Abstract Algebra Assignment (2): Groups

Mostafa Hassanein

11 November 2023

1.

The Cayley table for $(\overline{I_7^*}, *)$ is:

$*$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

i.

a.

$$\begin{aligned}(\overline{5})^3 &= [5]^3 \\ &= [5] * [5]^2 \\ &= [5] * [4] = [6]\end{aligned}$$

b.

$$\begin{aligned}(\overline{4})^{-4} &= [4]^{-4} \\ &= ([4]^{-1})^4 \\ &= [2]^4 \\ &= [2]^2 * [2]^2 \\ &= [4] * [4] = [2]\end{aligned}$$

c. By definition $x^0 = e$. So we have:

$$(\overline{2})^0 = [1]$$

ii.

In a group G, the order of an element x is the smallest positive integer m such that $x^m = e$, if no such m exists, then the order of x is infinite.

For the group $(\overline{I_7^*}, *)$, we have $e = [1]$. So we should solve for $x^m = [1]$ for all $x \in (\overline{I_7^*}, *)$. And since $|(\overline{I_7^*}, *)| = 6$, then if an m exists, it will be in the range $1 \leq m \leq 6$:

k	$[1]^k$	$[2]^k$	$[3]^k$	$[4]^k$	$[5]^k$	$[6]^k$
1	[1]	[2]	[3]	[4]	[5]	[6]
2	[1]	[4]	[2]	[2]	[4]	[1]
3	[1]	[1]	[6]	[1]	[6]	[6]
4	[1]	[2]	[4]	[4]	[2]	[1]
5	[1]	[4]	[5]	[2]	[3]	[6]
6	[1]	[1]	[1]	[1]	[1]	[1]

From the powers table, we deduce that:

$$
\begin{aligned}
ord([1]) &= 1 \\
ord([2]) &= 3 \\
ord([3]) &= 6 \\
ord([4]) &= 3 \\
ord([5]) &= 6 \\
ord([6]) &= 2
\end{aligned}
$$

2.

Let's construct the powers table for all $x \in (\overline{I_5^*}, *)$:

k	$[1]^k$	$[2]^k$	$[3]^k$	$[4]^k$
0	[1]	[1]	[1]	[1]
1	[1]	[2]	[3]	[4]
2	[1]	[4]	[4]	[1]
3	[1]	[3]	[2]	[4]

$(\overline{I_5^*}, *)$ is a cyclic group.
Because it contains elements, namely [2] and [3], that can generate all other elements in the group.

3.

Proof. We have to study the following properties: Closure, associativity, existence of an identity, existence of inverses.

i. Closure: Let $\overline{a}, \overline{b} \in \overline{I_p^*}$, then:

$$
\begin{aligned}
\overline{a} \otimes \overline{b} = \overline{ab} = ab & & \mod p \\
= (q_1 p + r_1)(q_2 p + r_2) & & \mod p \\
= q_1 q_2 p^2 + q_1 r_2 p + q_2 r_1 p + r_1 r_2 & & \mod p \\
= (q_1 q_2 p + q_1 r_2 + q2_r 1)p + r_1 r_2 & & \mod p \\
= r1r2 & & \mod p
\end{aligned}
$$

Where $r_1, r_2 > 0$, because $\overline{0} \notin \overline{I_p^*}$.
p is prime and $r_1, r_2 > 0 \Rightarrow r_1$ and r_2 do not divide $p \Rightarrow r1r2$ does not divide $p \Rightarrow 1 \leq (r1r2 \mod p) < p \Rightarrow a \otimes b \in \overline{I_p^*}$.

ii. Associativity: Let $\overline{a}, \overline{b}, \overline{c} \in \overline{I_p^*}$. We want to show that $\overline{a} \otimes (\overline{b} \otimes \overline{c}) = (\overline{a} \otimes \overline{b}) \otimes \overline{c}$:

$$
\begin{aligned}
L.H.S. : \overline{a} \otimes (\overline{b} \otimes \overline{c}) &= \overline{a} \otimes (\overline{bc}) \\
&= \overline{abc} \\
R.H.S. : (\overline{a} \otimes \overline{b}) \otimes \overline{c} &= \overline{ab} \otimes \overline{c} \\
&= \overline{abc}
\end{aligned}
$$

$L.H.S. = R.H.S.$

iii. Identity: $\exists e = \overline{1} \in \overline{I_p^*} \ni \forall a \in \overline{I_p^*} : e \otimes a = a \otimes e = a.$
iv. Inverse: p is prime $\Rightarrow \forall \overline{a} \in \overline{I_p^*} : gcd(a, p) = 1$
$\Rightarrow \forall \overline{a} \in \overline{I_p^*}\ \exists r, s \in Z : ar + ps = 1$
$\Rightarrow \forall \overline{a} \in \overline{I_p^*}\ \exists r, s \in Z : \overline{ar + ps} = \overline{1}$
$\Rightarrow \forall \overline{a} \in \overline{I_p^*}\ \exists r, s \in Z : \overline{ar} = \overline{1}$
$\Rightarrow \forall \overline{a} \in \overline{I_p^*}\ \exists r, s \in Z : \overline{a} \otimes \overline{r} = \overline{1}$
$\Rightarrow \forall \overline{a} \in \overline{I_p^*}\ \exists \overline{r} \in \overline{I_p^*} : \overline{a} \otimes \overline{r} = \overline{1}$

i, ii, iii, iv $\Rightarrow \overline{I_p^*}$ is a group.
And since I_p^* contains $p - 1$ elements, then $|\overline{I_p^*}| = p - 1$.

□

4.

Proof. The set of elements generated by $+1$ under $+$ is given by: $\{k(+1) = k : k \in I\} = I$. This shows that $+1$ is a generator for the additive group of integers.

Similarly, the set of elements generated by -1 under $+$ is given by: $\{k(-1) = -k : k \in I\} = I$. This shows that -1 is a generator for the additive group of integers. (Alternatively, we could have used the fact that if a is a generator then so is a^{-1}.)

This shows that I is a cyclic group with +1 and -1 as generators.

Since $|I| = \infty$, then I is an infinite cyclic group.

□

5.

Proof. The set of elements generated by $\overline{1}$ under $+$ are given by:

$$\begin{aligned} < \overline{1} > &= \{\overline{k\overline{1}} : \ k \in Z\} \\ &= \{\overline{k} : \ k \in Z\} \\ &= \{\overline{k} : \ 0 \leq k < n\} \\ &= \overline{I_n} \end{aligned}$$

□