Math 110AH Homework 6

Nathan Solomon

November 16, 2023

Assignment due November 16th at 11:59 pm.
Problems 1, 8, and 10 are graded.

1

Assume that a subset $S \subset G$ of a group G satisfies $gSg^{-1} \subset S$ for all $g \in G$. Prove that the subgroup $\langle S \rangle$ generated by S is normal in G.

Remember that $\langle S \rangle$ can be defined as

$$\langle S \rangle = \{s_1^{p_1} s_2^{p_2} \dots s_n^{p_n} : n \in \mathbb{N}_0, \text{ and for every index } j \leq n, \, s_j \in S \text{ and } p_j \in \mathbb{N}\}.$$

Now take an arbitrary element $s_1^{p_1} s_2^{p_2} \dots s_n^{p_n}$ of that subgroup and conjugate it by an arbitrary element $g \in G$. We can now show that the new element is also in $\langle S \rangle$:

$$g(s_1^{p_1} s_2^{p_2} \dots s_n^{p_n})g^{-1} =$$
$$(gs_1^{p_1} g^{-1})(gs_2^{p_2} g^{-1}) \dots (gs_n^{p_n} g^{-1}) =$$
$$(gs_1 g^{-1})^{p_1} (gs_2 g^{-1})^{p_2} \dots (gs_n g^{-1})^{p_n} \in \langle S \rangle.$$

That last step is valid because for any index $j \leq n$, the fact that $s_j \in S$ implies $gs_j g^{-1} \in S$, and by the definition of $\langle S \rangle$, the finite product of elements of S is also in $\langle S \rangle$.

2

Prove that for every integer $n > 0$ there exists a unique cyclic subgroup $H_n \subset \mathbb{Q}/\mathbb{Z}$ of order n.

For any n, let $h_n = \frac{1}{n}$ and let $H_n = \langle h_n \rangle$. For any integer a, $a \cdot h_n$ is an integer if and only if a is an integer multiple of n. Therefore h_n and H_n both have order n. Now we just need to show that H_n is unique.

Suppose there exists some other cyclic subgroup G of $\mathbb{Q}/\mathbb{Z}$ which has order n. Then since it's cyclic, there exists a generator $g \in G$ such that g has order n. In other words, $n \cdot g$ is an integer, which means g is an integer multiple of $\frac{1}{n}$. Since G is generated by g, every element of G is an integer multiple of $\frac{1}{n}$. H_n is the set of all integer multiples of $\frac{1}{n}$, and we know that H_n and G both have n elements, so $H_n = G$. Therefore H_n is unique.

3

Let $H_n \subset G = \mathbb{Q}/\mathbb{Z}$ be a cyclic subgroup of order n. Prove that G/H_n is isomorphic to G. (Hint: consider the homomorphism $f : G \to G, f(x) = nx$.)

In the previous problem, we found the unique group H_n which satisfies that property. Now let $f : G/H_n \to G$ be the function defined by $f([x]) = n[x]$. We need to show that f is a homomorphism, it's well-defined, and it's bijective.

- **Homomorphism:** $f(x_1) + f(x_2) = nx_1 + nx_2 = n(x_1 + x_2) = f(x_1 + x_2)$.
- **Well-defined:** For any element $[x] \in G/H_n$, let x_1 and x_2 be any two representative elements of $[x]$. Then $x_2 - x_1$ is an integer multiple of $1/n$, since $x_2 - x_1 \in H_n$, which means
$$f(x_1) = nx_1 + \mathbb{Z} = n(x_1) + n(x_2 - x_1) + \mathbb{Z} = nx_2 + \mathbb{Z} = f(x_2).$$
- **Injective:** Let x_1, x_2 be distinct elements of G/H_n, meaning $x_1 - x_2$ is not an integer multiple of $1/n$. Then
$$f(x_1) - f(x_2) = n(x_1 - x_2)$$
which is not an integer, so $f(x_1) \neq f(x_2)$.
- **Surjective:** For any element $x \in G$, x/n is in G/H_n and $f(x/n) = n(x/n) = x$.

Therefore f is an isomorphism from G/H_n to G.

4

Find all elements of finite order in $\mathbb{R}/\mathbb{Z}$.

First, I will show rational numbers have finite order, then I will show that irrational elements do not have finite order.

Let $[x] \in \mathbb{Q}/\mathbb{Z}$ be any rational number in that group. Then there exist integers a and b such that $[x] = [\frac{a}{b}]$. Since $|b| \cdot [x] = [\frac{a \cdot |b|}{b}] = [0]$, the order of $[x]$ is at most $|b|$, so it's finite. Therefore every rational number in $\mathbb{R}/\mathbb{Z}$ has finite order.

Now let $[x] \in (\mathbb{R}/\mathbb{Z})\backslash(\mathbb{Q}/\mathbb{Z})$ be an irrational number, and suppose $[x]$ has finite order b in $\mathbb{R}/\mathbb{Z}$. That means $[b \cdot x] = 0$, so let x be any representative element of $[x]$, and $b \cdot x$ will be an integer, which we'll call a. Then $x = \frac{a}{b} \in \mathbb{Q}$, so $[x] \in \mathbb{Q}/\mathbb{Z}$, which is a contradiction. Therefore any element $[x] \in \mathbb{R}/\mathbb{Z}$ that is not in $\mathbb{Q}/\mathbb{Z}$ cannot have finite order.

The set of elements in $\mathbb{R}/\mathbb{Z}$ with finite order is $\mathbb{Q}/\mathbb{Z}$.

5

Show that $Aut(\mathbb{Z})$ is a cyclic group of order 2. What is $Inn(\mathbb{Z})$?

Let f be an automorphism on $\mathbb{Z}$. For any $n \in \mathbb{Z}, n \cdot 1$, so 1 is a generator of $\mathbb{Z}$. Isomorphisms map generators to generators, so $f(1)$ must also be a generator (of $\mathbb{Z}$). If $|f(1)| = n$, then the group generated by $f(n)$ is all the integer multiples of n, which is equal to $\mathbb{Z}$ if and only if $n = \pm 1$. Let f be the identity map on $\mathbb{Z}$ and let g be the negation map, so $Aut(\mathbb{Z}) = \{f, g\}$. Since $f^2 = g^2 = f$, this is the cyclic group of order 2.

The group of integers is abelian, so $\mathbb{Z} = Z(\mathbb{Z})$. Using the fact that $G/Z(G) \cong Inn(G)$ for any group G and the fact that G/G is the trivial group, we see that $Inn(\mathbb{Z})$ is the trivial group.

6

Prove that every automorphism of S_3 is inner.

Let $\varphi : S_3 \to Aut(S_3)$ be the homomorphism defined by $\varphi(g)(h) = ghg^{-1}$. As shown in question 8, the center of S_3 is trivial, and since the kernel of φ is equal to the center of S_3, φ has to be injective. $Inn(S_3)$ is equal to the image of φ, so $Inn(S_3)$ has 6 elements – the same as $|S_3|$.

We know that the elements of S_3 are

$$\{e, (12), (13), (23), (123), (132)\}.$$

Let f be any automorphism on S_3. Then f must map (12) to some order 2 element. There are 3 options for $f((12))$, since S_3 has 3 elements with order 2. Then f must map (23) to a different order 2 element, which gives 2 options. Since S_3 is generated by (12) and (23), these two choices fully determine f, so there are 6 possible values of f.

We know that $Inn(S_3) \subset Aut(S_3)$, but we have just shown that those groups both have 6 elements, so they must be equal.

7

Prove that $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ is isomorphic to the symmetric group S_3. (Hint: Notice that every automorphism of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ permutes all three nonzero elements of the group.)

Label the elements of K_4 as $a = (0,0), b = (1,0), c = (0,1), d = (1,1)$. Let $\varphi : S_3 \to Aut(K_4)$ be the function defined by the following table. One can check that all of the functions $\varphi(p) : K_4 \to K_4$ are indeed isomorphisms. Also, one can check that φ is an isomorphism by comparing the multiplication table for S_3 to the multiplication table for $Aut(K_4)$, or just by noticing that the right hand side of the table resembles the permutation p. The last thing to check is that we have listed all 6 elements of S_3 and of $Aut(K_4)$ – we know $|S_3| = 3! = 6$, and we can confirm that there are no more automorphisms on K_4, because automorphisms fix the identity (a) and are bijections.

$p \in S_3$	$(\varphi(p)(a), \varphi(p)(b), \varphi(p)(c), \varphi(p)(d))$
e	(a, b, c, d)
(12)	(a, c, b, d)
(13)	(a, d, c, b)
(23)	(a, b, d, c)
(123)	(a, c, d, b)
(132)	(a, d, b, c)

8

Show that the center of S_n is trivial if $n \geq 3$.

In this proof, I'll use L to mean any set with n elements, and S_n to mean the set of bijections from L to L.

Let $p \in S_n$ (where $n \geq 3$) be a nontrivial permutation of a set of n letters, which I'll call L. Then there exists elements $a, b \in L, a \neq b$, such that $p(a) = b$. Since L has at least 3 elements, we can let $c \in L$ be an element other than a or b, and let $q \in S_n$ be the transposition which switches b and c, but does not change any other elements of L.

One can check that $q \circ p$ maps a to c, but $p \circ q$ maps a to b, so $q \circ p \neq p \circ q$. We have shown that for any element $p \in S_n$, if $n \geq 3$, there exists an element $q \in S_n$ which does not commute with p, so the center of S_n is trivial.

9

- (a) A subgroup H of G is called *characteristic*, if $f(H) = H$ for any automorphism f of G. Show that a characteristic subgroup of H is normal in G.
- (b) Prove that if K is a characteristic subgroup of H and H is a characteristic subgroup of G, then K is characteristic subgroup of G.
- (c) Prove that if K is a characteristic subgroup of H and H is normal in G, then K is normal in G.

- (a) For any element $g \in G$, let f be the automorphism on G which maps h to ghg^{-1}. If H is a characteristic subgroup of G, then $f(h) \in H$ for any $h \in H$, so $H \trianglelefteq G$.
- (b) Let f be any automorphism of G. Then $f(H) = H$, so the restriction $f|_H$ is an automorphism of H. Since K is a characteristic subgroup of H, $f|_H(K) = K$, meaning $f(K) = K$, so K is a characteristic subgroup of G.
- (c) For any $k \in K$ and any $g \in G$, let $f : G \to G$ be the automorphism which maps any element $h \in G$ to ghg^{-1}. Since H is normal in G, $f(H) = H$, so the restriction $f|_H$

is an automorphism of H. Then K is a characteristic subgroup of H, so $f(K) = K$, meaning $gkg^{-1} \in K$, so $K \trianglelefteq G$.

10

Let N be an abelian normal subgroup of a finite group G. Assume that the orders $|G/N|$ and $|Aut(N)|$ are relatively prime. Prove that N is contained in the center of G. (Hint: Consider the conjugation homomorphism $f : G \to Aut(N), f(g)(n) = gng^{-1}$.)

Let f be the function defined in the hint. Then $Ker(f)$ is the set of elements $g \in G$ such that $f(g)$ is the identity map on N – that is, such that g commutes with every element of N. Since N is abelian, it is clearly a subgroup of $Ker(f)$. Also, by the first isomorphism theorem, $Ker(f)$ is a normal subgroup of G, so we have

$$N \subset Ker(f) \trianglelefteq G.$$

By the the third isomorphism theorem, that implies

$$\frac{G/N}{Ker(f)/N} \cong G/Ker(f).$$

Now we can apply the first isomorphism theorem to replace $G/Ker(f)$ with $Im(f)$.

$$\frac{G/N}{Ker(f)/N} \cong Im(f) \subset Aut(N).$$

Applying Lagrange's theorem to that, we get

$$\frac{|G/N|}{|Ker(f)/N|} < |Aut(N)|.$$

Since $|G/N|$ and $|Aut(N)$ are coprime, and $|Ker(f)/N|$ is an integer, we know the two sides of that inequality are coprime, but since the left hand side is smaller, the left hand side is one. By Lagrange's theorem again, that implies $Ker(f) = G$, meaning every element of N commutes with every element of G. Therefore $N \subset Z(G)$.