Homework 3

Warren Kim

October 23, 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

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

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,

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

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

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,

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

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

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:

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

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

$$7^1 = 7 \equiv 7 \ (mod\ 18) \not\equiv 1 \ (mod\ 18)$$

$$7^2 = 49 \equiv 13 \ (mod\ 18) \not\equiv 1 \ (mod\ 18)$$

So the solution is 7.

Question 5

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

Response

Proof. $\square$

Question 6

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

Response

Question 7

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

Response

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

Question 10

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

Response