# Math 110AH Homework 3

Nathan Solomon

December 14, 2023

**Assignment due October 25th at 11:59 pm**

**1.** Prove that for an element $a$ of a group, $a^n \cdot a^m = a^{n+m}$ and $(a^{-1})^n = (a^n)^{-1}$ for every $n, m \in \mathbb{Z}$.

By definition,

$$a^n = \begin{cases} a \text{ multiplied by itself } n \text{ times if } n > 0 \\ \text{the identity element if } n = 0 \\ a^{-1} \text{ multiplied by itself } -n \text{ times if } n < 0 \end{cases}$$

If $n = 0$ then both parts of this question are obvious, and if $m = 0$, the first part is obvious. Therefore we only need to consider the cases where both $n$ and $m$ are either positive or negative.

- If $n$ and $m$ are both positive, then $a^n \cdot a^m$ is $a$ multiplied by itself $n+m$ times. If $n$ and $m$ are both negative, then $a^n \cdot a^m$ is $a^{-1}$ multiplied by itself $-n-m$ times, so we get $a^n \cdot a^m = a^{n+m}$ in this case too. If one of $(n, m)$ is positive but the other is negative, assume without loss of generality that $n$ is positive.

  If $n < -m$ then $a^n \cdot a^m = a^n \cdot (a^{-1})^{-m} = (a^{-1})^{-m-n} = a^{n+m}$. If $n > -m$ then $a^n \cdot a^m = a^n \cdot (a^{-1})^{-m} = a^{n-(-m)} = a^{n+m}$.

  We have proven that in all cases, $a^n \cdot a^m = a^{n+m}$.

- If $n$ is positive, $(a^{-1})^n \cdot a^n$ is $a^{-1}$ multiplied by itself $a$ times, times $a$ multiplied by itself $n$ times, which is clearly 1. If $n$ is negative, it's 1 again, for the exact same reason (except we use the property that $(a^{-1})^{-1} = a$). In either case, we get that $a^n$ is the inverse of $(a^{-1})^n$.

**2.** Show that $((ab)c)d = a(b(cd))$ for all elements $a, b, c, d$ of a group.

Repeatedly applying the associative rule, we get

$$\begin{aligned} ((ab)c)d &= (ab)(cd) \\ &= a(b(cd)). \end{aligned}$$

In the first line, we use the rule $(xy)z = x(yz)$ where $x = ab, y = c, z = d$, and to get to the second line, we use the same rule, except with $x = a, y = b, z = cd$.

**3.** Show that if $G$ is a group in which $(ab)^2 = a^2b^2$ for all $a, b, \in G$, then $G$ is abelian.

For any two elements $a, b \in G$, the product $ab$ can be rewritten as

$$ab = a^{-1}aabbb^{-1}.$$

But if we know that $(ab)^2 = a^2b^2$, then that's equivalent to

$$\begin{aligned} ab &= a^{-1}a^2b^2b^{-1} \\ &= a^{-1}(ab)^2b^{-1} \\ &= a^{-1}ababb^{-1} \\ &= ba. \end{aligned}$$

We have proven that $ab = ba$ for any elements $a, b \in G$, so $G$ is abelian.

**4.** Find all elements of order 3 in $\mathbb{Z}/18\mathbb{Z}$.

Suppose $x$ is an element that satisfies that property. Then $3x = 18m$ for some integer $m$. That's equivalent to $x = 6m$, so $x \in \{\dots, -6, 0, 6, 12, 18, \dots\}$. But in $\mathbb{Z}/18\mathbb{Z}$, that's equivalent to $\{0, 6, 12\}$. Now there are only 3 possible solutions, so we check them manually and see that the only elements of order 3 in $\mathbb{Z}/18\mathbb{Z}$ are 6 and 12.

**5.** Prove that the composite of two homomorphisms (resp. isomorphisms) is also a homomorphism (resp. isomorphism).

Suppose $f$ and $g$ are both group homomorphisms, and the domain of $f$ is the codomain of $g$. Then for any $a, b$ in the domain of $g$,

$$f(g(a)) \times f(g(b)) = f(g(a) \times g(b)) = f(g(a \times b))$$

so $f \circ g$ is a group homomorphism.

Suppose $f$ and $g$ are isomorphisms. Then in addition to being group homomorphisms (which implies $f \circ g$ is a group homomorphism), they are also both injective and surjective. According to a result from an earlier homework, that implies their composition is also injective and surjective. Since $f \circ g$ is a bijective group homomorphism, it is also an isomorphism.

**6.** Prove that the group $(\mathbb{Z}/9\mathbb{Z})^\times$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

*Alternate proof:* $(\mathbb{Z}/9\mathbb{Z})^\times$ *is a group with 6 elements and which has a generator (either 2 or 5), and* $\mathbb{Z}/6\mathbb{Z}$ *is a group of 6 elements which has a generator (either 1 or 5). This implies* *they are both isomorphic to the cylcic group of order 6 ($C_6$), and therefore isomorphic to each other. If this proof is rigorous enough for you, no need to read the rest of my answer.*

The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is defined as the multiplicative group of integers in $[0, n-1]$ which are coprime to $n$, so
$$\text{Forget}((\mathbb{Z}/9\mathbb{Z})^\times) = \{1, 2, 4, 5, 7, 8\}.$$
Now consider the function $f : \mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/9\mathbb{Z})^\times$, defined as
$$f(x) = 2^x \qquad \forall x \in \mathbb{Z}/6\mathbb{Z}.$$
By the properties of exponentials,
$$f(a) \cdot f(b) = 2^a \cdot 2^b = 2^{a+b} = f(a+b),$$
so $f$ is a homomorphism. Also, from the table below, we clearly see $f$ is bijective:

| x | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| f(x) | 1 | 2 | 4 | 8 | 7 | 5 |

Therefore $f$ is an isomorphism from $\mathbb{Z}/6\mathbb{Z}$ to $(\mathbb{Z}/9\mathbb{Z})^\times$.

**7.** Let $G$ be an abelian group an let $a, b \in G$ have finite order $n$ and $m$ respectively. Suppose that $n$ and $m$ are relatively prime. Show that $ab$ has order $nm$.

*Proof outline: First, I'll show that the order of ab is at most nm. Then if the order of ab is less than nm, I'll consider the case where the order is divisible by n, divisible by m, or divisible by both, and show that all of those cases lead to a contradiction.*

Since $G$ is abelian,
$$(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = 1^m 1^n = 1.$$
Let $x$ be the order of $ab$. Since $x$ is the smallest positive integer such that $(ab)^x = 1$, and $nm$ is a positive integer, $x$ cannot be larger than $nm$.

Since $n$ and $m$ are coprime, their greatest common divisor is $nm$. That means that if $x$ is a positive integer and $x < nm$, then either $n$ or $m$ will not divide $x$. Without loss of generality, we can suppose $x$ is not divisible by $n$ (and $m$ may or may not divide $x$; we still need to check both cases).

- If $m$ divides $x$, then $(ab)^x = a^x b^x = a^x \neq 1$, which contradicts our earlier statement that $n$ does not divide $x$.

- If $x$ isn't divisible by $n$ or by $m$, then let $c = a^x$. Since $(ab)^x = a^x b^x = 1$, $b^x$ must be equal to $c^{-1}$. We have shown that the subgroup generated by $a$ and the subgroup generated by $b$ both contain $c$. That means $c^n = 1$ and $c^m = 1$. Since $n$ and $m$ are coprime (and positive), that can only be true if $c$ is the identity.

  However, $c$ was defined as $a^x$, and the subgroup generated by $a$ has order $n$, and $n$ does not divide $x$, so $c$ cannot be the identity. This is also a contradiction.

We have shown that the order $x$ of $ab$ cannot be larger than $nm$, but also that if $x < nm$, then we get a contradiction in all cases. Therefore the order of $ab$ is $nm$.

**8.** a) Prove that for every positive integer $n$ the set of all complex $n$-th roots of unity is a cyclic group of order $n$ with respect to complex multiplication.
b) Prove that if $G$ is a cyclic group of order $n$ and $k$ divides $n$, then $G$ has exactly one subgroup of order $k$.

- (a) A number $z \in \mathbb{Z}$ is an $n^{th}$ root of unity if and only if it satisfies $z^n = 1$. By breaking $z$ into polar form (that is, $|z| \times \frac{z}{|z|}$), we see that $z$ must have magnitude 1 and an argument which, when multiplied by $n$, gives an integer multiple of $2\pi$. In other words, the $n^{th}$ roots of unity are

$$\{\exp(2\pi ik/n) : k \in \mathbb{Z}\}.$$

But by the division theorem, there exist integers $a, b$ such that $k = an+b$ and $0 \leq b < n$. Since $\exp(2\pi ik) = \exp(2\pi ian)\exp(2\pi ib/n)$, that set is equivalent to

$$\left\{\exp\left(\frac{2\pi ik}{n}\right) : k \in \{0, 1, 2, \ldots, n-1\}\right\}.$$

That set contains $n$ distinct elements, one of which is the multiplicative identity. Also, every element has a unique multiplicative inverse (which is its complex conjugate) and multiplication is associative. One can easily prove that all those properties hold, and that it's closed under multiplication, so it's a group. Specifically, it's the cyclic group of order $n$, because

$$\exp(2\pi i/n)$$

is a generator.

- (b) Let $g$ be a generator of $G$ and let $H$ be the set of all elements $a \in G$ such that $a^k = 1$. Then for each of those elements, there exists some $j$ such that $g^j = a$, which implies $g^{jk} = 1$. But since $g$ generates the whole group $G$, which has order $n$, $jk$ must be an integer multiple of $n$, and so $j$ is an integer multiple of $n/k$. Therefore $a$ is an element of

$$H = \{1, g^{n/k}, g^{2n/k}, \ldots, g^{(k-1)n/k}\}$$

which is a subgroup of order $k$. But if there's any other subgroup $H'$ of $G$ which also has order $k$, then every element $a'$ of that subgroup would also satisfy $(a')^k = 1$. According to the logic above, that would imply $a$ is in $H$, so we can conclude that $H$ is the only subgroup of order $k$.

**9.** Prove that if $G$ is a finite group of even order, then $G$ contains an element of order 2. (Hint: Consider the set of pairs $(a, a^{-1})$.)

Consider the set of ordered pairs $(a, a^{-1})$ for every element $a \in G$. Since there is one unique such pair for each element $a \in G$, there are an even number of those pairs.

Additionally, there are an even number of those pairs for which $a \neq a^{-1}$, and since an even number minus an even number is an even number, there must also be an even number of those pairs for which $a = a^{-1}$. We already know that there is one pair which satisfies that property: $(e, e)$. Therefore there must be at least one such pair in addition to $(e, e)$.

Call the first number of that other pair $a$. Then $a$ is not the identity, but it does satisfy $a = a^{-1}$ (which implies $a^2 = 1$), so it has order 2.

**10.** Find the order of $GL_n(\mathbb{Z}/p\mathbb{Z})$ for a prime integer $p$.

First, note that $\mathbb{Z}/p\mathbb{Z}$ is a ring with $p$ elements.

The $n^{th}$ general linear group over a ring is the set of $n$ by $n$ matrices over that ring for which all the columns are linearly independent. Any such matrix can be constructed by the following process: choose the first (leftmost) column to be any nonzero module (over that ring) with $n$ elements, then choose each column after that to be any module (over that ring) with $n$ elements that is linearly independent from all the other columns which have been chosen.

The first column can be anything except the zero vector, so there are $p^n - 1$ options. The $j^{th}$ column can be anything outside the span of the first $j-1$ columns. That span must have dimension $j-1$, meaning it contains $p^{j-1}$ distinct elements, so there are $p^n - p^{j-1}$ options for the $j^{th}$ column.

Therefore when choosing elements for the entire $n$ by $n$ matrix, there are

$$\left[p^n - p^0\right] \times \left[p^n - p^1\right] \times \left[p^n - p^2\right] \times \cdots \times \left[p^n - p^{n-1}\right]$$

distinct options. That expression can't really be simplified, so we conclude that the order of $GL_n(\mathbb{Z}/p\mathbb{Z})$ is

$$\prod_{i=0}^{n-1} [p^n - p^i].$$