Tutorial 2

27/01/2022

Q4.

WTS $\sigma(a_1 a_2 \cdots a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2) \cdots \sigma(a_k))$

where $\sigma \in S_n$.

$\sigma(a_1 \cdots a_k)\sigma^{-1}(\sigma(a_1))$

$= \sigma(a_1 \cdots a_k)\,\sigma^{-1}\sigma(a_1)$

$= \sigma(a_1 \cdots a_k)(a_1)$

$= \sigma(a_2$

Q6. Any cyclic gp will be isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n = 0, 1, 2, \cdots$

If G is infinite $\cong \mathbb{Z}$.

$|G| = m$ is cyclic gp $\cong \mathbb{Z}/m\mathbb{Z}$.

Q7. $\mathbb{Z} \longrightarrow \mathbb{Z}$.

$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

$\mu_1(1) = 1. \Rightarrow \mu_1(x) = x.$

$\mu(1) + \cdots \mu(1)$ (x-times).

$\mu_2(1) = -1.$

$\mu_2(x) = -x.$

$Aut(\mathbb{Z}) = \{ f : \mathbb{Z} \to \mathbb{Z} \mid f \text{ is an gp isomorphism} \}$

$|Aut(\mathbb{Z})| = 2.$

$Aut(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}.$

$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \bar{5}\} = \langle \bar{1} \rangle$

$= \langle \bar{5} \rangle$

$\mathbb{Z}/6\mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z}$.

$\phi_1 : \bar{1} \longmapsto \bar{1}$

$\phi_2 : \bar{1} \longmapsto \bar{5}$

$|\mathrm{Aut}(\mathbb{Z}/6\mathbb{Z})| = 2$.

$\mathrm{Aut}(\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

$\mathbb{Z}/n\mathbb{Z} = \langle \bar{a} \rangle$ where $\gcd(a,n) = 1$

$|\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})| = \phi(n)$ ~> Euler's ϕ fn. which counts the no. of elts $< n$ which are co-prime to n.

$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$

$= \{\bar{a} \mid \gcd(a,n) = 1\}$ forms a gp wrt multiplication.

$\gcd(a,n) = 1$.

$ax + ny = 1 \quad \exists\, x, y \in \mathbb{Z}$.

$\hookrightarrow \bar{a}\bar{x} = \bar{1} \qquad \mathbb{Z}/n\mathbb{Z}$

$$S_3 = \{ (1),\ (123),\ (132),\ (12),\ (13),\ (23) \}$$
$$= \{ 1,\ a,\ a^2,\ b,\ ab,\ a^2b \}$$
$$= \langle a, b \mid a^3 = 1,\ b^2 = 1,\ ba = a^2b \rangle.$$

$S_3 \longrightarrow S_3$

$a \mapsto a$ or a^2

$b \mapsto b$ or ab or a^2b.

$|\mathrm{Aut}(S_3)| = 6$.

φ_1: $a \mapsto a$, $b \mapsto b$; φ_2: $a \mapsto a^2$, $b \mapsto b$

φ_3: $a \mapsto a$, $b \mapsto ab$; φ_4: $a \mapsto a$, $b \mapsto a^2b$

φ_5: $a \mapsto a^2$, $b \mapsto ab$; φ_6: $a \mapsto a^2$, $b \mapsto a^2b$.

Observe $|\Phi_2| = 2$. & $|\Phi_3| = 3$.

check. $\mathrm{Aut}(S_3) \cong S_3$.

Q11. $GL_3(\mathbb{F}_2) = \langle A, B \mid |A| = 4,\ |B| = 2$ & $AB = BA^3 \rangle$.

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad |A| = 4.$$

$D_4 = \langle a, b \mid |a| = 4,\ |b| = 2$
$ab = ba^3 \rangle$.

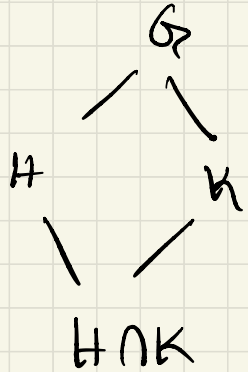
$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad |B| = 2.$$

check $AB = BA^3$.

$A \longmapsto a$

$B \longmapsto b$.

Q15.



$$l = [G : H\cap K] = [G:H][H:H\cap K]$$

$$= m\,[H : \underbrace{H\cap K}_{\parallel p_1}]$$

$$l = [G : H\cap K] = [G:K][K:H\cap K]$$

$$= n\,[K : \underbrace{H\cap K}_{\parallel p_2}]$$

$$l = m p_1$$

$$= n p_2$$

Since $m \mid l$ & $n \mid l \Rightarrow l.c.m \mid l$.

$$\therefore \quad l.c.m\,(n,n) \le [G : H\cap K].$$

WTJ $[G : H\cap K] \le [G:H]\cdot[G:K]$.

WTS. $[H : H\cap K] \le [G:K]$.

$[H : H \cap K]$ = no. of left cosets of $H \cap K$ in H.

$$H/H\cap K \longrightarrow G/K$$

$$\varphi : h(H\cap K) \longmapsto hK.$$

Let $\varphi(h_1(H\cap K)) = \varphi(h_2(H\cap K))$

WTS $h_1(H\cap K) = h_2(H\cap K)$.

$\Rightarrow h_1 K = h_2 K$.

$\Rightarrow h_2^{-1} h_1 \in K$.

But $h_2^{-1} h_1 \in H$.

$\therefore h_2^{-1} h_1 \in H \cap K$.

$\Rightarrow h_1(H\cap K) = h_2(H\cap K)$.

$\therefore [H : H\cap K] \leq [G : K]$.

Q19

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} = \left\{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1 \right\}.$$

$$\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}\right| = \phi(n)$$

If p is a prime no.

$$G_2 = \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times} = \left\{ \bar{1}, \bar{2}, \cdots, \overline{p-1} \right\}.$$

$$|G_2| = p-1.$$

Let $a \in \mathbb{Z}$, $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$

$$\bar{a}^{p-1} = 1.$$

$$\Rightarrow \bar{a}^{p} = \bar{a}.$$

$$\Rightarrow a^p \equiv a \pmod{p}.$$

Q20

$G = \left(\mathbb{Z}/(p^n-1)\mathbb{Z}\right)^{\times}$ $\quad \mathbb{Z}/(p^n-1)\mathbb{Z}$

$p^n - 1 \equiv 0$ in $\mathbb{Z}/(p^n-1)\mathbb{Z}$.

$\Rightarrow \bar{p}^n \equiv \bar{1}$ in G.

$\Rightarrow |\bar{p}| \mid n$.

If $1 \le k < n$ s.t $\bar{p}^k = \bar{1}$

$p^k < p^n - 1$. and $\bar{p}^k = \bar{1}$

which is not possible in $\mathbb{Z}/(p^n-1)\mathbb{Z}$.

$\therefore |\bar{p}| = n$.

$|G| = \phi(p^n-1)$.

$\therefore |\bar{p}| = n \mid |G| = \phi(p^n-1)$

i.e $n \mid \phi(p^n-1)$.