SOLUTION KEY
Produced by: Kyle Dahlin

Problem 3.42. Let G be a group and let $H \leq G$. Define $C(H) = \{x \in G | xh = hx \text{ for all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

Solution:
Clearly $e \in C(H)$. Now suppose that $a, b \in C(H)$. Let $h \in H$ be arbitrary. Since H is a subgroup, we know that $h^{-1} \in H$. Hence,

$$(ab^{-1})h = a(b^{-1}h) = a(h^{-1}b)^{-1} = a(bh^{-1})^{-1} = ahb^{-1} = h(ab^{-1})$$

Thus $ab^{-1} \in C(H)$ and by Theorem 3.1, $C(H)$ is a subgroup. ■

Problem 3.52. Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2, \mathbb{R})$. Find $|A|$, $|B|$, and $|AB|$.

Solution:
We'll just do the computations and see what we get:

$$\begin{aligned} A^2 &= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\ A^3 &= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \\ A^4 &= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \end{aligned}$$

So that $|A| = 4$. Now for B:

$$\begin{aligned} B^2 &= \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \\ &= \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \\ B^3 &= \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \end{aligned}$$

Hence $|B| = 3$. Now $AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. We will use the following claim to show that AB has infinite order.

Claim: $(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

Proof: We proceed by induction. The base case, $(AB)^1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, is clear. Now suppose that $(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. Then

$$\begin{aligned}(AB)^{n+1} &= \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1+n \\ 0 & 1 \end{bmatrix}\end{aligned}$$

Hence since $n+1 \neq 0$ for any $n \in \mathbb{N}$, the order of AB is infinite. ■

Comment: Checking that $A^3 \neq I$ is actually not necessary. Why is it sufficient to check that $A^4 = (A^2)^2 = I$ in order to prove that $|A| = 4$.

If instead A and B have elements from a group with finite order, say $A, B \in SL(2, Z_{12})$, what would the order of AB be?

Problem 3.58. $U(15)$ has six cyclic subgroups. List them.

Solution:
The elements of $U(15)$ are $1, 2, 4, 7, 8, 11, 13, 14$. The cyclic subgroups generated by a single element are:

1. $\{1\}$, the trivial subgroup
2. $\langle 2 \rangle = \{1, 2, 4, 8\} = \langle 8 \rangle$
3. $\langle 4 \rangle = \{1, 4\}$
4. $\langle 7 \rangle = \{1, 4, 7, 13\} = \langle 13 \rangle$
5. $\langle 11 \rangle = \{1, 11\}$
6. $\langle 14 \rangle = \{1, 14\}$

■

Problem 4.2. Suppose that $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are cyclic groups of order 6, 8, and 20, respectively. Find all generators of $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$.

Solution:
Corollary 1 on page 79 tells us that if $|\langle a \rangle| = 6$ then $|a| = 6$. Then by Corollary 3 on page 81, $\langle a \rangle = \langle a^i \rangle$ if and only if $\gcd(6, i) = \gcd(6, 1) = 1$. The set of numbers less than 6 that are relatively prime to 6 are 1 and 5. Hence

$$\langle a \rangle = \left\langle a^5 \right\rangle.$$

We can follow the same process for b and c to get

$$\langle b \rangle = \left\langle b^3 \right\rangle = \left\langle b^5 \right\rangle = \left\langle b^7 \right\rangle$$

and
$$\langle c\rangle = \left\langle c^3\right\rangle = \left\langle c^7\right\rangle = \left\langle c^9\right\rangle = \left\langle c^{11}\right\rangle = \left\langle c^{13}\right\rangle = \left\langle c^{17}\right\rangle = \left\langle c^{19}\right\rangle.$$

■

Comment: Notice that the powers of a for the generators of $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$ have exponents that belong to $U(6)$, $U(8)$, and $U(20)$, respectively.

Problem 4.8. Let a be an element of a group G and let $|a| = 15$. Compute the orders of the following elements of G.

a. a^3, a^6, a^9, a^{12}

b. a^5, a^{10}

c. a^2, a^4, a^8, a^{14}

Solution:

a. a^3, a^6, a^9, a^{12}
Notice that each of these elements, a^i, have the property that $\gcd(15, i) = \gcd(15, 3) = 3$. Thus they must all have the same order as a^3, by Corollary 2 on page 81. Therefore they all have order $15/\gcd(15, 3) = 5$ by Theorem 4.2.

b. a^5, a^{10}
As above, these both have the same order as a^5: $|a^5| = 15/\gcd(15, 5) = 3$.

c. a^2, a^4, a^8, a^{14}
As above, these all have the same order as a^2: $|a^2| = 15/\gcd(15, 2) = 15$

■

Problem 4.10. In Z_{24}, list all generators for the subgroup of order 8. Let $G = \langle a\rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.

Solution:
By the Corollary on page 84, the set $\langle 24/8\rangle = \langle 3\rangle$ is the unique subgroup of Z_{24} of order 8. By Corollary 2 on page 81, this subgroup is also generated by the numbers i such that $\gcd(24, i) = \gcd(24, 3)$, namely $\{3, 9, 15, 21\}$.

Since G is cyclic of order $24 = 8 \times 3$, by Theorem 4.3 it has exactly one subgroup of order 8, namely $\langle a^3\rangle$. By Corollary 2 on page 81, the other generators are given by a^i where $\gcd(24, i) = \gcd(24, 3)$, that is a^3, a^9, a^{15}, a^{21}. ■

Problem 4.41. Suppose that a and b are group elements that commute and have orders m and n. If $\langle a\rangle \cap \langle b\rangle = \{e\}$, prove that the group contains an element whose order is the least common multiple of m and n. Show that this need not be true if a and b do not commute.

Solution:
Consider the element ab. Since a and b commute, powers of ab have the form $a^i b^i$ for $i \in \mathbb{Z}$. Let $l = \operatorname{lcm}(m, n)$ and let $r = |ab|$. We will show that $l = r$.

Since $(ab)^r = a^r b^r = e$, we have that $a^r = b^{-r}$ and hence $a^r = e$ because

$$a^r \in \langle a \rangle \cap \langle b \rangle = \{e\}.$$

So $|a| = m$ divides r and, by a similar argument, n divides r. Hence r is a common multiple of m and n, so that l divides r.

Now since $l = jm = kn$ for some $j, k \in \mathbb{Z}$, we get that

$$(ab)^l = a^l b^l = a^{jm} b^{kn} = (a^m)^j (b^n)^k = e.$$

Hence $r = |ab|$ divides l and because $r, l > 0$, we have that $r = l$.

Consider now the group D_3, where F is a reflection. We have shown before that $|F| = 2$, $|R_{120}| = 3$, and $FR_{120} = R_{240}F$, so that these elements do not commute. We know that $|D_3| = 6 = \operatorname{lcm}(2, 3)$ but that D_3 is not cyclic, meaning there can be no element of D_3 of order 6. ■

Problem 4.62. Given the fact that $U(49)$ is cyclic and has 42 elements, deduce the number of generators that $U(49)$ has without actually finding any of the generators.

Solution:
Let a be an arbitrary generator of $U(49)$. For $j \in \mathbb{N}$, $\langle a^j \rangle = \langle a \rangle = U(49)$ if and only if $\gcd(42, j) = 1$ by Corollary 3 on page 81. Since $U(49)$ is cyclic with order 42, we only need find the number of values of j less than 42 and relatively prime to 42. This is exactly $\phi(42) = \phi(7)\phi(3)\phi(2) = 6 \cdot 2 \cdot 1 = 12$.

The list of possible values of j is: $1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$. ■

Problem 4.64. Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Solution:
Let $c \in \langle a \rangle \cap \langle b \rangle$. Then $c = a^j = b^k$ for some $j, k \in \mathbb{Z}$. Now $c^{|a|} = (a^j)^{|a|} = (a^{|a|})^j = e$ and similarly $c^{|b|} = e$. Hence $|c|$ divides both $|a|$ and $|b|$. Since $|a|$ and $|b|$ are relatively prime, $|c| = 1$ and therefore $c = e$. ■

Comment: Alternately, since there exist $s, t \in \mathbb{Z}$ with $|a|s + |b|t = 1$, we immediately get that

$$c = c^{|a|s+|b|t} = (c^{|a|})^s (c^{|b|})^t = e$$

.

Problem 4.72. Let a be a group element such that $|a| = 48$. For each part, find a divisor k of 48 such that

a. $\langle a^{21} \rangle = \langle a^k \rangle$;

b. $\langle a^{14} \rangle = \langle a^k \rangle$;

c. $\langle a^{18} \rangle = \langle a^k \rangle$.

Solution:
We will use Corollary 2 on page 81 throughout this problem. This Corollary tells us that $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(48, i) = \gcd(48, j)$.

a. $\langle a^{21} \rangle = \left\langle a^k \right\rangle$;
We seek numbers k such that $\gcd(48, k) = \gcd(48, 21) = 3$. Clearly $k = 3$ works.

b. $\langle a^{14} \rangle = \left\langle a^k \right\rangle$;
We seek numbers k such that $\gcd(48, k) = \gcd(48, 14) = 2$. Clearly $k = 2$ works.

c. $\langle a^{18} \rangle = \left\langle a^k \right\rangle$.
We seek numbers k such that $\gcd(48, k) = \gcd(48, 18) = 6$. Clearly $k = 6$ works.

■

Problem 4.85. Prove that for any prime p and positive integer n, $\phi(p^n) = p^n - p^{n-1}$.

Solution:
Since p is prime, the only positive integers $k < p^n$ with $\gcd(p^n, k) \neq 1$ are integers of the form mp where $0 < m \leq p^{n-1} - 1$. There are precisely $p^{n-1} - 1$ such integers. There are exactly $p^n - 1$ integers strictly between 0 and p^n. Hence $\phi(p^n)$, the number of positive integers less than and relatively prime to p^n, must be: $p^n - 1 - (p^{n-1} - 1) = p^n - p^{n-1}$. ■