LECTURE 9

13.02.2024

(2) Let G be a finite group of prime order. Then, G is a cyclic group.

Proof. Let $|G| = p$, a prime number. So, there are non-identity elements in G. Take any such element, g, say. Consider the cyclic subgroup $\langle g \rangle$ generated by g. Then, by Lagrange's theorem $|\langle g \rangle| \mid |G|$. So, $|\langle g \rangle| = 1$ or, p. Since $g \neq e_G$, $|\langle g \rangle| = p$. But, $\langle g \rangle \subseteq G$, and, hence, $\langle g \rangle = G$. Thus, G is a cyclic group.

Q. Any group with prime p as its order is cyclic. What about any group of order p^2? Not necessarily.

Consider the group of order 4:

$$\left(\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}, \right.$$

matrix multiplication), where all non-identity elements are of order 2.

Some more examples of cosets

Consider the group $(\mathbb{Z}, +)$. We know that the subgroups are of the form $(n\mathbb{Z}, +)$, where $n \in \mathbb{Z}$.

Q. What are the cosets of $(5\mathbb{Z}, +)$?

A. $\{0+5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$

H.W. Prove the answer above, that is, show that the above collection of sets partitions $\mathbb{Z}$.

Q. What are the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$, $n \geq 1$?

The collection of cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ is:

$\{a + n\mathbb{Z} : 0 \leq a \leq n-1\}$. [We can always assume that $n \geq 1$].

Another way of writing this set is as follows: $\{[0], [1], \ldots, [n-1]\}$.

We denote this set as $\underline{\mathbb{Z}_n}$ or $\underline{\mathbb{Z}/n\mathbb{Z}}$

Q. <u>Does $\mathbb{Z}_n$ form a group under some operation?</u>

Consider $[a], [b] \in \mathbb{Z}_n$.

Define $\underbrace{[a]}_{\text{set of integers}} +_n \underbrace{[b]}_{\text{set of integers}} = \underbrace{[a+b]}_{\text{set of integers}}$

Let us consider $n = 5$. Then, we have:

$[3] +_5 [4] = [7] = [2]$ (Why?)

To answer this query we should consider the equivalence relation underlying these classes, which would give us different representative members of the same class.

Now, what is the equivalence relation $\sim$ here for which $2 \sim 7$?

Let $a, b \in \mathbb{Z}$. We define $a \sim_n b$ iff $[a] = [b]$ in $\mathbb{Z}_n$ iff $n \mid a-b$.

Above, we have defined the operation $+_n$ between such equivalence classes.

In these cases, we need to check well-definedness of such operations.

We have defined $[a] +_n [b] = [a+b]$.

Now, if $a \sim a'$ and $b \sim b'$, then we should have $a+b \sim a'+b'$.

Proof: Suppose $a \sim a'$ and $b \sim b'$

Then, $n \mid a-a'$ and $n \mid b-b'$

So, $n \mid (a-a') + (b-b')$

or, $n \mid (a+b) - (a'+b')$

Hence, $a+b \sim a'+b'$. Thus,

- $+_n$ is well-defined on $\mathbb{Z}_n$.

- Is $+_n$ associative?

$$([a] +_n [b]) +_n [c]$$
$$= [a+b] +_n [c]$$
$$= [(a+b) + c]$$
$$= [a + (b+c)]$$
$$= [a] +_n [b+c]$$
$$= [a] +_n ([b] +_n [c]).$$

- $[0]$ is the identity element.

$$[a] +_n [0] = [a+0] = [a]$$
$$[0] +_n [a] = [0+a] = [a].$$

- Inverse of $[a]$ is $[n-a]$

$$[a] +_n [n-a] = [a+(n-a)] = [n] = [0]$$
$$[n-a] +_n [a] = [(n-a)+a] = [n] = [0].$$

So, $\mathbb{Z}_n$ forms a group under $+_n$.

Another operation on $\mathbb{Z}_n$

Define $\times_n$ on $\mathbb{Z}_n$ as follows:

$$[a] \times_n [b] = [a \cdot b]$$

H.W. Does $\mathbb{Z}_n$ form a group under this operation? If not, can you find a non-trivial subset of $\mathbb{Z}_n$ which will form a group under $\times_n$?

Let G be a group and f be a homomorphism with domain G. Consider $\operatorname{Ker} f$.

Q. Does the cosets of $\operatorname{Ker} f$ in the group G form a group under certain operation?

Let $H = \operatorname{Ker} f$, a subgroup of G.

Consider $\mathcal{K} = \{aH : a \in G\}$, the set of all cosets of H in G.

Define $aH * bH = abH$

- $*$ is well-defined.

Take $a_1, a_2, b_1, b_2 \in G$.

Let $a_1, a_2 \in aH$, that is $a_1 \sim a_2$.

and $b_1, b_2 \in bH$, that is $b_1 \sim b_2$.

We need to show that:

$a_1 b_1 \sim a_2 b_2$, that is: $a_1 b_1, a_2 b_2 \in abH$

Now, $a_1 = ah_1$ $\quad a_2 = ah_2$

$b_1 = bh_3$ $\quad b_2 = bh_4$,

$h_1, h_2, h_3, h_4 \in H$.

We have:

$$
\begin{aligned}
& f(a_1 b_1) \\
&= f(ah_1 bh_3) \\
&= f(a) f(h_1) f(b) f(h_3) \\
&= f(a) f(b) \\
&= f(a) f(h_2) f(b) f(h_4) \\
&= f(ah_2 \cdot bh_4) \\
&= f(a_2 b_2).
\end{aligned}
$$

So, $a_1 b_1 \sim a_2 b_2$, that is :

$$a_1 b_1 H = a_2 b_2 H$$

[Here : $a \sim b$ iff $f(a) = f(b)$]

- $*$ is associative :

$$(aH * bH) * cH$$

$$= (ab)H * cH$$

$$= (ab)c\, H$$

$$= a(bc)\, H$$

$$= aH * (bc)H$$

$$= aH * (bH * cH).$$

[It follows from associativity of the group operation $\circ$, say, in G]

- H is the identity element.

- Inverse of aH is $a^{-1}H$.

Thus $(K, *)$ forms a group.

We denote this group by $G/\ker f$.

We have now seen that cosets in $\mathbb{Z}$ forms a group. Also, if we consider the subgroup to be $\ker f$ for some homomorphism f, cosets of $\ker f$ also form a group.

Q. Take any group G and take any subgroup H of G. Would the cosets of H in G always form a group under the operation we considered earlier? If not, what condition should we impose on subgroups to make this operation on cosets work?

Claim: For this operation on cosets to work, we have to consider normal subgroups.

A proof of the claim:

Let G be a group and H be a subgroup of G which is not a normal subgroup. Then, there is a $g \in G$ and there is an $h \in H$, s.t. $ghg^{-1} \notin H$. Now, we consider the cosets of H in G and consider the operation:

$aH * bH = abH$ for all $a, b \in G$.

If we take $b = a^{-1}$, we have:

$$aH * a^{-1}H = aa^{-1}H = e_G H = H.$$

Then, for any $h_1, h_2 \in H$, there $h_3 \in H$, s.t. $ah_1a^{-1}h_2 = h_3 \in H$.

Now, take $a = g$; $h_1 = h$; $h_2 = e_G$. Then:

$ghg^{-1} \in H$, a contradiction.

So, H has to be a normal subgroup.

This completes the proof. $\square$

Quotient Group :

Let G be a group and H be a normal subgroup of G. The group formed by the cosets of H in G, denoted by G/H, is called a quotient group of H in G. The group operation is given by :

$aH * bH = abH$ for all $a, b \in G$.

Examples :

① $\left(\mathbb{Z}/n\mathbb{Z}, +_n\right)$: $(a + n\mathbb{Z}) +_n (b + n\mathbb{Z})$

$= (a+b) + n\mathbb{Z}$.

② $\left(G/\operatorname{Ker} f, *\right)$: $(a \cdot \operatorname{Ker} f) * (b \cdot \operatorname{Ker} f)$

$= (a \cdot b) \cdot \operatorname{Ker} f$