MATH 7210 Homework 2

Andrea Bourque

September 2021

1 Problem 1

Let $\phi : G \to H$ be a group homomorphism.

(a) Show that $|\phi(a)|$ divides $|a|$ for all $a \in G$ of finite order.

Proof. We have $(\phi(a))^{|a|} = \phi(a^{|a|})$ by the homomorphism property. Since $a^{|a|} = e = id_G$, we have $(\phi(a))^{|a|} = \phi(e) = e' = id_H$. The result follows now from the general fact that $x^n = e$ implies $|x|$ divdes n. □

(b) If ϕ is an isomorphism, show that $|\phi(a)| = |a|$ for all $a \in G$.

Proof. First assume a has finite order. From (a), we have $|\phi(a)| \leq |a|$. Let $\psi = \phi^{-1}$ and let $b = \phi(a)$. Since b has finite order, we then apply (a) with ψ to show that $|\psi(b)|$ divides $|b|$. But $\psi(b) = a$ by definition. Thus $|a| \leq |\phi(a)|$, so we have $|a| = |\phi(a)|$.

Now assume a has infinite order. If $\phi(a)$ has finite order n, then $(\phi(a))^n = \phi(a^n) = e' = id_H$. But since ϕ is an isomorphism, we must have $a^n = e = id_G$. This is a contradiction, so $\phi(a)$ has infinite order as well.

Thus $|a| = |\phi(a)|$ for all $a \in G$. □

2 Problem 2

Let G be a group.

(a) If $a \in G$, show that there is a unique homomorphism $f : \mathbb{Z} \to G$ such that $f(1) = a$.

Proof. For $0 < n \in \mathbb{Z}$, $f(n) = f(1 + ... + 1) = (f(1))^n = a^n$, where $1 + ... + 1$ is a sum of 1 with itself, n times, and then the homomorphism property of f is used. $f(0) = e = id_G$, since homomorphisms preserve identity. Finally, if $0 > n \in \mathbb{Z}$, then $n = -k$ for $0 < k \in \mathbb{Z}$, so $f(n) = f(-k) = (f(k))^{-1} = (a^k)^{-1} = a^{-k} = a^n$, since homomorphisms preserve inverses. Thus, we see that for all $n \in \mathbb{Z}$, $f(n) = a^n$. That is, f is uniquely determined by its value at 1. □

(b) When is there a homomorphism $h : \mathbb{Z}/n\mathbb{Z} \to G$?

Proof. Let $a = h(1)$. Then $a^n = (h(1))^n = h(1 + ... + 1) = f(0) = e = id_G$, where we have used the homomorphism property, then the fact that $1+...+1 = 0$ in $\mathbb{Z}/n\mathbb{Z}$, and then that homomorphisms preserve identity. Also, note that if $a = h(1)$, then we can see $h(k) = a^k$ for $k = 0, 1, ..., n-1$, in a manner which is the same as in the proof of (a). Thus the value of $h(1)$ uniquely determines h. Since we have seen that $(h(1))^n = e$, we have a homomorphism $h : \mathbb{Z}/n\mathbb{Z} \to G$ exactly when $h(1)$ has an order which divides n. □

(c) Show that if a, n are coprime, the homomorphism $h : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $h(\overline{1}) = \overline{a}$ is an isomorphism. Use this to conclude that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to the group $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. By the results of (b), any $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ gives rise to a homomorphism $h : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, since the order of $\mathbb{Z}/n\mathbb{Z}$ is n, so any element has an order which divides n. We now show that if a, n are coprime, $|\overline{a}| = n$. Suppose, to the contrary, that $|\overline{a}| = m < n$. That is, $m|n$ and $ma \equiv 0 \bmod n$. Since a, n are coprime, a has an inverse mod n, so multiplying by the inverse gives $m \equiv 0 \bmod n$. Since $m < n$, this would imply $m = 0$, which is not a valid order. Thus $m = n$ as desired. Since $|\overline{a}| = n$, the set $\{\overline{0}, \overline{a}, ..., \overline{(n-1)a}\}$ consists of n distinct elements in $\mathbb{Z}/n\mathbb{Z}$, meaning that this set is equal to all of $\mathbb{Z}/n\mathbb{Z}$. But if $h(\overline{1}) = \overline{a}$, then $h(\overline{k}) = \overline{ka}$ for $k = 0, 1, ..., n-1$, from h being a homomorphism. Thus h is surjective, and furthermore h is injective since the only element mapping to $\overline{0}$ is $\overline{0}$. Thus h is an isomorphism.

We have now seen that each $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ gives an automorphism of $\mathbb{Z}/n\mathbb{Z}$. We must then show that this association is an isomorphism. First, given two a, b which are coprime to n, let h_a, h_b be the associated automorphisms. ab is coprime to n (if a prime divides n and ab, it would also divide either a or b), so there is an associated automorphism h_{ab} which sends $\overline{1}$ to $\overline{ab}$. But the composition $h_a \circ h_b$ satisfies $h_a(h_b(\overline{1})) = h_a(\overline{b}) = \overline{a}\overline{b} = \overline{ab}$, so $h_{ab} = h_a \circ h_b$, showing that the association is a homomorphism. Now suppose h_a is the identity automorphism. It must send $\overline{1}$ to $\overline{1}$ to be the identity, but by definition it sends $\overline{1}$ to $\overline{a}$. Then $\overline{a} = \overline{1}$, so the association is injective. Now let h be any automorphism

of $\mathbb{Z}/n\mathbb{Z}$ and let $h(\overline{1}) = \overline{a}$. If a, n were not coprime, say $1 < d = \gcd(a, n)$, then $0 < m = n/d < n$ would satisfy $ma \equiv 0 \bmod n$. In otherwords, $\overline{ma} = \overline{0}$. But $h(\overline{m}) = \overline{ma} = \overline{0}$ implies $\overline{m} = \overline{0}$, since h is an automorphism. This contradicts $0 < m < n$, so a, n are coprime. Then $h = h_a$ for $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, showing that the association is surjective. $\square$

3 Problem 3

Let G be a group. Let $Z(G)$ be the center.

(a) Show that $Z(G)$ is a subgroup of G, and any subgroup of $Z(G)$ is normal in G.

Proof. Clearly $id_G = e \in Z(G)$, since for all $g \in G$, $eg = ge = g$. Let $a, b \in Z(G)$. Then for any $g \in G$, $abg = agb = gab$, using the fact that a, b commute with g. For $a \in Z(G)$ and $g \in G$, $ag = ga$ implies $ga^{-1} = a^{-1}g$. Since g is arbitrary, this shows $a^{-1} \in Z(G)$. Thus $Z(G)$ is a subgroup.

Now let H be a subgroup of $Z(G)$. For any $h \in H, g \in G$, we have $ghg^{-1} = hgg^{-1} = he = h$, since $h \in Z(G)$ commutes with g. Thus H is normal. □

(b) Show that if $G/Z(G)$ is cyclic, then G is abelian. Is it true that G is abelian if $G/Z(G)$ is abelian?

Proof. Let $a \in G$ be such that $aZ(g)$ is a generator for $G/Z(G)$. Then any $g \in G$ equals $a^k b$ for some $k \in \mathbb{Z}$, $b \in Z(G)$. But for $k_1, k_2 \in \mathbb{Z}, b_1, b_2 \in Z(G)$, we have $a^{k_1}b_1a^{k_2}b_2 = a^{k_1}a^{k_2}b_1b_2 = a^{k_2}a^{k_1}b_2b_1 = a^{k_2}b_2a^{k_1}b_1$, where we have used the fact that b_1, b_2 commute with any group element, and the fact that a group element a commutes with itself so $a^{k_1}a^{k_2} = a^{k_1+k_2} = a^{k_2}a^{k_1}$. Thus G is abelian.

It is not true that G is abelian if $G/Z(G)$ is abelian. Consider the group $G = \{1, -1, i, -i, j, -j, k, -k\}$ of quaternions. G is not abelian since $ij = k \neq -k = ji$. The center is $\{1, -1\}$. The group $G/Z(G)$ can then be written as $\{\overline{1}, \overline{i}, \overline{j}, \overline{k}\}$. Notice that $G/Z(G)$ is abelian, since for example, $\overline{i}\overline{j} = \overline{ij} = \overline{k}$, and $\overline{j}\overline{i} = \overline{ji} = \overline{-k} = \overline{k}$, since $1, -1$ are identified in the quotient. Thus, this serves as an example where $G/Z(G)$ is abelian, while G is not. □

(c) Let p, q be prime numbers. If G is a group of order pq, show that either G is abelian or $Z(G) = \{e\}$.

Proof. The possible orders of $Z(G)$ are the divisors of pq, which are $1, p, q, pq$ if $p \neq q$, and $1, p, p^2$ if $p = q$. If the order of $Z(G)$ is pq (or p^2), then $Z(G) = G$ so $G/Z(G)$ is trivial and hence abelian. If the order of $Z(G)$ is p or q then the order of $G/Z(G)$ is prime, and thus cyclic. From (b) we know that G is abelian. The only case is where the order of $Z(G)$ is 1, which just means it is the trivial subgroup. □

4 Problem 2.4.14

(a) Prove that every finite group is finitely generated.

Proof. Clearly, any group is generated by the set of its elements, since the only subgroup containing all elements is the group itself. Thus a finite group is generated by a finite set consisting of its elements. □

(b) Prove that $\mathbb{Z}$ is finitely generated.

Proof. We show $\mathbb{Z}$ is generated by $\{1\}$. In particular, we show any subgroup G in $\mathbb{Z}$ which contains 1 is equal to $\mathbb{Z}$. Thus, let $1 \in G \leq \mathbb{Z}$. Since G is closed under addition, every positive integer $n = 1+...+1 \in G$. Since G is closed under inverses, a negative integer $n = -k$ is the inverse of a positive integer $k \in G$, so $n \in G$. Since G is a subgroup, it contains $id_{\mathbb{Z}} = 0$. Thus G contains $\mathbb{Z}$, meaning $G = \mathbb{Z}$. Thus $\{1\}$ generates $\mathbb{Z}$, since $\{1\}$ generates a subgroup containing 1. □

(c) Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic.

Proof. Let H be a subgroup of $\mathbb{Q}$ generated by the finite set of rationals $\{p_1/q_1, ..., p_n/q_n\}$. Let $k = q_1...q_n$. Each $p_i/q_i = (q_1...q_{i-1}p_iq_{i+1}...q_n)/k$ is an integer multiple of $1/k$, so each generator of H is contained in the cyclic subgroup generated by $1/k$. Thus implies H is a subgroup of $\langle 1/k \rangle$, and subgroups of cyclic groups are cyclic, so H is cyclic as desired. □

(d) Prove that $\mathbb{Q}$ is not finitely generated.

Proof. If $\mathbb{Q}$ is finitely generated, then (c) implies $\mathbb{Q}$ is cyclic. This is false, since if p/q were a generator for $\mathbb{Q}$, then every rational would of the form np/q for $n \in \mathbb{Z}$, but there is no integer n with $np/q = p/(2q) \in \mathbb{Q}$ (assuming that $p/q \neq 0$, but $p/q = 0$ would only generate the trivial subgroup). Thus $\mathbb{Q}$ is not cyclic, so it cannot be finitely generated. □

5 Problem 3.2.10

Let H, K be subgroups of finite index in G; $|G : H| = m, |G : K| = n$. Prove that $\text{lcm}(m, n) \leq |G : H \cap K| \leq mn$. Deduce that if m, n are coprime, then $|G : H \cap K| = mn$.

Proof. Let $a_1H, ..., a_mH$ be disjoint cosets of H, and let $b_1K, ..., b_nK$ be disjoint cosets of K. For any $c \in G$, there are unique cosets a_iH, b_jK such that $c \in a_iH, c \in b_jK$; $c \in a_iH \cap b_jK$. Consider the coset $c(H \cap K)$ and let $d \in c(H \cap K)$. Then for some $x \in H \cap K$, $d = cx$. Since $x \in H$, d is in the same H coset as c, and since $x \in K$, d is in the same K coset as c. Thus $d \in a_iH \cap b_jK$, showing that $c(H \cap K) \subset a_iH \cap b_jK$. If $c(H \cap K), d(H \cap K)$ are two cosets contained in $a_iH \cap b_jK$, then we have $c, d \in a_iH \cap b_jK$. Then $c = dx$ for $x \in H$, $c = dy$ for $y \in K$. But then $x = y \in H \cap K$, so the two cosets $c(H \cap K), d(H \cap K)$ are equal. Thus far, we have shown that every coset of $H \cap K$ is contained in some $a_iH \cap b_jK$, and that if two cosets of $H \cap K$ are contained in $a_iH \cap b_jK$, they are equal. Since there are mn such sets $a_iH \cap b_jK$, there are at most mn cosets of $H \cap K$.

Using the result of Problem 3.2.11, since $H \cap K \leq H \leq G$, we have that $|G : H|$ divides $|G : H \cap K|$; similarly, $|G : K|$ divides $|G : H \cap K|$. Thus $|G : H \cap K|$ is a multiple of m and n, so by definition of lcm, $\text{lcm}(m, n) \leq |G : H \cap K|$.

Now, if m, n are coprime, then $\text{lcm}(m, n) = mn$, so the inequality gives $mn \leq |G : H \cap K| \leq mn$, implying $|G : H \cap K| = mn$. □

6 Problem 3.2.11

Let $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$.

Proof. Let $|G : K| = m, |K : H| = n$. Let the disjoint cosets of K in G be $a_1K, ..., a_mK$, and let the disjoint cosets of H in K be $b_1H, ..., b_nH$. For $g \in G$, there is a unique i such that $g \in a_iK$, so let $k \in K$ be such that $g = a_ik$. Then there is a unique j such that $k \in b_jH$, so let $h \in H$ be such that $k = b_jh$. Then $g = a_ib_jh$, so $g \in a_ib_jH$. Thus every coset of H in G can be written in the form a_ib_jH.

Consider the cosets $a_ib_jH, a_{i'}b_{j'}H$, and suppose they are equal. Then for some $h \in H$, $a_ib_j = a_{i'}b_{j'}h$. Since $b_j, b_{j'}, h \in K$, we have that $a_ib_jK = a_iK$ and $a_{i'}b_{j'}hK = a_{i'}K$. Thus $a_iK = a_{i'}K$, so by definition of the $a_i's$ we have $i = i'$. Cancelling out the $a_i = a_{i'}$ terms, we get $b_j = b_{j'}h$, implying that $b_jH = b_{j'}H$, so by definition of the $b_j's$ we have $j = j'$. Therefore, the cosets $a_ib_jH, a_{i'}b_{j'}H$ are disjoint if $i \neq i'$ or $j \neq j'$. This gives mn distinct cosets of H in G, and we have seen that all cosets arise as a_ib_jH, so $|G : H| = mn$ as desired. □