MATH 4041 HW 12

David Chen, dc3451

November 29, 2020

Problem 1

i

We have that

$$f_{a,b} \circ f_{r,0} \circ f_{a,b}^{-1} = f_{ra,b} \circ f_{a^{-1},-a^{-1}b} = f_{r,b-rb}$$

so for example,

$$f_{2,2} \circ f_{2,0} \circ f_{2,2}^{-1} = f_{4,2} \circ f_{1/2,-1} = f_{2,-2}$$

but $f_{2,-2} \notin K$, while $f_{2,0} \in K$, so K is not normal.

ii

We have that

$$f_{a,b} \circ f_{1,s} \circ f_{a,b}^{-1} = f_{a,as+b} \circ f_{a^{-1},-a^{-1}b} = f_{1,as}$$

and $as \in \mathbb{R}$ since $a, s \in \mathbb{R}$, so $hNh \subseteq N$ for any $h \in H$, so N is normal.

Next, $H/N \cong \mathbb{R}^*$. To see this, we use Noether's first isomorphism theorem: consider the homomorphism $F : H \to \mathbb{R}^*$ which takes $f_{a,b} \mapsto a$ and $F(f_{a,b} \circ f_{c,d}) = F(f_{ac,ad+b}) = ac = F(f_{a,b})F(f_{c,d})$. Then, $F(f_{a,b}) = 1 \iff a = 1$, so the kernel of F is N. Then, the theorem gives that the image of F, which is all of $\mathbb{R}^*$ (since every $r \in \mathbb{R}^*$ has preimage $f_{r,0}$, for example), is isomorphic to H/N.

Problem 2

i

First, note that $gH = H \implies g \cdot 1 = g \in H$ since $1 \in H$, and if $g \in H$, then $gH = H$ since H is a subgroup and closed under the operation. Then, $gH = H \iff g \in H$.

From definition of coset multiplication, we have that $(aH)^n = a^n H$; then, $a^n H = H$ (here, H is the identity for coset multiplication) if and only if $a^n \in H$, so the integers n which satisfy $a^n \in H$ and which satisfy $(aH)^n = H$ are the same, and by definition of order, the order of aH is the least positive integer n such that $(aH)^n = H$ and thus the least positive integer that $a^n \in H$. Further, if $a^n \notin H$ for all positive integers n, then we have that $(aH)^n \neq H$, so aH has infinite order in this case.

ii

Consider $G = \mathbb{Z}$, $H = \langle 2 \rangle$. Clearly $a = 1 \in \mathbb{Z}$ has infinite order, but $2 \cdot 1 = 2 \in \langle 2 \rangle$, so aH has finite order 2 (the subgroup is normal since $\mathbb{Z}$ is abelian).

iii

We have that if $a^n = 1$, then $(aH)^n = a^n H = 1H = H$, so aH has order at most n in G/H. To see that aH must have order dividing n, suppose that aH has order m and $n = qm + r$ where $0 \leq r < m$. Then,

$$H = (aH)^n = (aH)^{qm+r} = (aH)^{qm}(aH)^r = ((aH)^m)^q (aH)^r = H^q (aH)^r = aH^r$$

but then $aH^r = H$, so since $r < m$, if $r > 0$, then aH has order $r < m$; $\Rightarrow\!\Leftarrow$, so $r = 0$ and $n = qm$, so $m \mid n$.

The order of aH is not always n: consider the cyclic group $G = \mathbb{Z}/4\mathbb{Z}$, and let $H = \{0, 2\}$, $a = 1$. a has order 4 in G, but $aH = \{1, 3\}$, $a^2 H = \{2, 4\} = \{0, 2\} = H$, so aH only has order 2 in G/H.

Problem 3

i

$f^{-1}(H_2) = \{h \in G_1 \mid f(h) \in H_2\}$. Suppose that $f^{-1}(H_2)$ was not normal, such that $\exists h \in f^{-1}(H_2)$ and $g \in G_1$ such that $ghg^{-1} \notin f^{-1}(H_2) \implies f(ghg^{-1}) \notin H_2$. But then, $f(g)^{-1} = f(g^{-1})$, so $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \notin H_2$, and $f(h) \in H_2$, so H_2 is not normal. $\Rightarrow\!\Leftarrow$, so the preimage of a normal group under a homormorphism is itself normal.

ii

Consider the mapping $f : S_3 \to S_4$ where $f(\sigma) = \tau$ where $\sigma(n) = \tau(n)$ for $1 \leq n \leq 3$ and $\tau(4) = 4$. This is a homomorphism: $(f(\sigma_1\sigma_2))(n) = (\sigma_1\sigma_2)(n) = (f(\sigma_1)f(\sigma_2))(n)$ for

$1 \leq n \leq 3$, since $\sigma_2(n) \in \{1,2,3\}$ for $1 \leq n \leq 3$. Lastly, if $n = 4$, $(f(\sigma_1\sigma_2))(4) = 4 = (\sigma_1\sigma_2)(4) = (f(\sigma_1)f(\sigma_2))(4)$ Then, $f(A_3)$ is not normal even though A_3 is normal; consider

$$(3,4)f((1,2,3))(4,3) = (3,4)(1,2,3)(4,3) = (3,4)(1,2,3,4) = (1,2,4)$$

but $(1,2,4)$ moves 4, so $(1,2,4) \notin f(A_3)$.

iii

Pick any $g \in G_2$ and any $h \in f(H_1)$. We wish to show that $ghg^{-1} \in f(H_1)$. In particular, let $h = f(h')$ for some $h' \in H_1$, and $g = f(g')$ for some $g' \in G$ since f is surjective. Then, $f(g'^{-1}) = f(g')^{-1} = g^{-1}$, and so

$$f(g'h'g'^{-1}) = f(g')f(h')f(g'^{-1}) = ghg^{-1}$$

but since H_1 is normal, $g'h'g'^{-1} \in H_1$, so $f(g'h'g'^{-1}) = ghg^{-1} \in f(H_1)$, and so $f(H_1)$ is normal.

Problem 4

The first isomorphism theorem gives that $G/K \cong H$ where K is the kernel of f (H is the image of f since f is surjective). Then, since $|G/K| = |G|/|K|$, and there is a bijection between G/K and H, $|G|/|K| = |H| \implies |K| = |G|/|H|$.

Problem 5

If $g = 1$, then $H = \{1\}$ and is trivially both normal and contained in the center. Assume otherwise for the rest of the problem:

($\implies$) If H is normal, then $hgh^{-1} \in H$ for any $h \in G$. Then, either $hgh^{-1} = 1$ or $hgh^{-1} = g$; in the first case, we have that $hgh^{-1} = 1 \implies hgh^{-1}h = h \implies hg = h \implies g = 1$, which contradicts the earlier assumption that $g \neq 1$. Then, $hgh^{-1} = g \implies hg = gh \implies g \in Z(G)$.

($\impliedby$) If $H \leq Z(G)$, then $1, g$ must both commute with every element of G. In particular, this is always true for the identity, and for any $h \in G$, $h \cdot 1 \cdot h^{-1} = hh^{-1} = 1 \in H$, and since $g \in Z(G)$, $hgh^{-1} = hh^{-1}g = g \in H$ as well, so H is normal.

Problem 6

$\mathbb{Z} \times \mathbb{Z}$ is abelian, so $\langle (a,b) \rangle$ is normal.

We have that all homomorphisms $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ take the form $f(n, m) = cn + dm$ for integers c, d. Then, if we want that the kernel of f is $\langle (a, b) \rangle$, consider $f(n, m) = bn - am$, such that $f(ka, kb) = bka - akb = 0$, so every element $(ka, kb) \in \langle (a, b) \rangle$ is killed by f. Further, if $bn - am = 0$, then $bn = am$, and since $gcd(a, b) = 1$, we have that $b \mid m$ and $a \mid n$, so $b(k_n a) = a(k_m b) \implies k_n = k_m$ so the only (n, m) which are killed are $(n, m) = (ka, kb)$, and so the kernel of f is $\langle (a, b) \rangle$. Then, f is still surjective since $\gcd(a, b) = 1$, as was proved in the earlier homework 10.

The first isomorphism theorem then gives that $(\mathbb{Z} \times \mathbb{Z})/\langle (a, b) \rangle \cong \mathbb{Z}$, since the image of f is $\mathbb{Z}$ since it is surjective and $\langle (a, b) \rangle$ is the kernel of f.

Problem 7

Consider any element $n(a, b)+m(c, d) = (na+mc, nb+md) \in K$. Then, $f(na+mc, nb+md) = -b(na+mc)+a(nb+md) = -bmc+amd = m(ad-bc) = mN \in \langle N \rangle$, so the image of $f \subseteq \langle N \rangle$. Then, we have that any element $kN \in \langle N \rangle$ has preimage $0(a, b) + k(c, d)$, so the image of $f \supseteq \langle N \rangle$, so the image of f is exactly $\langle N \rangle$. This gives by the first isomorphism theorem that (since everything is abelian, K is a normal subgroup of G and H is a normal subgroup of K) $K/H \cong \langle N \rangle$. Then, by the third isomorphism theorem, $(\mathbb{Z} \times \mathbb{Z})/K \cong ((\mathbb{Z} \times \mathbb{Z})/H)/(K/H)$.

Now, since $(\mathbb{Z} \times \mathbb{Z})/H \cong \mathbb{Z}$ and $K/H \cong \langle N \rangle$, let g be the isomorphism given in the first isomorphism theorem taking $(\mathbb{Z} \times \mathbb{Z})/H \to \mathbb{Z}$ and $\pi : \mathbb{Z} \to \mathbb{Z}/\langle N \rangle$ the quotient homomorphism. Then, the function $\pi \circ g : (\mathbb{Z} \times \mathbb{Z})/H \to \mathbb{Z}/\langle N \rangle$ is a surjective homomorphism. Further, the kernel of $\pi \circ g$ is the preimage of the kernel of π under g, namely $g^{-1}(\langle N \rangle)$. However, the way that the first isomorphism theorem constructs the isomorphism g gives that $f = g \circ \pi'$ where $\pi' : (\mathbb{Z} \times \mathbb{Z}) \to (\mathbb{Z} \times \mathbb{Z})/H$ is the quotient homomorphism, but $f(K) = \langle N \rangle$, so $g(\pi'(K)) = g(K/H) = \langle N \rangle$. In particular, since g is a bijection, we can invert this to $K/H = g^{-1}(\langle N \rangle)$. Finally, we have that by the first isomorphism theorem, $((\mathbb{Z} \times \mathbb{Z})/H)/(K/H) \cong \mathbb{Z}/\langle N \rangle = \mathbb{Z}/N\mathbb{Z}$, as desired.

Problem 8

($\implies$) Let f by a homomorphism $G \to H$; then, since G is simple and $\ker f$ is a normal subgroup of G, either $\ker f = \{1\}$ or $\ker f = G$. In the first case, f is injective, and in the second, f is trivial since every element is mapped to the identity.

($\impliedby$) If every homomorphism $f : G \to H$ is either trivial or injective, the quotient homomorphism $\pi : G \to G/K$ for some normal subgroup K of G is either trivial or injective. In particular, if it is trivial, then every $g \in G$ satisfies $\pi(g) = gK = K$ for every $g \in G$, so $g \in K$ for every $g \in G$, so $K = G$. If it is injective, then $K = \{1\}$; to see this suppose otherwise, such that K contains both 1 and some other distinct element $g \in G$ (we can do this since $G \neq \{1\}$). Then, $\pi(1) = K$ and $\pi(g) = gK = K$ since K is closed under the operation, so π is not injective; $\Rightarrow\Leftarrow$, so $K = \{1\}$. These two are clearly mutually exclusive, so we have that the only possibilities for normal subgroups of G are $\{1\}$ and G itself, so it is simple.

Problem 9

Consider that for any normal subgroup H of S_n, $H \cap A_n \lhd A_n$ by past homework and also the notes. However, since the only normal subgroups of A_n are itself and the trivial group, either $H \cap A_n = \{1\}$ or $H \cap A_n = A_n$. In the latter case, we have that $A_n \leq H \leq S_n \implies |A_n| \leq |H| \leq |S_n|$ since all of these groups are finite. Then, $|S_n|/|H| \leq |S_n|/|A_n| = 2$, but by Lagrange $|S_n|/|H|$ is integral, so $|S_n|/|H| = 1 \implies |H| = |S_n|$, and since these groups are finite and H is contained in S_n, $|H| = |S_n| \implies H = S_n$. The second case is that $|S_n|/|H| = 2 \implies |H| = |A_n| = |H \cap A_n|$, but then $|H \cap A_n| = |H| \iff H \cap A_n = H$ for finite sets. In either case, either $H = S_n$ or $H = A_n$.

Then, if $H \cap A_n = \{1\}$, we have that H must be composed of odd permutations only (and the identity). Then, consider that $\varepsilon : H \to \{\pm 1\}$ where ε returns the sign of the permutation, is a homomorphism since it is a homomorphism on S_n. Clearly only one element of H can be even (that is, the identity), since otherwise $H \cap A_n$ would contain multiple elements. Then, the kernel of ε is exactly the identity, so ε is injective, so $|H| \leq 2$ (otherwise, there are > 2 distinct nonidentity elements, all of which have sign -1, so ε would not be injective). Then, by problem 5, $H \leq Z(G)$, but by an earlier homework (problem 8, HW 8), the only element that commutes with everything in S_n, $n \geq 3$ is the identity, so $H = \{1\}$. Thus, any normal subgroup of S_n is either $1, A_n, S_n$ (for $n \geq 5$).