SOLUTION KEY
Produced by: Kyle Dahlin

Problems:
Chapter 5: 11, 24
Chapter 6: 24
Chapter 7: 1, 2, 6, 8, 18, 30, 42

Problem 5.11. Determine whether the following permutations are even or odd.

a. (135)

b. (1356)

c. (13567)

d. (12)(134)(152)

e. (1243)(3521)

Solution:

a. $(135) = (15)(13)$ is even.

b. $(1356) = (16)(15)(13)$ is odd.

c. $(13567) = (17)(16)(15)(13)$ is even.

d. $(12)(134)(152) = (15)(234) = (15)(24)(23)$ is odd.

e. $(1243)(3521) = (1)(2)(354) = (34)(35)$ is even.

■

Problem 5.24. Suppose that H is a subgroup of S_n of odd order. Prove that H is a subgroup of A_n.

Solution:
Let $\alpha \in H$. Then since $|\alpha|$ divides $|H|$, which is odd, α must have odd order. By Exercise 5.71, α must be an even permutation. Hence $\alpha \in A_n$ and thus $H \leq A_n$. ■

Problem 6.24. Suppose that $\phi : Z_{20} \to Z_{20}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$?

Solution:
Since $5\phi(1) = \phi(5) = 5$, and $\phi(1)$ must be a generator of Z_{20}, the possible automorphisms are defined by where they send 1. The possibilities are $\phi(1) \in \{1, 9, 13, 17\}$ so that the automorphisms are given by $x \mapsto x$, $x \mapsto 9x$, $x \mapsto 13x$ and $x \mapsto 17x$. ■

Problem 7.1. Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4 (see Table 5.1 on page 111).

Solution:
By the Lemma on page 145, $\alpha_1 H = \alpha_2 H = \alpha_3 = \alpha_4 H = H$,
$\alpha_5 H = \alpha_6 H = \alpha_7 H = \alpha_8 H = \{(123), (243), (142), (134)\}$, and
$\alpha_9 H = \alpha_{10} H = \alpha_{11} H = \alpha_{12} H = \{(132), (143), (234), (124)\}$. ■

Problem 7.2. Let H be as in Exercise 1. How many left cosets of H in S_4 are there? (Determine this without listing them.)

Solution:
The number of left cosets of H in S_4 is $[S_4 : H] = |S_4|/|H| = 24/4 = 6$. ■

Problem 7.6. Let n be a positive integer. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$. Find all left cosets of H in $\mathbb{Z}$. How many are there?

Solution:
The left cosets are given by $a+H = \{a, a\pm n, a\pm 2n, a\pm 3n, \ldots\}$. Suppose that $a+H = b+H$. Then there exist $j, k \in \mathbb{Z}$ such that $a + jn = b + kn$ and thus $a - b = (k - j)n$. Hence $a+H = b+H$ if and only if $a \bmod n = b \bmod n$. Thus there are n cosets of H, corresponding to $H, 1 + H, 2 + H, \ldots, (n - 1) + H$. ■

Problem 7.8. Suppose that a has order 15. Find all of the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.

Solution:
$a \langle a^5 \rangle = a^6 \langle a^5 \rangle = a^{11} \langle a^5 \rangle = \{a, a^6, a^{11}\}$,
$a^2 \langle a^5 \rangle = a^7 \langle a^5 \rangle = a^{12} \langle a^5 \rangle = \{a^2, a^7, a^{12}\}$,
$a^3 \langle a^5 \rangle = a^8 \langle a^5 \rangle = a^{13} \langle a^5 \rangle = \{a^3, a^8, a^{13}\}$,
$a^4 \langle a^5 \rangle = a^9 \langle a^5 \rangle = a^{14} \langle a^5 \rangle = \{a^4, a^9, a^{14}\}$,
$a^5 \langle a^5 \rangle = \langle a^5 \rangle = a^{10} \langle a^5 \rangle = \langle a^5 \rangle$. ■

Problem 7.18. Recall that, for any integer n greater than 1, $\phi(n)$ denotes the number of positive integers less than n relatively prime to n. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)} \bmod n = 1$.

Solution:
Let $b = a \bmod n$. Then, b is relatively prime to n and less than n, hence $b \in U(n)$. Since $|U(n)| = \phi(n)$, $b^{\phi(n)} = 1$. By Exercise 0.9, $a^{\phi(n)} \bmod n = b^{\phi(n)} = 1$. ■

Problem 7.30. Let $|G| = 8$. Show that G must have an element of order 2.

Solution:
By Corollary 2 to Lagrange's Theorem, elements of G may have orders of 1, 2, 4, or 8. Let $a \in G$ with $a \neq e$. If $|a| = 8$, then $|a^4| = 8/4 = 2$. If $|a| = 4$, then $|a^2| = 4/2 = 2$. Hence there must always be an element of order 2. ■

Problem 7.42. 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 $g \mapsto g^k$ is one-to-one. If G is also Abelian, show that the mapping given by $g \mapsto g^k$ is an automorphism of G.

Solution:
Since $\gcd(k,n)=1$, there exist $s,t\in\mathbb{Z}$ such that $ks+nt=1$.

Define $\phi(g)=g^k$. Suppose that $\phi(g_1)=\phi(g_2)$.

$$\begin{aligned} g_1^k &= g_2^k \\ g_1^{ks} &= g_2^{ks} \\ g_1^{ks+nt} &= g_2^{ks+nt} \\ g_1 &= g_2 \end{aligned}$$

since for any $g\in G$, $g^{nt}=e$. Hence ϕ is one-to-one.

Now suppose that G is Abelian. We know already that ϕ is one-to-one. Since G is finite and ϕ is a one-to-one self-map, it must also be onto.

It remains to show that ϕ is a homomorphism. Let $g,h\in G$ be arbitrary. Then $\phi(gh)=(gh)^k=g^kh^k=\phi(g)\phi(h)$, since G is Abelian. Hence ϕ is an automorphism. ■