Lec 9/21

Friday, September 21, 2018 11:33

Presentations: Nov 26 – 30 (Soft deadline friday Sept 28, hard deadline Nov 2).

<u>MT1</u>: Median 49

(yesterday: $\mathrm{Aut}_{gp}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$)

$\mathrm{Aut}_{gp}(W)$ same group.

$\mathrm{Aut}_{gr}(\mathbb{Z}/12\mathbb{Z}) = ?$

$1 \longmapsto$ any of the $\phi(12) = 4$ elements $1, 5, 7, 11$.

So $\mathrm{Aut}_{gp}(\mathbb{Z}/12\mathbb{Z}) = \mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$.

$1 \longmapsto 1$ id.

$1 \longmapsto 5 \longmapsto \underset{\text{}}{25} = 1$ aut. of order 2

$1 \longmapsto 7 \longmapsto 49 = 1$

$1 \longmapsto 11 = -1 \longmapsto 1$

<u>Lemma</u>: If $G = \langle \sigma \rangle$ is a cyclic group, $\mathrm{Aut}_{gp}(G) \ni \varphi$ is abelian.

φ_k has the form $\sigma \longmapsto \sigma^k$ another generator

$\varphi_k \cdot \varphi_\ell = \varphi_{k\ell} = \varphi_\ell \cdot \varphi_k$

<u>Ex</u>: $\mathrm{Aut}(\mathbb{Z}^2) \cong SL_2(\mathbb{Z})$. not abelian.

not cyclic.

<u>Recall</u>: G abelian, $|G| = n = p_1^{a_1} \cdots p_\ell^{a_\ell}$.

(1) $G = P_1 \times P_2 \times \cdots \times P_\ell$; $|P_i| = p_i^{a_i}$ ← sylow p-subgroups

(2) $P_j \cong \mathbb{Z}/p_j^{a_{j1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_j^{a_{jn_j}}\mathbb{Z}$ s.t. $\sum_{i=1}^{n_j} a_{ji} = a_j$,

$a_{j1} \geq a_{j2} \geq \cdots \geq a_{jn_j}$.

$$\boxed{\begin{matrix} a_{11} \geq a_{12} \geq \cdots \geq a_{1r} \\ a_{21} \geq a_{22} \geq \cdots \geq a_{2r} \\ \vdots \\ a_{\ell 1} \geq a_{\ell 2} \geq \cdots \geq a_{\ell r} \end{matrix}} \begin{matrix} \geq 0 \\ \geq 0 \\ \\ \geq 0 \end{matrix}$$

→ these #s tell you everything about your group.

eg $|G| = 18 = 2^1 \cdot 3^2$ ↑ abelian

$p_1 = 2$ $a_1 = 1$

$p_2 = 3$ $a_2 = 2$

2 groups:

$$\begin{array}{c|cc} & \geq & \\ \hline (1) & 1 & 0 \\ (2) & 2 & 0 \end{array} \qquad\qquad \begin{array}{c|cc} & \geq & \\ \hline (1) & 1 & 0 \\ (2) & 1 & 1 \end{array}$$

$$\underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}}_{\cong\ \mathbb{Z}/18\mathbb{Z}} \qquad\qquad \underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}} \times \mathbb{Z}/3\mathbb{Z} .$$

$$\mathbb{Z}/18\mathbb{Z} \qquad\qquad \cong \quad \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} .$$

result we're using:

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \cong \mathbb{Z}/m_1m_2\mathbb{Z}$$

iff $(m_1, m_2) = 1$.

$$(x \bmod m_1, x \bmod m_2) \xleftarrow{f} x \bmod m_1 m_2$$

ex: f is injective gp hom.
$\operatorname{Ker} f = \{e\}$ since $(m_1, m_2) = 1$ and $x \in \operatorname{Ker} f$ is $0 \bmod m_1, m_2$
So it's $0 \bmod m_1 m_2$.

$$\mathbb{Z}/q_1\cdots q_t\mathbb{Z} \cong \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_t\mathbb{Z}$$

So using table. define

$$n_1 = p_1^{a_{11}} p_2^{a_{21}} \cdots p_\ell^{a_{\ell 1}}$$
$$n_2 = p_1^{a_{12}} p_2^{a_{22}} \cdots p_\ell^{a_{\ell 2}}$$
$$\vdots$$
$$n_r = p_1^{a_{1r}} p_2^{a_{2r}} \cdots p_\ell^{a_{\ell r}}$$

So $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$.

$n_r \mid n_{r-1}$, $n_{r-1} \mid n_{r-2}$, $\ldots$, $n_2 \mid n_1$

and $n_1 \cdot n_2 \cdot \cdots \cdot n_r = n$.

Theorem
if G is abelian and $|G| = n$.

Corollary: Exponent of a group $G = \max\{\text{ord}(x) : x \in G\}$

→ and this is n_1 in the above theorem.

→ also, if $m = \exp(G)$ then $\tau^m = e$ for all $\tau \in G$.

Remark: we can prove this directly (without using Sylow / remainder thms).

Pf pick $\sigma \in G$ of order m. take $\tau \in G$ & we'll prove $\tau^m = e$.

if $\tau \in \langle \sigma \rangle$ then we have nothing to prove.

Pick smallest $k \neq 0$ s.t. $\tau^k \in \langle \sigma \rangle$ $(2 \leq k \leq \text{order}(\tau) \leq m)$.

$\tau^k = \sigma^j$. $j = kq + r$ with $(0 \leq r \leq k-1)$

$$(\underbrace{\tau \sigma^{-q}}_{\tau'})^k = \sigma^r$$

Ex: $\Rightarrow \text{order}(\tau') = k \cdot \gcd(r, m) > m$ if $r \neq 0$.

Ex: use this argument to prove the theorem directly!