Math 110AH Homework 4

Nathan Solomon

November 8, 2023

Assignment due November 1st at 11:59 pm

1. Prove that the group $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ is cyclic if and only if the m_i's are pairwise relatively prime. (Hint: Let n be the least common multiple of the m_i's. Show that $nx = 0$ for any x in the group.)

- If the m_i's are pairwise coprime, then for any element $x = (x_1, x_2, \ldots, x_k)$ in that group, by the Chinese Remainder Theorem, there exists a unique number n such that $[n]_{m_1} = x_1, [n]_{m_2} = x_2, \ldots, [n]_{m_k} = x_k$. Let $g = (1, 1, \ldots, 1)$. Then $n \cdot g = x$. Since this works for any x in that group, g is a generator of that group, so it's cyclic.
- If the m_i's are not pairwise coprime, then let i and j be distinct indices such that $\gcd(m_i, m_j) > 1$, and let $n = m_1 \times m_2 \times \cdots \times m_k / \gcd(m_i, m_j)$. Then n is an integer which divides all of the m_i's, so for any element $x = (x_1, x_2, \ldots, x_k)$ in that group, $nx = 0$. Therefore the order of x is less than or equal to n, which is less than the product of all the m_i's. Since the order of every element x in that group is less than the order of that group, that group is not cyclic.

Note: another way to do this problem would be to show that the LCM of a set of numbers is equal to their product if and only if they are pairwise coprime. This would make the rest of the proof very easy.

2. Let K and H be two subgroups of a group G. Prove that the union $K \cup H$ is a subgroup if and only if either $K \subset H$ or $H \subset K$.

- Suppose either $K \subset H$ or $H \subset K$. Without loss of generality, we can say that $K \subset H$. Then $K \cup H = H$, which we already said is a subgroup of G.
- Suppose K is not a subgroup of H and H is not a subgroup of K. Then there exist elements $k \in K \backslash H$ and $h \in H \backslash K$. Their product, kh, is not in K, because if it were, then $k^{-1}(kh) = h$ would also be in K. By the same logic, kh can't be in H, so $K \cup H$ is not a subgroup (because it's not closed under multiplication).

3. Show that if K and H are two finite subgroups in a group G of relatively prime order, then $K \cap H = \{e\}$.

Let $a \in G$ be any element which is in K and also in H, and let d be the order of a. According to Lagrange's theorem, d must divide the order of K, and it also must divide the order of H. Since $|K|$ and $|H|$ are coprime, this would imply $d = 1$, so a has to be the identity. K and H both contain e, and we just showed their intersection can't contain anything other than e, so

$$K \cap H = \{e\}.$$

4. Show that if a group G has only a finite number of subgroups, then G is finite. (Hint: Note that G is the union of cyclic subgroups.)

First, note that

$$G = \text{union of all cyclic subgroups of } G = \bigcup_{g \in G} \langle g \rangle.$$

This is true because the right hand side contains every element of G, but since $\langle g \rangle \subset G$ (for any $g \in G$), it can't contain anything that is not in G.

Lemma 1. *Any cyclic group $\langle g \rangle$ with finitely many subgroups is finite.*

Proof. If $\langle g \rangle$ is infinite, then

$$\langle g \rangle = \{\dots, g^{-1}, e, g, g^2, g^3, \dots\}$$

and all of the elements g^a, g^b are distinct – if they weren't, then we could say $g^{b-a} = e$. However, that would imply any element g^x is equal to g^r, where r is the remainder when x is divided by $b - a$. But if that were true, then $\langle g \rangle$ would have $|b - a|$ elements, which is a contradiction, since $|b - a| < \infty$.

Since the elements $\{\dots, g^{-1}, e, g, g^2, \dots\}$ are all distinct, $\{\langle g^2 \rangle, \langle g^3 \rangle, \langle g^4 \rangle, \dots\}$ are all distinct subgroups of $\langle g \rangle$.

Therefore if $\langle g \rangle$ is infinite, it has infinitely many subgroups. The contrapositive of that is also true: if $\langle g \rangle$ has finitely many subgroups, it is finite. □

We showed above that G is equal to the union of all the cyclic subgroups of G. Since G has only finitely many cyclic subgroups, and all of the cyclic subgroups have finitely many elements, G has finitely many elements.

5. Prove that if a is an element of a finite group G such that $ord(a) = |G|$, then G is cyclic.

Consider the x^{th} and y^{th} (where $x \neq y$) terms of the sequence

$$A := \{a, a^2, \dots, a^{|G|}\}$$

and suppose without loss of generality that $x < y$. Then $a^{y-x} \neq e$, because $0 < y - x < ord(a)$, which means $a^x \neq a^x a^{y-x} = a^y$, so the x^{th} and y^{th} terms in A are distinct.

Because this is true for any $x, y \in \{1, 2, \ldots, |G|\}$ (such that $x \neq y$), no two terms in A are equal to each other. Since A contains $|G|$ terms which are all distinct elements of G, a is a generator for G, so G is cyclic.

6. Find a non-cyclic group of the smallest order.

Solution outline: there are two steps here. First, we show that K_4 is not cyclic, then we show that any group with 3 elements or fewer has to be cyclic. For that second step, we only need to consider groups with 1, 2, or 3 elements, because every group has either infinitely many elements or a natural number of elements.

Let $\mathbb{Z}_2 = \{0, 1\}$ be the additive group of integers modulo 2. Then define the Klein 4-group as

$$K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}.$$

The identity element in K_4 is $(0,0)$, and we can easily see that all other elements have order 2. Since K_4 has order 4 but no element of order 4 (that is, no generator), it is not cyclic.

If a group G has one element, it is the trivial group, which is cyclic because the identity generates it.

If G has two elements, a and b, then one of those elements (lets say a) has to be the identity. Since b is not the identity, $b^2 \neq b$, therefore $b^2 = a$, so b is a generator.

Now suppose G has three elements, a and b and c, and suppose a is the identity. Then b and c must be inverses, because if they were not, it would be possible to form a 4th element bc which is not equal to the identity, but is also not equal to b or to c. Therefore $b^{-1} = c$, and we also know that $b^0 = a$ and $b^1 = b$, so b generates G.

Therefore if G is a group with one, two, or three elements, it must be cyclic, but K_4 is a group with 4 elements that is not cyclic.

7. Find all subgroups of S_3 and determine which ones are normal.

In cycle notation, the elements of S_3 are

$$S_3 = \{e, (12), (13), (23), (123), (132)\}.$$

Now we want to list all subgroups of S_3. To do this, we consider the trivial group $\{e\}$, then all of the subgroups generated by one element, then all of the subgroups generated by two elements, and so on. That process is not as tedious as it sounds, because most of the subgroups we come across will have already been listed, so we can skip them.

Then for each of the subgroups we list, we can check whether it's normal by conjugating by all the elements outside of the subgroup (except this is not necessary for the subgroup $\{e\}$, because $geg^{-1} = e$ for any $g \in S_3$).

Subgroup	Order	Normal
$\{e\}$	1	yes
$\langle(12)\rangle$	2	no
$\langle(13)\rangle$	2	no
$\langle(23)\rangle$	2	no
$\langle(123)\rangle$	3	yes
S_3	6	yes

8. Prove that if H is a subgroup of G then $\langle H\rangle = H$.

We have defined $\langle H\rangle$ to be the group of all "words" $h_1h_2\cdots h_n$ where each h_i is an element of H. Since H is closed under multiplication, that product is also in H. Therefore every element of $\langle H\rangle$ is in H. And obviously every element in H is in $\langle H\rangle$, so we conclude that H and $\langle H\rangle$ are equal.

9. Show that the groups $GL_2(\mathbb{Z}/2\mathbb{Z})$ and S_3 are isomorphic. (Hint: Compare the multiplication tables.)

In homework 3, we proved that for any prime number p, the group $GL_n(\mathbb{Z}/p\mathbb{Z})$ has exactly

$$\prod_{i=0}^{n-1}(p^n - p^i)$$

distinct elements, and we described an algorithm for finding those elements. When n and p are both 2, that expression is equal to 6. Now lets label the 6 elements of $GL_2(\mathbb{Z}/2\mathbb{Z})$ as follows:

a	b	c	d	e	f
$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&0\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}1&1\\1&0\end{bmatrix}$	$\begin{bmatrix}1&0\\1&1\end{bmatrix}$

The multiplication table for these elements is

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	f	c	d
c	c	d	a	b	f	e
d	d	c	f	e	a	b
e	e	f	b	a	d	c
f	f	e	d	c	b	a

Note that S_3 contains $3! = 6$ elements, and when we label those elements (which are written in one-line notation) as follows, we get the exact same multiplication table as above, meaning $GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$.

a	b	c	d	e	f
(123)	(213)	(132)	(312)	(231)	(321)

10. Prove that every homomorphism $f : \mathbb{Q} \to \mathbb{Z}/m\mathbb{Z}$ is trivial, i.e. $f(x) = [0]_m$ for all $x \in \mathbb{Q}$.

Lemma 2. *For any natural number n, any element g of a multiplicative group G, and any homomorphism f from G to another multiplicative group,*

$$f(g^n) = f(g)^n.$$

Proof. The base case, where $n = 1$, is obvious. If the lemma is true for some n, then it is also true for $n + 1$, because

$$f(g^{n+1}) = f(g \cdot g^n) = f(g) \cdot f(g^n) = f(g) \cdot f(g)^n = f(g)^{n+1}.$$

So by induction, the lemma is true for all $n \in \mathbb{N}$. □

Let $f : \mathbb{Q} \to \mathbb{Z}/m\mathbb{Z}$ be a homomorphism. By the lemma above, $m \cdot f(x/m) = f(x)$. Since $f(x)$ is equal to m times an element of $\mathbb{Z}/m\mathbb{Z}$, we conclude that $f(x) = [0]_m$ (for any $x \in \mathbb{Q}$).