HW 2 - MATH403

Danesh Sivakumar

June 14, 2022

Problem 1 (Chapter 3, Exercise 20)

For any group elements a and b, prove that $|ab| = |ba|$.

Proof. Suppose that $|ab| = n$, so that $(ab)^n = e$. Then:

$$(ab)^n = ababab \cdots ab = ababab \cdots abaa^{-1} = a(bababa \cdots ba)a^{-1} = a(ba)^n a^{-1} = e$$

Right multiplying both sides of the last equality by a yields $a(ba)^n = a$, which implies that $(ba)^n = e$. This means that $|ba|$ divides n, or that $|ba|$ divides $|ab|$, so that $|ba| \leq |ab|$.

Now suppose that $|ba| = m$, so that $(ba)^m = e$. Then:

$$(ba)^m = bababa \cdots ba = bababa \cdots babb^{-1} = b(ababab \cdots ab)b^{-}1 = b(ab)^m b^{-1} = e$$

Right multiplying both sides of the last equality by b yields $b(ab)^m = b$, which implies that $(ab)^m = e$. This means that $|ab|$ divides m, or that $|ab|$ divides $|ba|$, so that $|ab| \leq |ba|$.

Because $|ab| \leq |ba|$ and $|ba| \leq |ab|$, it follows that $|ab| = |ba|$.

$\square$

Problem 2 (Chapter 3, Exercise 28)

Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

Proof. Let $a, b \in G$ with $|a| = 2$, $|b| = 2$, and $ab = ba$. Consider $H = \{e, a, b, ab\} \subseteq G$. We claim that H is a subgroup of G. We must show that (1) $x, y \in H \implies x * y \in H$ and (2) $x \in H \implies x^{-1} \in H$. Clearly H is nonempty; to this end, observe the Cayley table of H:

	e	a	b	ab
e	e	a	b	ab
a	a	a^2	ab	a^2b
b	b	ba	b^2	bab
ab	ab	aba	abb	$abab$

Using the fact that $|a| = 2$ and $|b| = 2$, we deduce that $a^2 = e$ and $b^2 = e$. Furthermore, because a and b commute, observe that $aba = aab = b$ and $bab = bba = a$. Also, note that $abab = aabb = e$. With this, the simplified Cayley table becomes:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Since each row and column of the Cayley table contains each element exactly once, H is closed, so (1) is satisfied. $e^{-1} = e$ trivially, and because $a^2 = e$ and $b^2 = e$ it follows that $b^{-1} = b$ and $a^{-1} = a$. Because $abab = (ab)^2 = e$, it follows that $(ab)^{-1} = ab$; thus, each element in H has an inverse (namely itself), so (2) is satisfied. Thus, H is a subgroup of order 4.

□

Problem 3 (Chapter 3, Exercise 38)

Let G be an Abelian group and $H = \{x \in G |\ |x| \text{ is odd}\}$. Prove that H is a subgroup of G.

Proof. We must show that (1) $x, y \in H \implies x * y \in H$ and (2) $x \in H \implies x^{-1} \in H$. Note that H is nonempty because $|e| = 1$, so $e \in H$. To prove (1), consider $a, b \in H$. Because $|a|, |b|$ are odd, we have that $|a| = 2k + 1$ and $|b| = 2l + 1$ for nonnegative integers k, l. Because G is abelian, it follows that $ab = ba$, so $|ab|$ divides $(2k+1)(2l+1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$. By closure of integers under multiplication and addition, $2kl + k + l = c \in \mathbb{N}$, so $|ab|$ divides $2c + 1$, which is an odd nonnegative integer. To prove $|ab|$ is odd, suppose not, that is, that $|ab| = 2j$ for some nonnegative integer j. Then our previous result implies that there exists $m \in \mathbb{Z}$ such that $2jm = 2c + 1 \implies 2(jm - c) = 1 \implies (jm - c) = \frac{1}{2}$, which is a contradiction because j, c and m are all integers; thus $|ab|$ is odd, so $ab \in H$, proving (1). By a result in the previous homework, we have that the order of any element and its inverse are the same, so that for all $a \in H$, we have that $|a| = 2k + 1 \implies |a^{-1}| = 2k + 1$, so $a^{-1} \in H$, proving (2). Thus, H is a subgroup of G.

□

Problem 4 (Chapter 3, Exercise 42)

In the group $\mathbb{Z}$, find:

(a) $\langle 8, 14 \rangle$;

(b) $\langle 8, 13 \rangle$;

(c) $\langle 6, 15 \rangle$;

(d) $\langle m, n \rangle$;

(e) $\langle 12, 18, 45 \rangle$;

In each part, find an integer k such that the subgroup is $\langle k \rangle$.

Proof. Note that from a theorem in class, we have that $\langle m, n \rangle = \langle \gcd(m, n) \rangle$, so that:

(a) $\langle 8, 14 \rangle = \langle \gcd(8, 14) \rangle = \langle 2 \rangle$

(b) $\langle 8, 13 \rangle = \langle \gcd(8, 13) \rangle = \langle 1 \rangle = \mathbb{Z}$

(c) $\langle 6, 15 \rangle = \langle \gcd(6, 15) \rangle = \langle 3 \rangle$

(d) $\langle m, n \rangle = \langle \gcd(m, n) \rangle$

(e) $\langle 12, 18, 45 \rangle = \langle \gcd(12, 18, 45) \rangle = \langle 3 \rangle$

□

Problem 5 (Chapter 3, Exercise 46)

Suppose a belongs to a group and $|a| = 5$. Prove that $C(a) = C(a^3)$. Find an element a from some group such that $|a| = 6$ and $C(a) \neq C(a^3)$.

Proof. We must show that (1) $C(a) \subseteq C(a^3)$ and (2) $C(a^3) \subseteq C(a)$. To prove (1), suppose that $b \in C(a)$. Then $ab = ba$, so that

$$a^3b = aaab = aaba = abaa = baaa = ba^3$$

showing that $b \in C(a^3)$, proving (1). To prove (2), suppose that $b \in C(a^3)$. Then $a^3b = ba^3$; noting that because $|a| = 5 \implies a^5 = e$, observe

$$ab = a^5ab = a^6b = a^3a^3b = a^3ba^3 = ba^3a^3 = ba^6 = baa^5 = ba$$

showing that $b \in C(a)$, proving (2). Since $C(a) \subseteq C(a^3)$ and $C(a^3) \subseteq C(a)$, it follows that $C(a) = C(a^3)$.

For the counterexample, consider the dihedral group D_6, wherein $a \in D_6$ corresponds to a 60° rotation, and $b \in D_6$ corresponds to a reflection about the horizontal axis. Observe that $|a| = 6$, and $ba^3 = a^3b$, but $ba \neq ab$, so that $b \in C(a^3)$ but $b \notin C(a)$, showing that the two centralizers are not equal in this case.

□

Problem 6 (Chapter 3, Exercise 74)

If H and K are nontrivial subgroups of the rational numbers under addition, prove that $H \cap K$ is nontrivial.

Proof. Suppose that $\frac{a}{b} \in H$ and $\frac{c}{d} \in K$ for nonzero integers a, b, c, d. Then by closure of rationals under addition, $a \in H$ and $c \in K$. Applying closure under addition once more shows that $ac \in H$ and $ca \in K$. Because the rationals are commutative under multiplication, $ac = ca$, so that $ac \in H \cap K$.

□

Problem 7 (Chapter 4, Exercise 2)

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

Proof. From a theorem in class, we have that given $|\langle a \rangle| = n$, all generators of $\langle a \rangle$ are of the form a^k, where $\gcd(n, k) = 1$. From this, we deduce that 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}.

□

Problem 8 (Chapter 4, Exercise 4)

List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in $\mathbb{Z}_{18}$. Let a be a group element of order 18. List the elements of the subgroups $\langle a^3 \rangle$ and $\langle a^{15} \rangle$

Proof. $\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$.
Note that in $\mathbb{Z}_{18}$, $15 \equiv -3$, so that $\langle 15 \rangle = \langle -3 \rangle = \langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$.
$\langle a^3 \rangle = \{(a^3)^n\} = a^{3n} \in \langle a \rangle = \{e, a^3, a^6, a^9, a^{12}, a^{15}\}$
$\langle a^{15} \rangle = \langle a^{-3} \rangle = \langle a^3 \rangle = \{e, a^3, a^6, a^9, a^{12}, a^{15}\}$.

□

Problem 9 (Chapter 4, Exercise 8)

Let a be an element of a group 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}

Proof. From a formula proven in class, we have that if $|a| = n$, then $|a^k| = \frac{n}{\gcd(n,k)}$, so that:

(a) For all $k \in \{3, 6, 9, 12\}$, $\gcd(k, 15) = 3$, so it follows that $|a^k| = \frac{15}{3} = 5$.

(b) For all $k \in \{5, 10\}$, $\gcd(k, 15) = 5$, so it follows that $|a^k| = \frac{15}{5} = 3$.

(c) For all $k \in \{2, 4, 8, 14\}$, $\gcd(k, 15) = 1$, so it follows that $|a^k| = \frac{15}{1} = 15$.

□

Problem 10 (Chapter 4, Exercise 14)

Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$? What can you say if 7 is replaced with p where p is a prime?

Proof. By the fundamental theorem of cyclic groups, we have that the subgroups of a cyclic group G have orders equal to the divisors of the order of G. From this, we know that 7 divides $|G|$. The fact that there are exactly three subgroups means that $|G| = 7 \cdot 7 = 49$, because otherwise $|G|$ would not have three divisors and thus not have three subgroups, contradicting the supposition. More generally, $|G| = p^2$ if p is a prime, and there are three subgroups: one whose order is p^2, one whose order is p, and one whose order is 1 (the identity).

□

Problem 11 (Chapter 4, Exercise 32)

Determine the subgroup lattice for $\mathbb{Z}_{12}$. Generalize to $\mathbb{Z}_{p^2q}$, where p and q are distinct primes.

Proof. Note that the proper divisors of 12 are 1, 2, 3, 4, and 6, so we will consider the subgroups generated by these elements:

$$\langle 1 \rangle = \mathbb{Z}_{12}$$
$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$$
$$\langle 3 \rangle = \{0, 3, 6, 9\}$$
$$\langle 4 \rangle = \{0, 4, 8\}$$
$$\langle 6 \rangle = \{0, 6\}$$

To construct the subgroup lattice, we draw connections between any two subgroups whose elements are fully contained in other.

For the general case, notice that the proper divisors of p^2q are p, p^2, q, pq and 1, so that:

$$\langle 1 \rangle = \mathbb{Z}_{p^2q}$$
$$\langle p \rangle = \{0, p, 2p, \cdots, p^2, \cdots, p^2q\}$$
$$\langle q \rangle = \{0, q, 2q, \cdots, p^2q\}$$

$$\langle pq \rangle = \{0, pq, 2pq, \cdots, p^2 q\}$$
$$\langle p^2 \rangle = \{0, p^2, \cdots, p^2 q\}$$

□

Problem 12 (Chapter 4, Exercise 44)

Which of the following numbers could be the exact number of elements of order 21 in a group: 21600, 21602, 21604?

Proof. Using the fact that in any finite group, the number of elements of order d is a multiple of $\Phi(d)$, we deduce that the number of elements of order 21 is a multiple of $\Phi(21) = \Phi(3)\Phi(7) = (3-1)(7-1) = 2 \cdot 6 = 12$. The only number that is a multiple of 12 is 21600, so the only possible choice is 21600.

□

Problem A

Prove that every finite subgroup of $(\mathbb{C}^*, \times)$ is cyclic.

Proof. Let $H \in (\mathbb{C}^*, \times)$ be a finite subgroup. We claim that H is comprised of nth roots of unity. To this end, suppose not; that is, that $|a| \in H \neq 1$, where $|a|$ denotes the magnitude of a. There are two cases: (1) $|a| > 1$ and (2) $|a| < 1$. Let $a = re^{i\vartheta}$ where $r \neq 1$. For (1), we have that $|a^2| = |r^2 e^{i2\vartheta}| = r^2 > r = |re^{i\vartheta}| = |a|$, so that $|a^2| > |a|$. Suppose that $|a^{k+1}| > |a^k|$. Then $|a^{k+2}| = |a^{k+1}a| = |a^{k+1}||a| > |a^{k+1}|$, so that for all $n \in \mathbb{N}$ it follows that $|a^{n+1}| > |a^n|$, so that $a^{n+1} \neq a^n$, contradicting the fact that H is finite. For (2), we have that $|a^2| = |r^2 e^{i2\vartheta}| = r^2 < r = |re^{i\vartheta}| = |a|$, so that $|a^2| < |a|$. Suppose that $|a^{k+1}| < |a^k|$. Then $|a^{k+2}| = |a^{k+1}a| = |a^{k+1}||a| < |a^{k+1}|$, so that for all $n \in \mathbb{N}$ it follows that $|a^{n+1}| < |a^n|$, so that $a^{n+1} \neq a^n$, contradicting the fact that H is finite. Thus, $|a| = 1$, so that H can only be a group of nth roots of unity whose elements are of the form $e^{\frac{2k\pi\imath}{n}}$. Letting $k = 1$ gives us an $a \in H$ such that $\langle a \rangle = H$, so that $a = e^{\frac{2\pi\imath}{n}}$ is a generator for H, proving that H is cyclic.

□

Problem B

Show that the subgroup $\langle a, b \rangle$ is cyclic for any $a, b \in (\mathbb{Q}, +)$.

Proof. Let $a = \frac{m}{n}$ and $b = \frac{p}{q}$, where $m, n, p, q \in \mathbb{Z}$. Define $\gcd(a, b) = \frac{\gcd(m,p)}{\operatorname{lcm}(n,q)}$. First, we prove $\langle a, b \rangle \subseteq \langle \gcd(a, b) \rangle$: let $c \in \langle a, b \rangle$, so that $c = xa + yb$. But $\gcd(a, b)$ divides both a and b by definition, so $a = l \gcd(a, b)$ and $b = k \gcd(a, b)$ for nonnegative integers k and l. This implies that $c = \gcd(a, b)(xl + yk)$ by substitution, so that $c \in \langle \gcd(a, b) \rangle$. Now we show $\langle \gcd(a, b) \rangle \subseteq \langle a, b \rangle$: let $c \in \gcd(a, b)$, so that $c = k \gcd(a, b)$ for some $k \in \mathbb{N}$. By Bezout's theorem, we have that there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. Thus it follows that $c = k(ax + by) = kax + kby$. Because $kx, ky \in \mathbb{Z}$, it follows that $c \in \langle a, b\rangle$. Thus $\langle a, b\rangle \subseteq \langle \gcd(a, b)\rangle$ and $\langle \gcd(a, b)\rangle \subseteq \langle a, b\rangle$, so that $\langle \gcd(a, b)\rangle = \langle a, b\rangle$, meaning $\langle a, b\rangle$ is generated by $\gcd(a, b)$ and thus cyclic, so the result for integers holds more generally for rationals.

$\square$