Notes lectured by Dr. A.K. Yadav.
Deptt. of Mathematics Mansari College, DBG
B.Sc-part-I(H), paper—I Date -02—05-2020
Algebra

Q.1. Every subgroup of a cyclic group is also a cyclic group.

Proof: Let G be a cyclic group under the composition 'o' and H is a subgroup of G.

We have to prove that H is a cyclic group under the composition 'o'.

As (G, o) is a cyclic group, there exists an element $a \in G$ whose integral powers exhaust the set G, i.e. if $b \in G$ then there exists an integer m such that $b = a^m$.

As $H \subseteq G$, being a subgroup, we get every element of H can also be expressed as an integral power of a. Let K be the least positive integer such that $a^k \in H$. Let a^m be any other element of H. Then $m > K$.

Let $m = pK + r$ where $0 \le r < K$.

$\therefore a^m = a^{pK+r} = a^{pK} o a^r = (a^K)^p o a^r$

$\Rightarrow \{(a^K)^p\}^{-1} o a^m = \{(a^K)^p\}^{-1} o (a^K)^p o a^r$

$\Rightarrow (a^K)^{-p} o a^m = a^r \quad [\because b^{-1} o b = e]$

Now, $a^K \in H \Rightarrow (a^K)^p \in H \Rightarrow (a^K)^{-p} \in H$.

[As H is itself a group and inverse element exists in a group]

$\therefore$ By closure law, $(a^K)^{-p} o a^m \in H$.

$\therefore a^r \in H$ where $0 \le r < K$. This contradicts the fact that K is the least positive integer such that $a^K \in H$.

The contradiction does not arise only if $r = 0$

Then $m = pK$ and $a^m = (a^K)^p$.

Hence, H is also cyclic with a^m as a generator.

Thus, every subgroup of a cyclic group is also cyclic.

Proved

B.Sc. (Hons) Part-I (H), Paper-I, Date – 02-05-2020

Q.2. To prove that if H be a subgroup of the group G and $a, b \in G$, then either $aH \cap bH = \phi$ or $aH = bH$.

Proof: We know that the two left coset aH and bH are subset of G.

$\therefore$ either $aH \cap bH = \phi \Rightarrow aH \cap bH \neq \phi$

If we can prove that $aH \cap bH \neq \phi$ implies $aH = bH$ then our proposition will be established.

Let $x \in aH \cap bH$

$\Rightarrow x \in aH$ and $x \in bH \Rightarrow x = ah_1$ and $x = bh_2$ for some $h_1, h_2 \in H$.

$\Rightarrow ah_1 = bh_2 \Rightarrow b^{-1}(ah_1)h_1^{-1} = b^{-1}(bh_2)h_1^{-1}$

[operating b^{-1} from the left and h_1^{-1} from the right]

$\Rightarrow (b^{-1}a)(h_1 h_1^{-1}) = (b^{-1}b)(h_2 h_1^{-1})$ [by associative law]

$\Rightarrow (b^{-1}a)e = e(h_2 h_1^{-1}) \Rightarrow b^{-1}a = h_2 h_1^{-1} \in H$.

Similarly, $x \in aH \cap bH \Rightarrow a^{-1}b \in H$

Now, let $y \in aH$.

$\Rightarrow y = ah_3$, for some $h_3 \in H$

$\Rightarrow y = (bb^{-1})ah_3$, for $bb^{-1} = e$

$\Rightarrow y = b(b^{-1}a)h_3$

$\Rightarrow y = bh_4$, where $h_4 \in H$.

[for $b^{-1}a \in H$, $h_3 \in H \Rightarrow (b^{-1}a)h_3 \in H$]

$\therefore y \in bH$ $\therefore aH \subseteq bH$.

Similarly, if $z \in bH$, we can prove $z = a(a^{-1}b)h_5$, where $a^{-1}b, h_5 \in H$.

So, $z = ah_6$ where $h_6 = (a^{-1}b)h_5 \in H$

$\therefore z \in aH$. Thus $bH \subseteq aH$

$\therefore aH = bH$. Proved

[When $H = \{h_1, h_2, h_3 \cdots h_n, \cdots\}$. Then the set $\{ah_1, ah_2, ah_3 \cdots ah_n\}$ where $a \in G$, is called a left coset of the subgroup H in G generated by a. It is denoted by aH. Also the set $\{h_1a, h_2a, h_3a, \cdots h_na\}$ is called a right coset of the subgroup H in G generated by a. It is denoted by aH. In the above discuss let H be a subgroup of the group G where $H = \{h_1, h_2, h_3 \cdots h_n, \cdots\}$.]