HW 5 - MATH403

Danesh Sivakumar

June 14, 2022

Problem 1 (Chapter 7, Exercise 6)

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

Proof. We know that because a has order 15, $\langle a \rangle$ also has order 15. We also know that the order of $\langle a^5 \rangle$ is $15/\gcd(5, 15) = 15/5 = 3$ by the cyclic order formula. This means that there are $15/3 = 5$ distinct cosets of $\langle a^5 \rangle$ in $\langle a \rangle$; we claim that these are $\langle a^5 \rangle$, $a\langle a^5 \rangle$, $a^2\langle a^5 \rangle$, $a^3\langle a^5 \rangle$ and $a^4\langle a^5 \rangle$. To this end, notice:

$$\langle a^5 \rangle = \{e, a^5, a^{10}\}$$

$$\begin{aligned} a\langle a^5 \rangle &= \{a, a^6, a^{11}\} \\ a^2\langle a^5 \rangle &= \{a^2, a^7, a^{12}\} \\ a^3\langle a^5 \rangle &= \{a^3, a^8, a^{13}\} \\ a^4\langle a^5 \rangle &= \{a^4, a^9, a^{14}\} \end{aligned}$$

and all of these cosets form a disjoint union for $\langle a \rangle$, so they are indeed the only left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$. □

Problem 2 (Chapter 7, Exercise 8)

Give an example of a group G and subgroups H and K such that $HK = \{h \in H, k \in K\}$ is not a subgroup of G.

Proof. Take $G = S_3$, $H = \langle (12) \rangle$ and $K = \langle (23) \rangle$. Then H and K are subgroups of G, but $HK = \{1, (12), (23), (132)\}$; because this set is of size 4, it doesn't divide $|G| = 6$, so it cannot be a subgroup of G by Lagrange's theorem.

□

Problem 3 (Chapter 7, Exercise 12)

Let a and b be nonidentity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.

Proof. Suppose that H is a subgroup of G containing both a and b. By Lagrange's theorem, the only possible orders of H are 5, 31, or 155 (the trivial subgroup is not allowed because a and b are nonidentity elements). We will first prove that any group of prime order is cyclic, and that all of its nonidentity elements have the same order; the result will follow then. To this end, let G be a group of order p, where p is prime. Consider the subgroup generated by any arbitrary nonidentity $g \in G$; by Lagrange's theorem, the order of this subgroup must divide p; but since p is prime and $g \neq e$, this means $|\langle g \rangle| = p$, so that $\langle g \rangle = G$. Also, take any arbitrary nonidentity $a \in \langle g \rangle$; by similar reasoning, $|\langle a \rangle| = p$, meaning that any nonidentity element is a generator. Because 5 and 31 are primes, it follows that every nonidentity element in the subgroup of order 5 has order 5 and every nonidentity element in the subgroup of order 31 has order 31. This means that the only possibility for the order of H is 155, which implies that $H = G$. $\square$

Problem 4 (Chapter 7, Exercise 26)

Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime.

Proof. Suppose $|G| \geq 2$, with $|G|$ possibly ∞. If G has no proper, nontrivial subgroups, then the only subgroups of G are e and G itself. Take arbitrary nonidentity $a \in G$ and consider $\langle a \rangle$; clearly $\langle a \rangle \neq e$, so $\langle a \rangle = G$, meaning that G is cyclic. Now assume $|G| = \infty$; this means that $G \cong \mathbb{Z}$, which is a contradiction because $\mathbb{Z}$ has nontrivial subgroups. Thus $|G| = n$ for some finite n. Since G is cyclic, by the fundamental theorem of cyclic groups it follows that there is exactly one subgroup of order d for each positive divisor d of n, and these are the only subgroups of G. Thus, if $d \neq 1$ or $d \neq n$, then G has proper nontrivial subgroups, which is a contradiction; thus the only divisors of n are n and 1, meaning that n is prime. $\square$

Problem 5 (Chapter 7, Exercise 28)

Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G. Generalize to any group of order p^2 where p is prime.

Proof. If G is cyclic, we are done. Suppose that G is not cyclic; we claim that for all $g \in G, g^5 = e$. If $g = e$, then clearly $g^5 = e$, so suppose $g \neq e$. By Lagrange's theorem $|g|$ divides 25, so that g could possibly be 1, 5, or 25. However, $|g| \neq 1$ because $g \neq e$ and $|g| \neq 25$ because G is not cyclic; thus $|g| = 5$ so that $g^5 = e$. An analogous result holds true for any prime p; if G is a group of order p^2, then p is cyclic or $g^p = e$ for all $g \in G$ through the same line of reasoning because the only divisors of p^2 are 1, p and p^2 by the fundamental theorem of arithmetic. $\square$

Problem 6 (Chapter 7, Exercise 32)

Determine all finite subgroups of $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication.

Proof. Suppose $H \leq \mathbb{C}^*$, with $|H|$ finite, say $|H| = n$. By Lagrange's theorem, it follows that for any $z \in H$, $z^{|H|} = z^n = 1$, because 1 is the identity in $\mathbb{C}^*$. However, the solutions of $z^n = 1$ are by definition the nth roots of unity, which implies that H consists precisely of nth roots of unity. These roots certainly form a subgroup, because (1) they are closed under the operation of multiplication and (2) inverses exists. To show (1), let $z_1 = e^{a2\pi/n}$ and $z_2 = e^{b2\pi/n}$, with $a, b < n$. Notice that $z_1 z_2 = e^{(a+b)2\pi/n} = e^{(a+b \mod n)2\pi/n}$, and $0 < a + b \mod n < n$ so that $z_1 z_2 \in H$. To show (2), notice that $z_1^{-1} = e^{(n-a)2\pi/n}$, and $z_1 z_1^{-1} = e^{a2\pi/n} e^{(n-a)2\pi/n} = e^{n2\pi/n} = e^{2\pi} = 1$ (multiplication is commutative). □

Problem 7 (Chapter 7, Exercise 40)

Prove that a group of order 63 must have an element of order 3.

Proof. By Lagrange's theorem, the only possible orders for elements are 1, 3, 7, 9, 21, and 63 because those are the divisors of 63. Pick a non-identity element g. If $|g| = 3$, we are done. If $|g| = 9$, then $|g^3| = 3$. If $|g| = 21$, then $|g^7| = 3$. If $|g| = 63$, then $|x^2 1| = 3$. If none of these are the case, then there are 62 non-identity elements of order 7, which is impossible because 62 is not a multiple of $\phi(7) = 6$. □

Problem 8 (Chapter 7, Exercise 46)

Prove that a group of order 12 must have an element of order 2.

Proof. By Lagrange's theorem, the only possible orders for elements are 1, 2, 3, 4, 6 and 12 because those are the divisors of 12. Pick a non-identity element g. If $|g| = 2$, we are done. If $|g| = 4$, then $|g^2| = 2$. If $|g| = 6$, then $|g^3| = 2$. If $|g| = 12$, then $|g^6| = 2$. If none of these are the case, then there are 11 non-identity elements of order 3, which is impossible because 11 is not a multiple of $\phi(3) = 2$. □

Problem 9 (Chapter 7, Exercise 62)

Calculate the orders of the following

a. The group of rotations of a regular tetrahedron

b. The group of rotations of a regular octahedron

c. The group of rotations of a regular dodecahedron

d. The group of rotations of a regular icosahedron

Proof. We proceed via the Orbit-Stabilizer Theorem.

a. $|\text{stabilizer}|= 3$ because rotating about any vertex a multiple of $2\pi/3$ radians preserves structure and $|\text{orbit}|= 4$ because there are four vertices, so order of rotations is $3 \cdot 4 = 12$.

b. $|\text{stabilizer}|= 4$ because rotating about any vertex a multiple of $\pi/2$ radians preserves structure and $|\text{orbit}|= 6$ because there are six vertices, so order of rotations is $4 \cdot 6 = 24$.

c. $|\text{stabilizer}|= 5$ because rotation about any face a multiple of $2\pi/5$ radians preserves structure and $|\text{orbit}|= 12$ because there are twelve faces, so order of rotations is $5 \cdot 12 = 60$.

d. $|\text{stabilizer}|= 5$ because rotation about any vertex a multiple of $2\pi/5$ radians preserves structure, and $|\text{orbit}|= 12$ because there are twelve vertices, so order of rotations is $5 \cdot 12 = 60$.

$\square$

Problem 10 (Chapter 8, Exercise 8)

Is $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ isomorphic to $\mathbb{Z}_{27}$?

Proof. Notice that 3 and 9 are not relatively prime, so that $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ cannot be isomorphic to $\mathbb{Z}_{3 \cdot 9} = \mathbb{Z}_{27}$. Also, if there did exist an isomorphism, there would have to be an element of order 27 in $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ because isomorphism preserves order; but there are no elements $z_1 \in \mathbb{Z}_3$ and $z_2 \in \mathbb{Z}_9$ such that the least common multiple of their orders is 27; thus an isomorphism cannot exist. $\square$