Math 465 - Homework 2
SOLUTIONS
Prof. Arturo Magidin

1. Let G be a group with operation $\cdot$. We define THE OPPOSITE GROUP G^{op}, by taking the same underlying set as G, and defining the operation $\odot\colon G\times G\to G$ by

$$a\odot b = b\cdot a.$$

   (i) Prove that G^{op} is a group.

   Proof. From the definition it is clear that $\odot$ is an operation on G. To show it is associative, let $a,b,c\in G$. Then

$$\begin{aligned} a\odot(b\odot c) &= a\odot(c\cdot b) = (c\cdot b)\cdot a = c\cdot(b\cdot a) \qquad \text{(because } \cdot \text{ is associative)}\\ &= (b\cdot a)\odot c = (a\odot b)\odot c. \end{aligned}$$

   So we conclude that $\odot$ is associative.

   If e is the identity of G, then it is also the identity of G^{op}: for $a\odot e = e\cdot a = a$, and $e\odot a = a\cdot e = a$.

   And if $a\in G$, then its inverse a^{-1} under $\cdot$ is also an inverse under $\odot$: $a\odot a^{-1} = a^{-1}\cdot a = e$ and $a^{-1}\odot a = a\cdot a^{-1} = e$.

   Thus, G^{op} is a group. □

   (ii) Prove that $(G^{\mathrm{op}})^{\mathrm{op}} = G$.

   Proof. Say we denote the operation of $(G^{\mathrm{op}})^{\mathrm{op}}$ by $\otimes$. So $a\otimes b = b\odot a$. But

$$a\otimes b = b\odot a = a\cdot b,$$

   so for all $a,b\in G$, $a\otimes b = a\cdot b$. So the operation on $(G^{\mathrm{op}})^{\mathrm{op}}$ is the same as the operation on G. Same set and same operation on the set, so $(G^{\mathrm{op}})^{\mathrm{op}} = G$. □

2. Let G be a group. Prove that G is Abelian if and only if for every $a,b\in G$, we have that $(ab)^{-1} = a^{-1}b^{-1}$.

   Proof. We know that we always have $(xy)^{-1} = y^{-1}x^{-1}$.

   If G is Abelian, then $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ holds for all $a,b\in G$, since a^{-1} commutes with b^{-1}.

   Conversely, if we always have that $(ab)^{-1} = a^{-1}b^{-1}$, then taking inverses again we have

$$ab = ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba.$$

   So we conclude that for any $a,b\in G$, we have $ab = ba$. Thus, G is Abelian. □

3. Let G be a group, and $a,b\in G$. Prove that if $(ab)^2 = a^2b^2$, then $ab = ba$.

   Proof. Expanding $(ab)^2$, a^2, and b^2, we have $abab = aabb$. Then we can cancel an a on the left and a b on the right to obtain $ba = ab$, as desired. □

4. Let G be a group. Prove that if $g^2 = e$ for every $g\in G$, then G is Abelian (that is, for all $a,b\in G$, $ab = ba$).

   Proof. Let $a,b\in G$. Then $(ab)^2 = e$ because $ab\in G$ and the square of any element in G is the identity; and $a^2 = b^2 = e$ for the same reasons. But that means that $a^2b^2 = ee = e$. Therefore, $(ab)^2 = e = a^2b^2$.

   So we can conclude that $(ab)^2 = a^2b^2$. By Problem 3, it follows that $ab = ba$. Since a and b were arbitrary, we see that any two elements of G commute, so G is Abelian, as claimed. □

5. Determine the order of each element of $U(14)$.

   Answer. I will use $\equiv$ when we have an equality modulo 14.

   The elements of $U(14)$ are

   $$U(14) = \{1, 3, 5, 9, 11, 13\}.$$

   Listing the powers until we get 1 modulo 14 (at each step we can just multiply the previous reduced result; for example, we don't actually have to compute 3^5 and then reduce modulo 14; since $3^4 \equiv 11$ modulo 14, then $3^5 = 3(3^4) \equiv 3(11) = 33$ modulo 14), we have:

   - $|1| = 1$.
   - 3, $3^2 = 9$, $3^3 = 27 \equiv 13$, $3^4 \equiv 39 \equiv 11$, $3^5 \equiv 33 \equiv 5$, $3^6 \equiv 15 \equiv 1$. So $|3| = 6$.
   - 5, $5^2 = 25 \equiv 11$, $5^3 \equiv 55 \equiv 13$, $5^4 \equiv 65 \equiv 9$, $5^5 \equiv 45 \equiv 3$, $5^6 \equiv 15 \equiv 1$. Thus, we also have $|5| = 6$.
   - 9, $9^2 = 81 \equiv 11$, $9^3 \equiv 99 \equiv 1$, so $|9| = 3$.
   - 11, $11^2 = 121 \equiv 9$, $11^3 \equiv 99 \equiv 1$, and we again have $|11| = 3$.
   - 13, $13^2 = 169 \equiv 1$, so $|13| = 2$.

6. In the group $\mathbb{Z}_{12}$ of integers modulo 12 under addition modulo 12, find $|a|$, $|b|$, and $|a+b|$ in each of the following cases:

   (a) $a = 6$, $b = 2$;

   Answer. Since $a + a = 0$ in $\mathbb{Z}_{12}$, we have $|a| = 2$; and the smallest positive multiple of b that is a multiple of 12 is $6b$, so $|b| = 6$.

   Meanwhile, $a+b = 8$; the smallest positive multiple of 8 that is divisible by 12 is $24 = (3)(8)$, so $|a + b| = 3$.

   (b) $a = 3$, $b = 8$;

   Answer. Here we have $|a| = 4$, $|b| = 6$. and $a + b = 11$; the smallest positive multiple of 11 that is divisible by 12 is $(12)(11)$, so $|a + b| = 12$.

   (c) $a = 5$, $b = 4$.

   Answer. Here we have $|a| = 12$ and $|b| = 3$; the smallest positive multiple of $a + b = 9$ that is divisible by 12 is $(3)(9) = 36$, so $|a + b| = 3$.

7. Let G be a group, and let $a \in G$. Prove that $|a| = |a^{-1}|$, meaning that either they are both infinite, or they are both finite and equal to each other.

   Proof. If $a^n = e$, then $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. So

   $$\{k \in \mathbb{Z} \mid a^k = e\} \subseteq \{k \in \mathbb{Z} \mid (a^{-1})^k = e\}.$$

   Applying the same argument now to a^{-1}, and noting that $(a^{-1})^{-1} = a$, we conclude that the other inclusion also holds, so

   $$\{k \in \mathbb{Z} \mid a^k = e\} = \{k \in \mathbb{Z} \mid (a^{-1})^k = e\}. \tag{1}$$

   Since $|a| = \infty$ if and only if the set on the left of (1) consists only of 0; that is, is $\{0\}$; and similarly for a^{-1}. It follows that $|a| = \infty$ if and only if $|a^{-1}| = \infty$. And $|a| = n > 0$ if and only if the least positive integer in the set on the left of (1) is n, and similarly for a^{-1}, so if $|a|$ is finite, then $|a| = |a^{-1}|$ and likewise the converse. □

8. Let G be a group, and let $a, b \in G$. Prove that $|ab| = |ba|$, meaning that either they are both infinite, or they are both finite and equal to each other.

Proof. We claim that $(ab)^{n+1} = a(ba)^n b$ for all $n > 0$. We prove it by Induction on n. For $n = 1$, we have $(ab)^2 = a(ba)^1 b$, which holds. For the Inductive Step, assume that $(ab)^{k+1} = a(ba)^k b$ holds; we want to prove that $(ab)^{k+2} = a(ba)^{k+1} b$. We have

$$(ab)^{k+2} = (ab)(ab)^{k+1} = ab\left(a(ba)^k b\right) = a(ba)(ba)^k b = a(ba)^{k+1} b,$$

as required.

If $(ba)^n = e$, then $(ab)^{n+1} = a(ba)^n b = ab$. Therefore, $(ab)^{n+1} = ab$. Cancelling one ab, we obtain $(ab)^n = e$. That is, if $(ba)^n = e$, then $(ab)^n = e$. Exchanging the roles of a and b, we also obtain that if $(ab)^m = e$ then $(ba)^m = e$. Therefore,

$$\{k \in \mathbb{Z} \mid (ab)^k = e\} = \{k \in \mathbb{Z} \mid (ba)^k = e\}.$$

Since the two sets are equal, then arguing as we did in problem 7 we conclude that either both $|ab|$ and $|ba|$ are infinite, or else they are both finite and equal to each other, which is what we wanted to prove. □

9. Let $G = D_4$ be the dihedral group of order 8.

(a) Show that for every $g \in G$, we have $g^4 = R_0$ (the identity of G).

Proof. For the rotations, we have $R_{180}^2 = R_0$, so $(R_{180})^4 = R_0$; and $(R_{90})^2 = (R_{270})^2 = R_{180}$, so $(R_{90})^4 = (R_{270})^4 = (R_{180})^2 = R_0$

For each reflection we have that the square equals R_0, and therefore the fourth power equals R_0 as well. So $g^4 = R_0$ for every $g \in D_4$. □

(b) Show that for every $a, b \in G$, we have $(ab)^4 = a^4 b^4$.

Proof. Since the fourth power of any element of G equals R_0, we have $(ab)^4 = R_0$ for all $a, b \in G$; and $a^4 b^4 = R_0 R_0 = R_0$. Thus,

$$(ab)^4 = R_0 = a^4 b^4$$

holds for every $a, b \in G$.

(c) Show that G is not Abelian.

Proof. As we saw in class in the Cayley table, the result of doing a rotation of 90° and then a horizontal reflection is different from the result of first doing a horizontal reflection and then a rotation of 90°. One results in the reflection we called D, and the other in the reflection we called D'.

Alternatively, using the notation we saw in class, we have that if F is any reflection and R is the rotation by 90°, then $FR = R^{-1}F$, which cannot equal RF because $R \neq R^{-1}$. So $FR \neq RF$, proving the group is not abelian. □

Remark. Thinking about Problem 3 above, we see that if $(ab)^2 = a^2 b^2$ for every $a, b \in G$, then G is Abelian. Likewise, from Problem 2 we see that if $(ab)^{-1} = a^{-1} b^{-1}$ always holds, then G is Abelian. So one might wonder if for other values we might have that if $(ab)^n = a^n b^n$ always holds, then G will be Abelian. The answer is "no"; this problem shows that certainly $(ab)^4 = a^4 b^4$ does not suffice; in fact, there are examples for every n, $n \neq 2$, $n \neq -1$, of groups G in which $(ab)^n = a^n b^n$ always holds, but G is not Abelian.