Math 110AH Homework 5

Nathan Solomon

November 9, 2023

Assignment due November 9th at 11:59 pm
Questions 2, 5(a), 6, and 10 will be graded.

1

- (a) Let $H \subset G$ be a subgroup. Show that H is the image of a homomorphism from some group to G.
- (b) Let $N \subset G$ be a normal subgroup. Show that N is the kernel of a homomorphism from G to some group.

- (a) Let $f : H \to G$ be an inclusion map (aka "the canonical homomorphism"), defined by $f(h) = h$ for any $h \in H$. Then f is a homomorphism, and its image is H.
- (b)

2

Let n be a positive integer. Show that the map

$$f : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}, \qquad f(a + \mathbb{Z}) = na + \mathbb{Z}$$

is a well defined homomorphism. Find $Ker(f)$ and $Im(f)$.

Let z_1, z_2 be any integers. Then

$$f(a + z_1) = n(a + z_1) + \mathbb{Z} = n(a + z_2) + (nz_1 - nz_2 + \mathbb{Z}) = n(a + z_2) + \mathbb{Z} = f(a + z_2).$$

This proves that $f(a + \mathbb{Z})$ is the same no matter which representative element of $\mathbb{Z}$ we use, so f is well defined.

Also, f is a homomorphism, because

$$f(a+\mathbb{Z}) + f(b+\mathbb{Z}) = na + nb + \mathbb{Z} = f(a+b+\mathbb{Z}).$$

The coset $a+\mathbb{Z}$ is in the kernel of f if an only if $na+\mathbb{Z} = \mathbb{Z}$. In other words, $Ker(f)$ is the set of integer multiples of $1/n$.

Also, f is a surjective map because for any $b+\mathbb{Z}$ in the codomain, you can let $a = b/n$, so then $f(a+\mathbb{Z}) = na+\mathbb{Z} = b+\mathbb{Z}$. Since f is surjective, its image is the same as its codomain.

We have shown that f is a well defined homomorphism with

$$Ker(f) = \frac{1}{n} \cdot \mathbb{Z}$$

and

$$Im(f) = \mathbb{Q}/\mathbb{Z}.$$

3

Let $K \subset H \subset G$ be subgroups. Show that if K has finite index in G then $[G : K] = [G : H][H : K]$.

Note: everyone's first thought when they see this is to use Lagrange's theorem, but that's only applicable if G is a finite group.

4

Let $H \subset G$ be a subgroup. Show that the correspondence $Ha \mapsto a^{-1}H$ is a bijection between the sets of right and left cosets of H in G.

Proof outline: first, I'll prove that that mapping is injective, then I'll prove it's surjective.

- Let $a_1^{-1}H$ and $a_2^{-1}H$ be any two left cosets in the image of that map. If those two cosets are equal, then $a_2 a_1^{-1} \in H$, which means

  $$Ha_1 = (Ha_2a_1^{-1})a_1 = Ha_2.$$

  Since $a_1^{-1}H = a_2^{-1}H$ implies $Ha_1 = Ha_2$, that map is injective.

- Let bH be any left coset of H in G. Then Hb^{-1} is a right coset of H which that correspondence maps to bH. Therefore that correspondence is surjective.

Note: whenever I say something like "let $a^{-1}H$ be a left coset of H", what I really mean is "take any left coset of H, and call one element of that coset a^{-1}. Then that coset can be written as $a^{-1}H$."

Since that correspondence is both injective and surjective, it is a bijection (from the set of right cosets of H to the set of left cosets of H).

5

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

- (a) Let H' be a subgroup of H. Show that $G' = f^{-1}(H')$ is a subgroup of G. Prove that the correspondence $H' \mapsto G'$ is a bijection between the set of all subgroups of H and the set of all subgroups of G containing $Ker(f)$.
- (b) Let H' be a normal subgroup of H. Show that $G' = f^{-1}(H')$ is a normal subgroup of G. Prove that $G/G' \simeq H/H'$ and the correspondence $H' \mapsto G'$ is a bijection between the set of all normal subgroups of H and the set of all normal subgroups of G containing $Ker(f)$.

6

Show that every subgroup of index 2 is normal.

Let H be a subgroup of index 2 in G. We want to show that for any $h \in H$ and any $g \in G$, $g^{-1}hg \in H$. There are two cases to consider: when $g \in H$, and when $g \in G \backslash H$.

- If $g \in H$, then $g^{-1}hg$ is the product of three elements which are all in H, so $g^{-1}hg \in H$.
- If $g \notin H$, then hg is also not in H, because if it were, that would imply $h^{-1}(hg) = g$ is in H. Since H is index two, there are only two left cosets of H, which are H and gH, and the union of those two cosets is G. Since hg is not in H, it must be in gH, which means $g^{-1}hg \in g^{-1}gH = H$.

We have shown that for any $h \in H$ and any $g \in G$ (regardless of whether $g \in H$), $g^{-1}hg \in H$, so H is normal. The only restriction we placed on H is that it is a subgroup of index 2, so this proves that any subgroup of index 2 is normal.

7

Let $H \subset G$ be a subgroup. Suppose that for any $a \in G$ there exists $b \in G$ such that $aH = Hb$. Show that H is normal in G.

8

Show that the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, m > 1$, can be generated by three elements and cannot be generated by two elements.

Let $g_1 = (1,0,0), g_2 = (0,1,0), g_3 = (0,0,1)$. Then any element (x_1, x_2, x_3) of that group is equal to $x_1g_1 + x_2g_2 + x_3g_3$, so the three g_i's together generate $(\mathbb{Z}/m\mathbb{Z})^3$.

Now consider any two elements $x_1, x_2 \in (\mathbb{Z}/m\mathbb{Z})^3$. Since $\langle x_1, x_2 \rangle$ is abelian, any element of $\langle x_1, x_2 \rangle$ can be written as $a \cdot x_1 + b \cdot x_2$ for some integers a and b. However, $m \cdot x_1 = 0 = m \cdot x_2$, so there are only m possible values each for $a \cdot x_1$ and $b \cdot x_2$. Therefore the order of $\langle x_1, x_2 \rangle$ is at most m^2, which is less than the order of $(\mathbb{Z}/m\mathbb{Z})^3$, so those two groups are not equal. That means $(\mathbb{Z}/m\mathbb{Z})^3$ cannot be generated by two elements.

9

Let p be an odd prime. Prove that the congruence $x^2 \equiv -1 \pmod{p}$ has an integer solution if and only if $p \equiv 1 \pmod{4}$. (Hint: use Fermat's Little Theorem assuming we know that the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.)

- If $p \equiv 1 \pmod{4}$ then let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and let n be the smallest natural number such that $g^n = -1$. We know the order of g is $p-1$, so $n < p-1$. Also, $g^{2n} = (-1)^2 = 1$, so the order of g (which is $p-1$) must divide $2n$. This is enough for us to determine that $n = (p-1)/2$. Since $p-1$ is a multiple of 4, we can define $x := g^{(p-1)/4}$ which satisfies the property $x^2 \equiv -1 \pmod{p}$.
- If $p \equiv 3 \pmod{4}$ then suppose there exists some integer x such that $x^2 \equiv -1 \pmod{p}$. It's pretty clear that x is not ± 1, so $n = 4$ is the smallest natural number such that $x^n = 4$. We know the order of every element in a group must divide the order of the group, but x has order 4, and $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $p-1$, which is not divisible by 4. This is a contradiction, so there cannot be any integers x such that $x^2 \equiv 1 \pmod{p}$.

Since p is an odd prime, it must be congruent to either 1 or 3 (mod 4). By considering those two cases, we have proven that there exists a solution $x \in \mathbb{Z}$ to the congruence $x^2 \equiv -1 \pmod{p}$ if and only if $p \equiv 1 \pmod{4}$.

10

Prove that if a group G contains a subgroup H of finite index, then G contains a normal subgroup N of finite index such that $N \subset H$. (Hint: Consider the homomorphism of G to the symmetric group of all left cosets of H in G taking any $x \in G$ to f_x defined by $f_x(aH) = xaH$.)