Solutions: Homework 4

February 20, 2020

Problem 1. Find all cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.

Proof. Firstly, we notice that since $\mathbb{Z}$ is abelian, the left cosets and the right cosets are the same. So, we just find the left cosets of $4\mathbb{Z}$ in $\mathbb{Z}$. We start with the coset generated by the identity element, i.e.

$$0 + 4\mathbb{Z} = \{..., -8, -4, 0, 4, 8, ...\} = 4\mathbb{Z}$$

Now, $1 \notin 4\mathbb{Z}$. So, we look at the coset containing 1, i.e.

$$1 + 4\mathbb{Z} = \{..., -7, -3, 1, 5, 9, ...\}$$

Now, 2 is not in any of the two cosets we got above. So, we look at the coset containing 2, i.e.

$$2 + 4\mathbb{Z} = \{..., -6, -2, 2, 6, 10, ...\}$$

Now, 3 is not in any of the three cosets we got above. So, we look at the coset containing 3, i.e.

$$3 + 4\mathbb{Z} = \{..., -5, -1, 3, 7, 11, ...\}$$

Now, we observe that all the elements of $\mathbb{Z}$ are in one of the 4 cosets we got above. To see that, let n be any integer. Then, by the division algorithm, $n = 4q + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r \leq 3$. Then, notice that $n \in r + 4\mathbb{Z}$, which is one of the cosets that we got above. So, the cosets of $4\mathbb{Z}$ in $\mathbb{Z}$ are $0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}$ and $3 + 4\mathbb{Z}$. □

Problem 2. Find all cosets of the subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.

Proof. Let $H = \langle 4 \rangle = \{0, 4, 8\}$. Firstly, we notice that since $\mathbb{Z}_{12}$ is abelian, the left cosets and the right cosets are the same. So, we just find the left cosets of H in $\mathbb{Z}_{12}$. We start with the coset generated by the identity element, i.e.

$$0 + H = \{0, 4, 8\} = H.$$

Now, $1 \notin H$. So, we look at the coset containing 1, i.e.

$$1 + H = \{1, 5, 9\}$$

Now, 2 is not in any of the two cosets we got above. So, we look at the coset containing 2, i.e.

$$2 + H = \{2, 6, 10\}$$

Now, 3 is not in any of the three cosets we got above. So, we look at the coset containing 3, i.e.

$$3 + H = \{3, 7, 11\}$$

Now, we observe that all the elements of $\mathbb{Z}_{12}$ are in one of the 4 cosets we got above. So, the cosets of H in $\mathbb{Z}_{12}$ are $0 + H, 1 + H, 2 + H$ and $3 + H$. □

Problem 3. (a) Find all the left cosets of $\langle(1234)\rangle$ in S_4.
(b) Find the index of $\langle(1254)(23)\rangle$ in S_5.
(b) Find the index of $\langle(1245)(36)\rangle$ in S_6.

Proof. (a) Let $H = \langle(1234)\rangle = \{e, (1234), (13)(24), (1432)\}$. We start with the left coset generated by the identity element, i.e.

$$eH = \{e, (1234), (13)(24), (1432)\} = H.$$

Now, $(12) \notin H$. So, we look at the coset containing (12), i.e.

$$(12)H = \{(12), (234), (1324), (143)\}$$

Now, (13) is not in any of the two cosets we got above. So, we look at the coset containing (13), i.e.

$$(13)H = \{(13), (12)(34), (24), (14)(23)\}$$

Now, (14) is not in any of the three cosets we got above. So, we look at the coset containing (14), i.e.

$$(14)H = \{(14), (123), (1342), (243)\}$$

Now, (23) is not in any of the four cosets we got above. So, we look at the coset containing (23), i.e.

$$(23)H = \{(23), (134), (1243), (142)\}$$

Now, note that the number of left cosets of H is S_4 is $|S_4|/|H| = 24/4 = 6$, and note that (34) is not in any of the five cosets above. So, the last coset should be the one containing (34). So, the left cosets of H in S_4 are $H, (12)H, (13)H, (14)H, (23)H$ and $(34)H$.
(b) Note that $(1254)(23) = (12354)$ and so, $|\langle(1254)(23)\rangle| = 5$. So, the index of $\langle(1254)(23)\rangle$ in S_5 is $|S_5|/|\langle(1254)(23)\rangle| = 120/5 = 24$.
(c) $|\langle(1245)(36)\rangle| = \text{lcm}(4, 2) = 4$. So, the index of $\langle(1245)(36)\rangle$ in S_6 is $|S_6|/|\langle(1245)(36)\rangle| = 720/4 = 180$. □

Problem 4. In class, we defined the group $(M_n, \cdot_n)$ where $M_n = \{a \in \mathbb{Z}_n | \gcd(a, n) = 1\}$ and $\cdot_n$ is multiplication modulo n.
(a) Show that, for $n \geq 2$, $H = \{1, n - 1\}$ is a subgroup of M_n.
(b) Find the cosets of H in M_8.
(c) Use part (a) to show that, for any $n \geq 3$, M_n always has even order.

Proof. (a) Clearly, $1 \in H$ by the definition of H. Note that $(n-1)^2 = n^2 - 2n + 1 = 1$ modulo n. So $(n-1).{}_n(n-1) = (n-1)^2 = 1$ in M_n. This shows that the inverse of $n-1$ is $n-1$ and so H contains the inverses of all its elements and is closed under $._n$. So H is a subgroup of M_n.
(b) Since M_8 is abelian, the left cosets and the right cosets are the same. $M_8 = \{1, 3, 5, 7\}$ and $H = \{1, 7\}$. So, the number of cosets of H in M_8 is $|M_8|/|H| = 4/2 = 2$. We start with the coset generated by the identity element, i.e.

$$1H = \{1, 7\} = H.$$

3 is not in this coset, so the other coset should be the one containing 3, which is $3H = \{3, 5\}$. So, the cosets of H in M_8 are H and $3H$.
(c) Note that if $n \geq 3$, then $n - 1 \neq 1$ and so $|H| = 2$. By part (a), H is a subgroup of M_n. So, by Lagrange's theorem, the order of H should divide the order of M_n, i.e. 2 divides the order of M_n. So, M_n has even order. □

Problem 5. On last week's homework, we defined the center of G as the subgroup

$$Z(G) = \{x \in G | xy = yx \ \forall y \in G\}.$$

Show that every left coset of $Z(G)$ is also a right coset of $Z(G)$.

Proof. Any left coset of $Z(G)$ is of the form $gZ(G)$ for some $g \in G$. Note that for any $z \in Z(G), gz = zg$ by the definition of $Z(G)$. So, $gZ(G) = \{gz | z \in Z(G)\} = \{zg | z \in Z(G)\} = Z(G)g$ which is a right coset of $Z(G)$. So, every left coset of $Z(G)$ is also a right coset of $Z(G)$.

□

Problem 6. Let G be a group of order pq, where p and q are prime numbers. Show that every proper subgroup of G is cyclic.

Proof. Let H be a proper subgroup of G. Then $|H| < pq$. By Lagrange's theorem, $|H|$ divides pq, but the only divisors of pq are $1, p, q$ and pq. So, $|H| = 1, p$ or q. If $|H| = p$ or q, then we use the fact that every group of prime order is cyclic, and so H has to be cyclic. If $|H| = 1$, then $H = \{e\} = \langle e \rangle$, which is cyclic, generated by e. So, every proper subgroup of G is cyclic. □

Problem 7. Show that a group with at least two elements but with no proper nontrivial subgroups must be finite and of prime order.

Proof. Let G denote this group. Since G has at least two elements, there exists $a \in G$ such that $a \neq e$. Let $H = \langle a \rangle$. Then $H \neq \{e\}$. Since G has no proper nontrivial subgroups, this implies that $H = G$. So, $G = \langle a \rangle$. Now, suppose that G is an infinite group. Then a has infinite order. Let us look at $H = \langle a^2 \rangle$. Note that $a^2 \neq e$ as a has infinite order. So, $H \neq \{e\}$. But this implies that H has to be G. But note that $a \notin H$ because otherwise $a = (a^2)^k$ for some $k \in \mathbb{Z}$ which implies that $a^{2k-1} = e$, which contradicts our assumption that the order of a is infinite. So, G cannot be an infinite group. So, G is a finite group.

Let $|G| = n$. We want to show that n has to be prime. Suppose n is not prime. Then there exists n_1, n_2 with both n_1 and n_2 strictly greater than 1 such that $n = n_1 n_2$. Since $G = \langle a \rangle$, the order of a is n and the order of a^{n_1} is n_2. So, $\langle a^{n_1} \rangle$ is a subgroup of G of order n_2 which contradicts the fact that G has no proper nontrivial subgroups. So n has to be prime. $\square$

Problem 8. Let G be a group such that $|G| = 6$ and assume that, for every $a \in G$, $\text{ord}(a) < 6$. The goal of this problem is to prove that $G \cong S_3$.
(a) Prove that G must have an element a of order 2.
(b) Prove that G must have an element b of order 3.
(c) Prove that $ab \neq ba$.
(d) Prove that $G \cong S_3$.

Proof. (a) Problem 11 of the first homework assignment states that "if G is a group with identity e and an even number of elements, then there is $a \neq e$ in G such that $a^2 = e$." Since $|G| = 6$ is even, this implies that G must have an element a of order 2.
(b) Suppose for the sake of contradiction that G does not contain any element of order 3. Since the order of an element divides 6, this implies that the order of an element has to be 1, 2 or 6. But we are given that G does not contain any element of order 6. This implies that any non-identity element must have order 2. So, let $x, y \in G$ with $x \neq e, y \neq e$ and $x \neq y$. Also, $xy \neq e$ because if $xy = e$, then $y = x(xy) = x$, which contradicts our choice of x and y. Then xy has order 2, so $(xy)^2 = e$, i.e. $xyxy = e$. But note that $x^2 = e, y^2 = e$. So,

$$xyxy = e \implies yx(xyxy) = yx$$

But $yx(xyxy) = yx^2yxy = y^2xy = xy$. So, $xy = yx$. This implies that, if we put $H = \{e, x, y, xy\}$, H has to be a subgroup of G. This can easily be checked because $x(xy) = y, (xy)x = (yx)x = y, y(xy) = (yx)y = (xy)y = x$ etc. and $x^{-1} = x, y^{-1} = y$ and $(xy)^{-1} = xy$ because elements of order 2 are their own inverse. But H cannot be a subgroup of G as $4 = |H|$ does not divide $6 = |G|$ which contradicts Lagrange's theorem. So, we arrive at a contradiction. This implies that G must have an element b of order 3.
(c) Suppose that $ab = ba$ where a and b are what we obtained from parts (a) and (b) above. Note that if $ab = e$, then $b = a(ab) = a$, which is not true. So, $ab \neq e$. So the order of ab has to be 2 or 3. (It cannot be 6 because we are given that G has no elements of order 6.) Now, $(ab)^2 = abab = a(ba)b = a(ab)b = a^2b^2 = b^2 \neq e$. So, the order of ab is not 2. But, $(ab)^3 = (ab)(ab)^2 = (ab)b^2$ from our computations above. So, $(ab)^3 = ab^3 = a \neq e$. This implies that the order of ab cannot be 3, a contradiction. So, $ab \neq ba$.
(d) We can now write down some elements of G in terms of a and b. Note that e, a, b, b^2, ab and ba are distinct elements of G. So, $G = \{e, a, b, b^2, ab, ba\}$. We note that ab^2 is an element of G, so it has to equal one of the six elements mentioned here. If $ab^2 = e$, then $ab^3 = b \implies a = b$, which is not possible. So, $ab^2 \neq e$. If $ab^2 = a$, then $b^2 = e$, which is not possible as b has order 3. So, $ab^2 \neq a$. If $ab^2 = b$, then $ab^3 = b^2 \implies a = b^2$, which is not possible. So, $ab^2 \neq b$. If $ab^2 = b^2$, then $a = e$, which is not possible. So, $ab^2 \neq b^2$. If $ab^2 = ab$, then $b = e$, which is not possible. So, $ab^2 \neq ab$. So, we are left with only one option, i.e. ab^2 has to be equal to ba. This relation between a and b will help us construct a table for G. The goal is to construct a bijective map from G to S_3 and compare their tables to conclude that it is a homomorphism, and hence an isomorphism. We want to find a map $\phi : G \to S_3$ that is an

isomorphism. So, $\phi(b)$ has to have order 3. So, we put $\phi(b) = (123)$. So, obviously, we want $\phi(b^2) = (123)^2 = (132)$. Similarly, put $\phi(a) = (12)$. Thus, we define $\phi : G \to S_3$ by

$$e \mapsto e$$

$$a \mapsto (12)$$

$$b \mapsto (123)$$

$$b^2 \mapsto (132)$$

$$ab \mapsto (23)$$

$$ba \mapsto (13)$$

We now construct the table for G :

.	e	a	b	b^2	ab	ba
e	e	a	b	b^2	ab	ba
a	a	e	ab	ba	b	b^2
b	b	ba	b^2	e	a	ab
b^2	b^2	ab	e	b	ba	a
ab	ab	b^2	ba	a	e	b
ba	ba	b	a	ab	b^2	e

We have computed the table above by playing around with the relations $a^2 = e, b^3 = e$ and $ab^2 = ba$. As an example, $a(ba) = a(ab^2) = a^2b^2 = b^2$. Or $b^2(ab) = b(ba)b = b(ab^2)b = bab^3 = ba$ etc. Now, we write down the table for S_3 :

.	e	(12)	(123)	(132)	(23)	(13)
e	e	(12)	(123)	(132)	(23)	(13)
(12)	(12)	e	(23)	(13)	(123)	(132)
(123)	(123)	(13)	(132)	e	(12)	(23)
(132)	(132)	(23)	e	(123)	(13)	(12)
(23)	(23)	(132)	(13)	(12)	e	(123)
(13)	(13)	(123)	(12)	(23)	(132)	e

Comparing these two tables under the map ϕ, we see that they are identical. This proves that ϕ is an isomorphism. Hence $G \cong S_3$. $\square$