Lecture 20

(20.0) Recall that we introduced the notion of a semidirect product and proved that $\boxed{\begin{array}{l}(H, N, \alpha) \rightsquigarrow N \rtimes_{\alpha} H \\ \alpha : H \longrightarrow \mathrm{Aut}_{gp.}(N)\end{array}}$ method produces all semidirect products of H & N.

[Careful: different $\alpha : H \to \mathrm{Aut}_{gp}(N)$ can give rise to isomorphic groups.]

Later we focused on $\mathrm{Aut}_{gp.}(W) = \{\varphi : W \to W \text{ group iso.}\}$

(20.1) $W = \mathbb{Z}/p\mathbb{Z}$ example. For some small primes:

$$\mathrm{Aut}_{gp.}\left(\mathbb{Z}/p\mathbb{Z}\right) = \left\{\sigma_x : x \in \mathbb{Z}/p\mathbb{Z} ; x \neq 0\right\} \text{ where}$$

$$\sigma_x : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

$$1 \longmapsto x$$

Clear from the definition $\sigma_x \sigma_y = \sigma_{xy}$. So we obtain: $\mathrm{Aut}_{gp}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p^{\times}$ ← (multiplicative) group of non-zero elements.

(20.2) Revisiting finite abelian groups. (see Lecture 15 pages 3 & 4.)

Assume $|G| = n = p_1^{a_1} \cdots p_\ell^{a_\ell}$ is a finite abelian group.

Then

(i) $G \cong P_1 \times P_2 \times \cdots \times P_\ell$

where $|P_j| = p_j^{a_j}$ $(1 \le j \le \ell)$.

(Note: We used Sylow Thms to prove this see (15.2) on page 3 of Lecture 15.)

(ii) Each P_j has the following form:

$$P_j \cong \mathbb{Z}/p_j^{a_{j,1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_j^{a_{j,m_j}}\mathbb{Z}$$

$a_{j,1} \ge a_{j,2} \ge \cdots \ge a_{j,m_j} > 0$; they add up to $a_j < n$

This data can be organized as follows: (I have allowed 0 as an entry to make it rectangular; i.e. – $r = \max\{m_j : 1 \le j \le \ell\}$)

Sum total		
$a_1 \leftarrow$	$a_{11} \ge a_{12} \ge a_{13} \ge \cdots \ge a_{1r} \ge 0$	
$a_2 \leftarrow$	$a_{21} \ge a_{22} \ge a_{23} \ge \cdots \ge a_{2r} \ge 0$	
$\vdots$	$\vdots$	
$a_\ell \leftarrow$	$a_{\ell 1} \ge a_{\ell 2} \ge a_{\ell 3} \ge \cdots \ge a_{\ell r} \ge 0$	
$n = p_1^{a_1} \cdots p_\ell^{a_\ell}$	" $b_1 = a_{11} + \cdots + a_{\ell 1}$ " similar	Define $n_1 = p_1^{a_{11}} p_2^{a_{21}} \cdots p_\ell^{a_{\ell 1}}$

– (Fig. 1)

(20.3) Example - if $G \cong \left(\mathbb{Z}/_{2^3\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}\right) \times \left(\mathbb{Z}/_{5^2\mathbb{Z}}\right)$

(so $|G| = 16(25) = 400$)

$p_1 = 2$, $p_2 = 5$; ℓ = # primes = 2

$a_1 = 4$, $a_2 = 2$

$4 = 3+1$, $2 = 2+0$

organized as

3	1
2	0

$n_1 = 2^3 \cdot 5^2 = 200$, $n_2 = 2^1 \cdot 5^0 = 2$ (rearrangement of factors of G)

$$G \cong \left(\underbrace{\mathbb{Z}/_{2^3\mathbb{Z}} \times \mathbb{Z}/_{5^2\mathbb{Z}}}_{\text{112 Ex. - see below}}\right) \times \left(\mathbb{Z}/_{2\mathbb{Z}}\right)$$

$$\mathbb{Z}/_{200\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$$

(20.4) Sun Tzu's theorem - easier version.
("Chinese Remainder Thm")

$$\mathbb{Z}/_{p_1^{b_1} p_2^{b_2} \cdots p_t^{b_t}\mathbb{Z}} \cong \mathbb{Z}/_{p_1^{b_1}\mathbb{Z}} \times \mathbb{Z}/_{p_2^{b_2}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_t^{b_t}\mathbb{Z}}$$

m , q_1 , q_2 , $\cdots$, q_t

Define $f : \mathbb{Z}/_{m\mathbb{Z}} \longrightarrow \mathbb{Z}/_{q_1\mathbb{Z}} \times \mathbb{Z}/_{q_2\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{q_t\mathbb{Z}}$

f sends $x \pmod m$ to the tuple $(x \bmod q_1 ; x \bmod q_2 ; \dots ; x \bmod q_t)$.

This is clearly a group hom. Moreover,

$$\mathrm{Ker}(f) = \{ x \pmod m \text{ s.t. } \underbrace{q_j \text{ divides } x \ \forall j = 1, \dots, t}_{\Downarrow \ m \text{ divides } x} \}$$

$$= \{0\}$$

So f is injective. Since $\mathbb{Z}/m\mathbb{Z}$ & $\mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_t\mathbb{Z}$ have same size, we conclude that f is an iso. □

(20.5) Rearrangement of pieces : back from (20.2) –

G : abelian group $\quad |G| = n = p_1^{a_1} \cdots p_\ell^{a_\ell}$

see Fig-1 from page 2..

$$G \cong \underbrace{\left(\mathbb{Z}/p_1^{a_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{a_{12}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{a_{1r}}\mathbb{Z}\right)}_{\cong} \times \underbrace{\left(\mathbb{Z}/p_2^{a_{21}}\mathbb{Z} \times \mathbb{Z}/p_2^{a_{22}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_2^{a_{2r}}\mathbb{Z}\right)}_{\cong} \times \cdots \times \underbrace{\left(\mathbb{Z}/p_\ell^{a_{\ell 1}}\mathbb{Z} \times \mathbb{Z}/p_\ell^{a_{\ell 2}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{a_{\ell r}}\mathbb{Z}\right)}_{\cong}$$

$$\Rightarrow G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

where $n_1 = p_1^{a_{11}} p_2^{a_{21}} \cdots p_\ell^{a_{\ell 1}}$

$n_2 = p_1^{a_{12}} p_2^{a_{22}} \cdots p_\ell^{a_{\ell 2}}$ and so on. Note

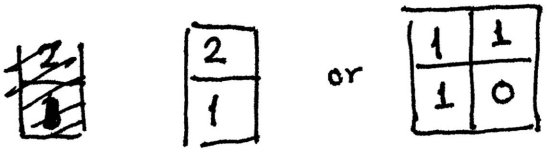
that the inequalities $a_{11} \geq a_{12} \geq a_{13} \geq \cdots$ imply that

$a_{21} \geq a_{22} \geq a_{23} \geq \cdots$

n_r divides n_{r-1} divides n_{r-2} $\cdots$ n_2 divides n_1.

e.g. List of all abelian groups of order (size) $12 = 2^2 \cdot 3^1$

Fig. 1 style labelling



Corresponding groups

$\underbrace{\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}}_{12}$ or $\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \times \mathbb{Z}/3\mathbb{Z}$

$\mathbb{Z}/12\mathbb{Z}$ $\qquad$ 12

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

# of ways of writing 12 ($= |G|$ in this example)

as a product $n_1 \cdot n_2 \cdot n_3 \cdots$ such that n_{i+1} divides n_i

$= 2$; namely $12 = 12 \cdot 1 \rightsquigarrow \mathbb{Z}/12\mathbb{Z}$

$= 6 \cdot 2 \rightsquigarrow \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Thus we have proved the following alternate characterization of finite abelian groups.

(20.6) Theorem. - $|G| = n$; G : abelian group.

Then $$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

where $\begin{cases} n_{i+1} \text{ divides } n_i & (i = 1, 2, \ldots, r-1) \text{ and} \\ n_1 \cdot n_2 \cdot \ldots \cdot n_r = n \end{cases}$

The number n_1 can be obtained from G as:

$$n_1 = \max \{ s \text{ such that } s = \text{order}(\sigma) \text{ for some } \sigma \in G \}$$

called <u>exponent of G</u>. (it divides n because $\text{order}(\sigma) \mid n$ $\forall\, \sigma \in G$.)

As a consequence of this theorem, we get

(20.7) Corollary. - Let G be a finite abelian group and

m = exponent of G.

Then $\tau^m = e$ for every $\tau \in G$.

Below, we will see a direct proof of this result. It is essentially the same argument as on page 8 of Lecture 15.

<u>Exercise:</u> Use the proof given below to prove Theorem above directly (i.e., no need for Sylow Thm-s or Remainder Thm.)

Proof. Choose $\sigma \in G$ such that $\text{order}(\sigma) = m$.

Let $\tau \in G$ be an arbitrary element of G.

By defn. of m, $\text{order}(\tau) \leq m$. Let us assume $\tau \notin \langle\sigma\rangle$, because if it is of the form σ^j then clearly $\tau^m = e$ which is what we want to show.

Let k = smallest such that $\tau^k \in \langle\sigma\rangle$.
$(2 \leq k \leq \text{order}(\tau))$

So $\tau^k = \sigma^j$ for some $j \in \{0, \ldots, m-1\}$

Write $j = qk + r$ $\left(q \geq 0 \text{ and } 0 \leq \underset{\uparrow}{r} \leq k-1\right)$
(i.e. divide j by k) remainder

$\tau^k = (\sigma^q)^k \cdot \sigma^r$. Let $\tau' = \tau \cdot \sigma^{-q}$, so that

$$(\tau')^k = \sigma^r$$

$0 \leq r \leq k-1$; And
$k \leq \text{order}(\tau) \leq m$

k = smallest s such that $(2 \leq s \leq \text{ord}(\tau'))$ $(\tau')^s \in \langle\sigma\rangle$
(because $\tau' \in \tau \cdot \langle\sigma\rangle$)

$$\text{order}(\tau') = k \cdot \frac{m}{\gcd(m,r)} \leq m \Longleftarrow$$

(by defn. of m)

If $r \neq 0$, $\frac{k}{\gcd(r,m)} \geq 1$ contradicting

So $r = 0$; meaning $(\tau')^k = e$; and hence $\text{ord}(\sigma\tau') = \text{lcm}(k, m) \leq m$

$(k = \text{order}(\tau')) \Rightarrow k$ divides m. $\square$