Math 465 - Homework 3

SOLUTIONS

Prof. Arturo Magidin

1. Let G be a group, and let $a, x \in G$.

   (i) Prove that for every integer n,
   $$(axa^{-1})^n = ax^n a^{-1}.$$
   SUGGESTION: Use induction on n to prove it for $n \geq 0$, then take inverses to prove it for negative n.

   Proof. Following the suggestion: the result holds for $n = 0$, since $(axa^{-1})^0 = e$, and $ax^0a^{-1} = aea^{-1} = aa^{-1} = e$.

   The result also holds for $n = 1$, as both sides of the equation equal axa^{-1}. Let $k \geq 1$.

   INDUCTIVE HYPOTHESIS: Assume that $(axa^{-1})^k = ax^k a^{-1}$.

   We want to show that $(axa^{-1})^{k+1} = ax^{k+1}a^{-1}$. We have:
   $$\begin{aligned}
   (axa^{-1})^{k+1} &= (axa^{-1})^k(axa^{-1}) && \text{(by definition)}\\
   &= (ax^ka^{-1})(axa^{-1}) && \text{(by the Induction Hypothesis)}\\
   &= ax^ka^{-1}axa^{-1}\\
   &= ax^kxa^{-1} && \text{(since } a^{-1}a \text{ cancels out)}\\
   &= ax^{k+1}a^{-1},
   \end{aligned}$$
   as we needed to show. This completes the inductive step, and thus the induction. Hence, we know the formula holds for all positive integers n.

   Now let $n < 0$, and write $n = -m$ with $m > 0$. Using the formula for the inverse of a product, we have:
   $$\begin{aligned}
   (axa^{-1})^n = (axa^{-1})^{-m} &= \big((axa^{-1})^m\big)^{-1} = \big(ax^ma^{-1}\big)^{-1}\\
   &= (a^{-1})^{-1}(x^m)^{-1}a^{-1} = ax^{-m}a^{-1} = ax^na^{-1}.
   \end{aligned}$$
   This proves the equality for every integer n, as desired.

   (ii) Let G be a group, $a, x \in G$. Prove that $|x| = |axa^{-1}|$. SUGGESTION: Show that the set of k for which $x^k = e$ is the same as the set of k for which $(axa^{-1})^k = e$.

   Proof. Since $(axa^{-1})^k = ax^ka^{-1}$, by Problem 1 we have that if $x^m = e$, then we also have $(axa^{-1})^m = ax^ma^{-1} = aea^{-1} = e$. Therefore,
   $$\{k \in \mathbb{Z} \mid x^k = e\} \subseteq \{k \in \mathbb{Z} \mid (axa^{-1})^k = e\}.$$
   Conversely, if $(axa^{-1})^m = e$, then $ax^ma^{-1} = e$. Multiplying by a^{-1} on the left and a on the right, we get $x^m = a^{-1}ea = e$. So
   $$\{k \in \mathbb{Z} \mid (axa^{-1})^k = e\} \subseteq \{k \in \mathbb{Z} \mid x^k = e\}.$$
   Thus, the two sets are equal.

   Therefore, either both sets are just $\{0\}$, and then $|x| = |axa^{-1}| = \infty$; or both sets have the same smallest element n, and $|x| = |axa^{-1}| = n$. In either case, $|x| = |axa^{-1}|$. □

   REMARK. An alternative argument is the following: after we have proven the inclusion $\{k \in \mathbb{Z} \mid x^k = e\} \subseteq \{k \in \mathbb{Z} \mid (axa^{-1})^k = e\}$, we can now replace x with axa^{-1}, and a with a^{-1}. Then the same argument shows that
   $$\{k \in \mathbb{Z} \mid (axa^{-1})^k = e\} \subseteq \{k \in \mathbb{Z} \mid a^{-1}(axa^{-1})^ka = e\}.$$
   But $a^{-1}(axa^{-1})^ka = a^{-1}(ax^ka^{-1})a = x^k$, we in fact we obtain the reverse inclusion this way.

2. If $n > 2$ and n is even, show that D_n has a subgroup of order 4.

   Answer. Because n is even, we know that the rotation by 180° is an element of D_n and lies in $Z(D_n)$, so it commutes with every element of D_n. Call this rotation R_{180}. If F is *any* reflection, then I claim that $H = \{I, R_{180}, F, R_{180}F\}$ is a subgroup of D_n.

   Indeed, the set is nonempty; each element is its own inverse, so the set is closed under inverses. As for products of two elements, remembering that R_{180} commutes with F; and that the square of any element is equal to I, we only need to verify that the product of $R_{180}F$ with both F and R_{180} lies in the set; and indeed, we have:

$$(R_{180}F)F = R_{180}(FF) = R_{180}, \qquad (R_{180}F)R_{180} = R_{180}(R_{180}F) = (R_{180}R_{180})F = F.$$

   So all the products of two elements of H are in H. Thus, H is a subgroup of D_n, and H has order 4. □

3. Let G a group, and let H, K be subgroups. Show that if $hk = kh$ for every $h \in H$ and $k \in K$, then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G.

   Proof. The set is not empty, since neither H nor K are empty. Now let $h_1k_1, h_2k_2 \in HK$, with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. We want to show that $(h_1k_1)(h_2k_2)^{-1} \in HK$. We have:

$$\begin{aligned}(h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\ &= h_1(k_1k_2^{-1})h_2^{-1} \\ &= h_1h_2^{-1}(k_1k_2^{-1}) \qquad \text{(because } k_1k_2^{-1} \in K, h_2^{-1} \in H\text{, so they commute)} \\ &= (h_1h_2^{-1})(k_1k_2^{-1}).\end{aligned}$$

   But this product lies in HK, since $h_1h_2^{-1} \in H$ (because H Is a subgroup and $h_1, h_2 \in H$), and $k_1k_2^{-1} \in K$ (because $k_1, k_2 \in K$ and K is a subgroup).

   By the "One-Step subgroup test", HK is a subgroup of G. □

4. (i) Find all the generators of the groups $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.

   Answer. An integer k, $1 \leq k < 6$ generates $\mathbb{Z}_6$ if and only if $\gcd(k, 6) = 1$. So the two generators are 1 and 5.

   Similarly, the generators of $\mathbb{Z}_8$ are the integers k with $1 \leq k < 8$ and $\gcd(k, 8) = 1$, namely 1, 3, 5, and 7.

   For $\mathbb{Z}_{20}$, we take the integers k, $1 \leq k < 20$ that are relatively prime to 20: 1, 3, 7, 9, 11, 13, 17, and 19. □

   (ii) Let $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$ be cyclic groups of order 6, 8, and 20, respectively. Find all the generators of $\langle a\rangle$, of $\langle b\rangle$, and of $\langle c\rangle$.

   Answer. If $|x| = n$, then x^k generates $\langle x\rangle$ if and only if $\gcd(k, n) = 1$. So the answers look similar to those above:

   The generators of $\langle a\rangle$ are a and a^5.

   The generators of $\langle b\rangle$ are b, b^3, b^5, and b^7.

   The generators of $\langle c\rangle$ are c, c^3, c^7, c^9, c^{11}, c^{13}, c^{17}, and c^{19}. □

5. Let G be a group, and let $a \in G$ be an element with $|a| = 15$. Compute the orders of each of the following elements of G:

   (i) a^3, a^6, a^9, and a^{12}.

   Answer. We know the order of a^k is $\frac{15}{\gcd(15,k)}$. Since

$$\gcd(15, 3) = \gcd(15, 6) = \gcd(15, 9) = \gcd(15, 12) = 3,$$

   we have that all four of these elements have order $\frac{15}{3} = 5$.

(ii) a^5 and a^{10}.

Answer. Since $\gcd(15,5) = \gcd(15,10) = 5$, the orders of both a^5 and a^{10} are both $\frac{15}{5} = 3$.

(iii) a^2, a^4, a^8, and a^{14}.

Answer. Since $\gcd(15,2) = \gcd(15,4) = \gcd(15,8) = \gcd(15,14) = 1$, all of these elements have order 15. □

6. In $\mathbb{Z}$, find all generators of the subgroup $\langle 3 \rangle$.

Answer. Because $|3| = \infty$ in $\mathbb{Z}$, we know that the only generators of $\langle 3 \rangle$ are 3 and -3. □

7. In $\mathbb{Z}$, find a generator for the subgroup $\langle 10 \rangle \cap \langle 12 \rangle$.

Answer. The subgroup $\langle 10 \rangle \cap \langle 12 \rangle$ is the subgroup of all elements that are both multiples of 10 and multiples of 12. As the least common multiple of 10 and 12 is $\frac{(10)(12)}{\gcd(10,12)} = \frac{120}{2} = 60$, we have $\langle 10 \rangle \cap \langle 12 \rangle = \langle 60 \rangle$, and so a generator is 60. (The only other generator is -60.)

8. In $\mathbb{Z}$, show that $\langle n \rangle \subseteq \langle m \rangle$ if and only if m divides n.

Proof. If $\langle n \rangle \subseteq \langle m \rangle$, then $n \in \langle n \rangle \subseteq \langle m \rangle$, so n must be a multiple of m; that is, m divides n.

Conversely, if m divides n, then we can write $n = mk$, and so $n \in \langle m \rangle$. Therefore, the cyclic subgroup generated by n is a subgroup of $\langle m \rangle$, so $\langle n \rangle \subseteq \langle m \rangle$, as desired. □

9. In $\mathbb{Z}$, if $n, m \in \mathbb{Z}$, what is a generator for $\langle n \rangle \cap \langle m \rangle$?

Answer. We know that $\langle n \rangle \cap \langle m \rangle$ is a subgroup of $\mathbb{Z}$ (a cyclic group), so it is cyclic. That is, there is an integer k such that $\langle n \rangle \cap \langle m \rangle = \langle k \rangle$. Because $\langle k \rangle \subseteq \langle n \rangle$, By Problem 8 we have that k is a multiple of n. Symmetrically, k is a multiple of m. So k is a common multiple of n and m.

And if r is any common multiple of n and m, then $r \in \langle n \rangle \cap \langle m \rangle$, so $\langle r \rangle \subseteq \langle n \rangle \cap \langle m \rangle = \langle k \rangle$, which again by Problem 8 tells us that r is a multiple of k.

So a generator of $\langle n \rangle \cap \langle m \rangle$ is a common multiple of m and n that divides any other common multiple of m and n; this is the least common multiple of m and n. Thus, we conclude that $\langle n \rangle \cap \langle m \rangle$ is generated by $\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)}$. □

10. Let G be an Abelian group, and let $H = \{g \in G \mid |g| \text{ divides } 12\}$.

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

Proof. Since $|e| = 1$, we have that $e \in H$.

Now assume that $x, y \in H$, so that $|x|$ divides 12 and $|y|$ divides 12. This implies that $x^{12} = y^{12} = e$. We want to prove that $|xy^{-1}|$ divides 12, and to that end it is enough to show that $(xy^{-1})^{12} = e$. Indeed, because G is Abelian, we know that

$$(xy^{-1})^{12} = x^{12}(y^{-1})^{12} = x^{12}(y^{12})^{-1} = ee = e.$$

Therefore, $xy^{-1} \in H$. By the One-Step subgroup test, it follows that H is a subgroup of G. □

(ii) Is there anything special about 12, or would your proof be valid if 12 were replaced by some other positive integer?

Answer. There is nothing special about 12: we used that $|e| = 1$ divides 12, and that if $|a|$ divides 12, then $a^{12} = e$. This will also work for any positive integer n.

(iii) State the general result derived from your answer of (ii).

Answer. "Let G be an Abelian group, let n be a positive integer, and let

$$H = \{g \in G \mid |g| \text{ divdes } n\}.$$

Then H is a subgroup of G."

Note that it is possible that, for some values of n we will have $H = \{e\}$; that is, that no element of G other than e will have order dividing n. But that still yields a subgroup.