K so $\frac{|K|}{|H|} = |K : H|$. Finally, we can view H as a subgroup of G so $|G : H| = \frac{|G|}{|H|} = \frac{|G|}{|K|} \frac{|K|}{|H|} = |G : K||K : H|$.

44: Prove that every subgroup of D_n of odd order is cyclic.

Let G be a subgroup of D_n with odd order. Then G can not contain any flips since the order of an element has to divide the order of a group. Thus $G \subseteq \langle r \rangle$, which is cyclic. We already know from the fundamental theorem of cyclic groups that all subgroups of cyclic groups are cyclic so G must be cyclic.

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.**

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

b. **Find the stabilizer of 3 and the orbit of 3.**

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

c. **Find the stabilizer of 5 and the orbit of 5.**

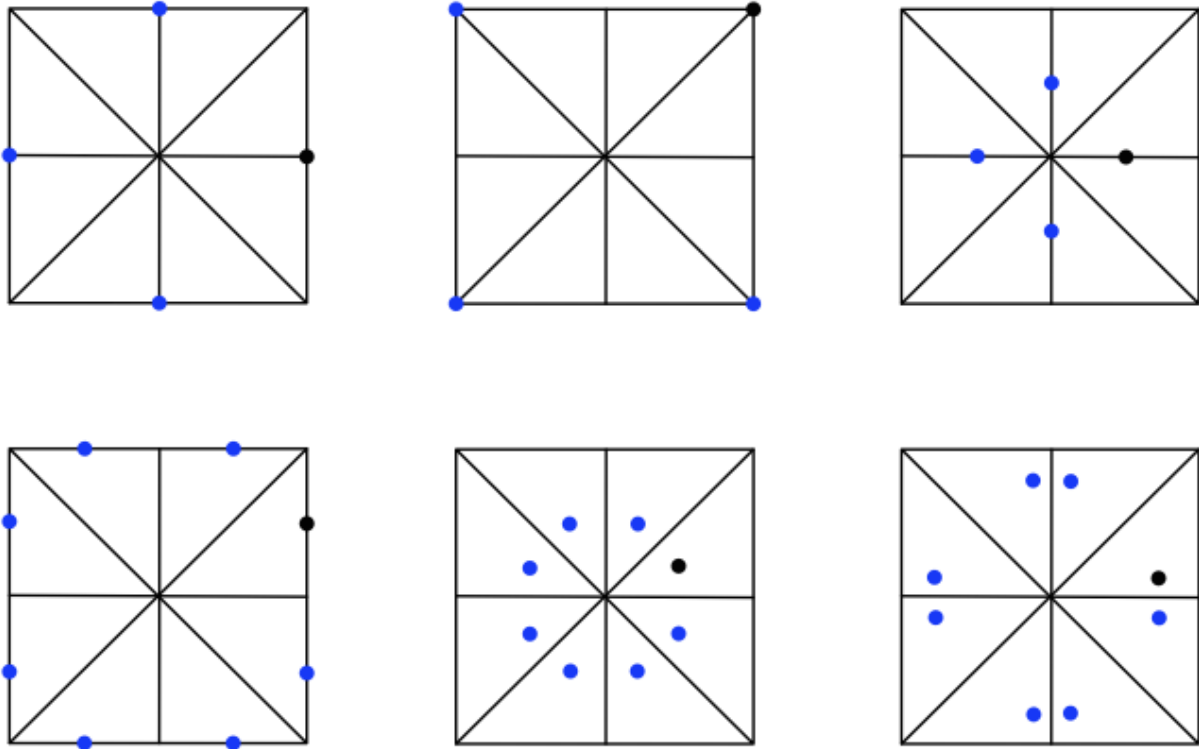
$$\text{stab}_G(5) = \{(1), (12)(34), (13)(24), (14)(23)\} \text{ and } \text{orb}_G(5) = \{5, 6\}$$

58: Let G be the group of rotations of a plane about a point P in the plane. Thinking of G as a group of permutations of the plane, describe the orbit of a point Q in the plane. (This is the motivation for the name “orbit”.)

The orbit of Q is a circle passing through Q with center P .

60: The group D_4 acts as a group of permutations of the square regions shown on page 159. For each square region, locate the points in the orbit of the indicated point under D_4 . In each case, determine the stabilizer of the indicated point.

The black dot below is the original (and included in the orbit), and the blue dots are the rest of the orbit.



Left to right, top to bottom, the stabilizers are $\{id, h\}$, $\{id, d_2\}$, $\{id, h\}$, $\{id\}$, $\{id\}$, $\{id\}$ where id is the identity symmetry, h is the flip across the horizontal line and d_2 is the diagonal from the upper right corner to the bottom left corner.

65: If G is a finite group with fewer than 100 elements and G has subgroups of orders 10 and 25, what is the order of G ?

Let G be as above. Since G has subgroups of orders 10 and 25, the order of G is divisible by both 10 and 25. Hence the order of G is 50.