Homework 3

Warren Kim

October 26, 2023

Please grade my HW carefully. Thank you.

Question 1

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

Response

Proof. Let a be an element of a group. Then, for every $n, m \in \mathbb{Z}$, we have

$$\begin{aligned} a^n \cdot a^m &= (a \cdot a \cdot \dots \cdot a) \cdot (a \cdot a \cdot \dots \cdot a) && n \text{ and } m \text{ times, respectively} \\ &= a \cdot a \cdot \dots \cdot a \cdot a \cdot a \cdot \dots \cdot a \\ a^n \cdot a^m &= a^{n \cdot m} \end{aligned}$$

We also want to show $\left(a^{-1}\right)^n = (a^n)^{-1}$. Then, it suffices to show that

$$a^n \cdot \left(a^{-1}\right)^n = e = a^n \cdot (a^n)^{-1}$$

Then,

$$\begin{aligned} a^n \cdot \left(a^{-1}\right)^n &= (a \cdot a \cdot \dots \cdot a \cdot a) \cdot (a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}) && \text{each } n \text{ times} \\ &= a \cdot a \cdot \dots \cdot a \cdot (a \cdot a^{-1}) \cdot a^{-1} \cdot \dots \cdot a^{-1} && \text{associativity} \\ &= a \cdot a \cdot \dots \cdot a \cdot e \cdot a^{-1} \cdot \dots \cdot a^{-1} \\ &= (a \cdot a \cdot \dots \cdot a \cdot a) \cdot (a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}) && \text{each } n-1 \text{ times} \\ a^n \cdot \left(a^{-1}\right)^n &= e && \text{by induction} \end{aligned}$$

Since inverses are unique, it must be the case that $\left(a^{-1}\right)^n = (a^n)^{-1}$. $\square$

Question 2

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

Response

Proof. Let a, b, c, d be elements of a group. Then by associativity, we get

$$((ab)c)d = (a(bc))d = a(b(cd))$$

$\square$

Question 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.

Response

Proof. Let G be a group, and assume $(ab)^2 = a^2b^2$ for all $a, b \in G$. That is,

$$\begin{aligned}
(ab)^2 &= a^2b^2 \\
(ab)(ab) &= (aa)(bb) \\
a^{-1}(ab)(ab)b^{-1} &= a^{-1}(aa)(bb)b^{-1} \\
(a^{-1}a)ba(bb^{-1}) &= (a^{-1}a)ab(bb^{-1}) && \text{associativity} \\
ebae &= eabe && aa^{-1} = e = a^{-1}a \\
ba &= ab
\end{aligned}$$

So, G is commutative; that is, G is abelian. $\square$

Question 4

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

Response

There are 18 cases:

$$\begin{gathered}
3 \cdot 0 = 0 \equiv 0 \ (mod\ 18) \\
3 \cdot 1 = 3 \equiv 3 \ (mod\ 18) \\
3 \cdot 2 = 6 \equiv 6 \ (mod\ 18) \\
3 \cdot 3 = 9 \equiv 9 \ (mod\ 18) \\
3 \cdot 4 = 12 \equiv 12 \ (mod\ 18) \\
3 \cdot 5 = 15 \equiv 15 \ (mod\ 18) \\
3 \cdot 6 = 18 \equiv 0 \ (mod\ 18) \\
3 \cdot 7 = 21 \equiv 3 \ (mod\ 18) \\
3 \cdot 8 = 24 \equiv 6 \ (mod\ 18) \\
3 \cdot 9 = 9 \equiv 9 \ (mod\ 18) \\
3 \cdot 10 = 12 \equiv 12 \ (mod\ 18) \\
3 \cdot 11 = 15 \equiv 15 \ (mod\ 18) \\
3 \cdot 12 = 18 \equiv 0 \ (mod\ 18) \\
3 \cdot 13 = 21 \equiv 3 \ (mod\ 18) \\
3 \cdot 14 = 24 \equiv 6 \ (mod\ 18) \\
3 \cdot 15 = 9 \equiv 9 \ (mod\ 18) \\
3 \cdot 16 = 12 \equiv 12 \ (mod\ 18) \\
3 \cdot 17 = 15 \equiv 15 \ (mod\ 18)
\end{gathered}$$

0 has order 1 since it is the identity, so it is not of order 3. 6 and 12 are both order 3 since 3 is the smallest positive integer such that $6 \cdot 3 \equiv 0 \ (mod\ 18)$ and $12 \cdot 3 \equiv 0 \ (mod\ 18)$, and are thus the only elements of order 3.

Question 5

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

Response

Homomorphism (i)

Proof. Let $f : G \to H$, $g : H \to K$ be two homomorphisms. Then,

$$f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2)$$
$$g(y_1 \cdot y_2) = g(y_1) \cdot g(y_2)$$

for all $x_1, x_2 \in G$ and for all $y_1, y_2 \in H$. The composition is $g \circ f : G \to K$.

$$\begin{aligned}
(g \circ f)(x_1 \cdot x_2) &= g(f(x_1 \cdot x_2)) \\
&= g(f(x_1) \cdot f(x_2)) && f \text{ is a homomorphism} \\
&= g(f(x_1)) \cdot g(f(x_2)) && g \text{ is a homomorphism} \\
(g \circ f)(x_1 \cdot x_2) &= (g \circ f)(x_1) \cdot (g \circ f)(x_2)
\end{aligned}$$

so the composition $g \circ f$ is a homomorphism. □

Isomorphism

Proof. It suffices to show that the composition of two homomorphisms (resp. bijections) is also a homomorphism (resp. bijection). Let $f : G \to H$, $g : H \to K$ be two bijections; i.e. they are injective and surjective. Then, $g \circ f : G \to K$ is the composition. We will show that this composition is also a bijection.

Injective

Take any $x_1, x_2 \in G$ and any $y_1, y_2 \in H$. Then,

$$\begin{aligned}
(g \circ f)(x_1) &= g(f(x_1)) \\
&= g(y_1) \\
&= g(y_2) && \text{Since } g \text{ is injective, } g(y_1) = g(y_2) \\
&= g(f(x_2)) && \text{Since } f \text{ is injective, } f(x_1) = f(x_2) \\
(g \circ f)(x_1) &= (g \circ f)(x_2)
\end{aligned}$$

So $g \circ f$ is injective.

Surjective

$$\begin{aligned}
(g \circ f)(x) &= g(f(x)) \\
&= g(y) && \text{Since } f \text{ is surjective, } y = f(x) \\
(g \circ f)(x) &= z && \text{Since } g \text{ is surjective, } z = g(y)
\end{aligned}$$

So $g \circ f$ is surjective. Therefore, $g \circ f$ is a bijection. From **(i)**, we know that the composition of two homomorphisms is also a homomorphism. Therefore, the composition of two isomorphisms is an isomorphism. $\square$

Question 6

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

Response

Proof. We have that $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$ and $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$. Note that both groups have order 6. Then, it suffices to show that both groups are cyclic, since two cyclic groups of equal order are isomorphic. Then, we find that 2 generates $(\mathbb{Z}/9\mathbb{Z})^\times$ since

$$\begin{aligned}
2^1 &= 2 \\
2^2 &= 4 \\
2^3 &= 8 \\
2^4 &= 16 \equiv 7 \ (mod\ 9) \\
2^5 &= 32 \equiv 5 \ (mod\ 9) \\
2^6 &= 64 \equiv 1 \ (mod\ 9)
\end{aligned}$$

so $(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic. Moreover, we have that 1 is a generator for the additive group $\mathbb{Z}/6\mathbb{Z}$ since

$$\begin{aligned}
1 \cdot 1 &= 1 \\
2 \cdot 1 &= 2 \\
3 \cdot 1 &= 3 \\
4 \cdot 1 &= 4 \\
5 \cdot 1 &= 5 \\
6 \cdot 1 &= 0
\end{aligned}$$

so $\mathbb{Z}/6\mathbb{Z}$ is cyclic. Since these two groups have the same order and are cyclic, they are isomorphic. $\square$

Question 7

Let G be an abelian group and 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.

Response

Proof. Let $a, b \in G$ have finite order n and m respectively. Assume that n and m are relatively prime; i.e. $\gcd(n, m) = 1$. Then,

$$\begin{aligned}
(ab)^{nm} &= a^{nm} b^{nm} \\
&= (a^n)^m (b^m)^n \\
&= e^m e^n \\
(ab)^{nm} &= e
\end{aligned}$$

Because n and m are coprime, $\operatorname{lcm}(n, m) = nm$, so ab has order nm. $\square$

Question 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 the 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.

Response

(a) *Proof.* Let $G = \left\{e^{2\pi ki/n} : k = 0, 1, \ldots, n-1\right\}$.

Closure
First, we show that G is closed under complex multiplication. Take any two elements $a, b \in G$. Then,

$$ab = e^{2\pi ji/n} \cdot e^{2\pi ki/n} = e^{2\pi(j+k)i/n}$$

Since j, k are integers, their sum $j+k$ is an integer. If $(j+k) > n$, due to the periodicity of teh function, it is equivalent to $(j+k) - n$. So, G is closed under complex multiplication.

Group
To show that G is a cyclic group of order n, we first need to show that it is a group with respect to complex multiplication; i.e.

(i) Since complex numbers are associative, we have that all elements in G is associative.

(ii) Let $k = 0$. Then, $e^{2\pi ki/n} = e^{2\pi(0)i/n} = e^0 = 1$. Then, for any $a \in G$, $1 \cdot a = a = a \cdot 1$. So, the identity element exists in G.

(iii) For any $a \in G$, define $a^{-1} = e^{2\pi(-k+n)i/n}$. So, we have that $a \cdot a^{-1} = 1 = a^{-1} \cdot a$. Therefore, there exists an inverse element in G.

So, G is a group.

G is cyclic and has order n
We find that the $e^{2\pi i/n}$ generates G:

$$\begin{aligned} e^{2\pi(0)i/n} &= e^{2\pi i} = 1 \\ e^{2\pi(1)i/n} &= e^{2\pi i/n} \\ &\vdots \\ e^{2\pi(n-1)i/n} &= e^{2\pi(n-1)i/n} \end{aligned}$$

so G is cyclic. Since G has n distinct elements, G has order n. $\square$

(b) *Proof.* ***Existence***

Let G be a cyclic group of order n and k divides n. Then, let $G = \langle g \rangle$ where g generates G since G is cyclic. Since $k \mid n$, we can write $n = kq$ for some integer q. Now consider the element $g^q \in G$. Then, the order of g^q is $(g^q)^s = g^{qs}$ for some integer s. But since g has order n, it is the smallest integer such that $g^n = e$. So, we have that

$$g^{qs} = g^n$$

which is true only when $s = k$. Then,

$$g^{qs} = g^{qk} = g^n = e$$

so g^q has order k. Now let $H = \langle g^q \rangle$ be the subgroup generated by g^q. H has order k.

Uniqueness

Let $H \subset G$ be a subgroup of order k. We want to show that H is unique. Let τ be a generator for H, so $\mathrm{ord}(\tau) = k$. Let σ be a generator for G, so $\mathrm{ord}(\sigma) = n$. Since H is a subgroup of G, $\tau = \sigma^j$ for some integer j. That is, $\mathrm{ord}(\sigma^j) = \frac{n}{\gcd(n,j)} = k$. We can rewrite this as $m = \gcd(n, j) = \frac{n}{k}$. Since $\gcd(n, j) = m$, j must take the form $j = ms$ for some integer s. Then,

$$\tau^k = \left(\sigma^j\right)^k = (\sigma^{ms})^k = \sigma^{msk} = \sigma^n s = (\sigma^n)^s = (e)^s\, \tau^k = e$$

So, $\langle \tau \rangle = \langle \sigma^{ms} \rangle$ is of order k. We want to show that $\langle \sigma^m \rangle = \langle \sigma^{ms} \rangle$. We notice that since $\gcd(k, s) = 1$, powers of σ^{ms} generates $\langle \sigma^m \rangle$ and vice versa; i.e. $\langle \sigma^m \rangle = \langle \sigma^{ms} \rangle$. $\square$

Question 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}).)

Response

Proof. Let G be a finite group of even order n. Consider the set of pairs

$$X := \{(a, a^{-1}) : a \in G\}$$

Since the identity element is unique, it is its own inverse, so $(e, e) \in X$. Then, we are left with $n - 1$ elements. Since n was even, there are an odd number of elements left. If we pair each nonidentity element with its distinct inverse, there would be one element left over. Call this element $a \in G$. Then, it must be true that a is its own inverse; i.e. $a = a^{-1}$. Then, a has order 2 since $a^2 = e$. $\square$

Question 10

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

Response

We have that $GL_n(\mathbb{Z}/p\mathbb{Z})$ represents all invertible $n \times n$ matricies in the field $\mathbb{Z}/p\mathbb{Z}$. Then, the order of the group is exactly the number of invertible matricies in $\mathbb{Z}/p\mathbb{Z}$. The first column of the vector is any non-zero vector, which is $p^n - 1$ choices. The second column is linearly independent from the first column, so there are $p^n - p$ choices. The third column must be linearly independent of the first two, giving us $p^n - p^2$ choices. We continue this, with the i^{th} choice being $p^n - p^{i-1}$ for $i = 1, 2, \dots, n$. To get, the total number of invertible matrices, we do

$$|GL_n(\mathbb{Z}/p\mathbb{Z})| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$$

giving us the order of the group.