

# Homework 3

Warren Kim

October 24, 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  $(a^{-1})^n = (a^n)^{-1}$  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

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

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

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

Then,

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

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

## 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

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

□

### 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,

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

So,  $G$  is commutative; that is,  $G$  is abelian. □

## Question 4

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

## Response

Note that there are solutions if  $3 \mid \varphi(18)$ .

$$\varphi(18) = 6$$

Since  $3 \mid 6$ , there are solutions. Then, there are 16 cases:

$$\begin{aligned} 2^3 &= 8 \equiv 8 \pmod{18} \not\equiv 1 \pmod{18} \\ 3^3 &= 9 \equiv 9 \pmod{18} \not\equiv 1 \pmod{18} \\ 4^3 &= 64 \equiv 10 \pmod{18} \not\equiv 1 \pmod{18} \\ 5^3 &= 125 \equiv 17 \pmod{18} \not\equiv 1 \pmod{18} \\ 6^3 &= 196 \equiv 16 \pmod{18} \not\equiv 1 \pmod{18} \\ 7^3 &= 343 \equiv 1 \pmod{18} \equiv 1 \pmod{18} \\ 8^3 &= 512 \equiv 8 \pmod{18} \not\equiv 1 \pmod{18} \\ 9^3 &= 729 \equiv 9 \pmod{18} \not\equiv 1 \pmod{18} \\ 10^3 &= 1000 \equiv 10 \pmod{18} \not\equiv 1 \pmod{18} \\ 11^3 &= 1331 \equiv 11 \pmod{18} \not\equiv 1 \pmod{18} \\ 12^3 &= 1728 \equiv 12 \pmod{18} \not\equiv 1 \pmod{18} \\ 13^3 &= 2197 \equiv 7 \pmod{18} \not\equiv 1 \pmod{18} \\ 14^3 &= 2744 \equiv 14 \pmod{18} \not\equiv 1 \pmod{18} \\ 15^3 &= 3375 \equiv 9 \pmod{18} \not\equiv 1 \pmod{18} \\ 16^3 &= 4096 \equiv 16 \pmod{18} \not\equiv 1 \pmod{18} \\ 17^3 &= 4913 \equiv 5 \pmod{18} \not\equiv 1 \pmod{18} \end{aligned}$$

So a potential solution is 7. To verify, we check  $7^1$  and  $7^2$ .

$$7^1 = 7 \equiv 7 \pmod{18} \not\equiv 1 \pmod{18}$$

$$7^2 = 49 \equiv 13 \pmod{18} \not\equiv 1 \pmod{18}$$

So the solution is 7.

## Question 5

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

### Response

#### Homomorphism

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

$$f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2)$$

for all  $x_1, x_2 \in G$  and

$$g(y_1 \cdot y_2) = g(y_1) \cdot g(y_2)$$

for all  $y_1, y_2 \in H$ .

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

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

#### Isomorphism \*\*\*\*\*INCOMPLETE\*\*\*\*\*

*Proof.* Let  $f : G \rightarrow H$ ,  $g : H \rightarrow K$  be two isomorphisms. Then,

$$f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2)$$

for all  $x_1, x_2 \in G$  and

$$g(y_1 \cdot y_2) = g(y_1) \cdot g(y_2)$$

for all  $y_1, y_2 \in H$ .

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

so the composition  $g \circ f$  is an isomorphism. □

## 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  $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$ .  
Let  $f : (\mathbb{Z}/9\mathbb{Z})^\times \rightarrow \mathbb{Z}/6\mathbb{Z}$  be the map:

□

## 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,  $\text{lcm}(n, m) = nm$ , so  $ab$  has order  $nm$ . □



### 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

## 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**