Lecture 22

(22.0) Summary of last lecture (analogies with Euler's φ-function).

- $\mathrm{Aut}_{gp}(\mathbb{Z}/n\mathbb{Z})$ has $\varphi(n)$ elements; and is an abelian group

- $n = p_1^{a_1} p_2^{a_2} \cdots p_\ell^{a_\ell} \longrightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{a_\ell}\mathbb{Z}$

- $\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_\ell^{a_\ell}) \rightarrow \mathrm{Aut}_{gp}(\mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Aut}_{gp}(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times \mathrm{Aut}_{gp}(\mathbb{Z}/p_\ell^{a_\ell}\mathbb{Z})$

- $\varphi(p^r) = p^{r-1}(p-1) \longrightarrow$ (p: odd) $\mathrm{Aut}_{gp}(\mathbb{Z}/p^r\mathbb{Z})$ is cyclic

  (p: even) $\mathrm{Aut}_{gp}(\mathbb{Z}/2^r\mathbb{Z})$ has 2 pieces

  $\mathbb{Z}/2\mathbb{Z}$ & $\mathbb{Z}/2^{r-2}\mathbb{Z}$.

(22.1) Example: Classify all groups of order 18.

Let G be a group with 18 elements $(18 = 2 \cdot 3^2)$.

By Sylow Theorems we have $P \leq G$ a subgroup w/ 2 elements

$Q \leq G$ a subgroup w/ 9 elts.

Note : $Q \trianglelefteq G$ (because it has index 2 - Ex.: for any group H, and a subgroup $K \leq H$ s.t. $|H/K| = 2$, we automatically get that K is <u>normal</u> in H).

Alternate proof (Sylow Thm part 3).

$$n_3 = \# \mathrm{Syl}_3(G) \equiv 1 \pmod 3 \quad \text{and } n_3 \text{ divides } 2$$

$$\Rightarrow \quad n_3 = 1.$$

In conclusion :
- $P \leq G$ and $Q \trianglelefteq G$
- $P \cap Q = \{e\}$ (because $|P|$ & $|Q|$ are coprime)
- $P . Q = Q . P = G$

because Q is normal

because $|P.Q|$ is divisible by $2 = |P|$ & $9 = |Q|$

(see Lecture 19, page 7).

Hence $G \cong Q \rtimes_\alpha P$

for some $\alpha : P \longrightarrow \mathrm{Aut}_{gp}(Q)$ group hom.

Options for P & Q :

$P \cong \mathbb{Z}/2\mathbb{Z}$; $Q \cong \mathbb{Z}/9\mathbb{Z}$ or $(\mathbb{Z}/3\mathbb{Z})^2$.

(22.2) Case $P \cong \mathbb{Z}/2\mathbb{Z}$, $Q \cong \mathbb{Z}/9\mathbb{Z}$.

As $\mathrm{Aut}_{gp}(Q)$ is cyclic with $\varphi(9) = 3(3-1) = 6$ elements,

let $\sigma \in \mathrm{Aut}_{gp}(Q)$ be a generator, so that

$$\mathrm{Aut}_{gp}(Q) = \{ \mathrm{Id}_Q, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 \} \quad \left(\begin{array}{l} \text{say, e.g.,} \\ \sigma : Q \longrightarrow Q \\ 1 \bmod 9 \longmapsto 5 \bmod 9 \end{array} \right)$$

Group hom-s

$$\begin{array}{ccc} P & \xrightarrow{\alpha} & \mathrm{Aut}_{gp}(Q) \\ \| & & \Downarrow \\ \{0,1\} & & \alpha(1) \end{array} \longleftrightarrow \begin{array}{c} \text{order 2 elements in} \\ \mathrm{Aut}_{gp}(Q) \\ (\& \ \mathrm{Id}_Q). \end{array}$$

The only possibilities are $\begin{cases} \alpha(1) = \mathrm{Id}_Q & \text{i.e. } \alpha \text{ is trivial} \\ \alpha(1) = \sigma^3 \end{cases}$

$$\alpha(1) = \mathrm{Id}_Q \quad \rightsquigarrow \quad Q \rtimes_\alpha P \cong Q \times P \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$\cong \mathbb{Z}/18\mathbb{Z}$$

$\alpha(1) = \sigma^3$. Now

$$\sigma^3 : Q \longrightarrow Q$$
$$1 \bmod 9 \longmapsto 5^3 \equiv -1 \pmod 9)$$

Meaning $Q \rtimes_\alpha P$ can be explicitly described as follows:

if $P = \langle x \rangle$, $Q = \langle y \rangle$ so that $x^2 = e_P$ (id of P)

$y^9 = e_Q$ (id of Q)

then

$$(e_Q, x) \cdot (y, e_P) = (\alpha(x)(y), x.e_P)$$
$$= (y^{-1}, x) = (y^{-1}, e_P)(e_Q, x).$$

Thus (identifying (e_Q, x) with x
(y, e_P) with y)

$$G \cong \langle x, y \mid x^2 = y^9 = e \ \& \ xyx = y^{-1} \rangle$$

i.e. D_{18}.

(22.3) $P \cong \mathbb{Z}/2\mathbb{Z}$ and $Q \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

- $\mathrm{Aut}_{gp}(Q)$ can be viewed as 2×2 invertible matrices with entries from $\mathbb{F}_3$ $(\cong \mathbb{Z}/3\mathbb{Z})$. (recall $|GL_2(\mathbb{F}_3)| = 8\cdot 6 = 48$)

Reason:

$$Q \ni (a \pmod 3,\ b \pmod 3)$$
$$\big\downarrow \sigma \longleftarrow \text{typical } \sigma \in \mathrm{Aut}_{gp}(Q)$$
$$Q \ni (\alpha a + \beta b \pmod 3,\ \gamma a + \delta b \pmod 3)$$

where
$$(\alpha \pmod 3,\ \gamma \pmod 3) = \sigma(\bar{1}, 0)$$
$$(\beta \pmod 3,\ \delta \pmod 3) = \sigma(0, \bar{1})$$

Thus σ can be written as $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$: 2×2-matrix w/ entries from $\mathbb{F}_3$.

Ex. Composition of elements of $\mathrm{Aut}_{gp}(Q)$
= Matrix multiplication

($\sigma = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ is an iso. $\iff \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ is invertible)

Now we are looking for $\alpha : P \longrightarrow \operatorname{Aut}_{gp}(Q) \; (= GL_2(\mathbb{F}_3))$
gp. hom-s

$$\text{generator} \longmapsto X$$

$$X^2 = Id_Q. \quad \text{i.e.} \quad \det(X) = \pm 1 \quad (= \mathbb{F}_3^\times)$$

$$X = X^{-1}.$$

$$\Rightarrow \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix} \quad (\text{if } \det = +1)$$

$$= - \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix} \quad (\text{if } \det = -1)$$

1st row: $X = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = -Id_Q$

2nd row: $\alpha + \delta = 0.$ $\quad \alpha\delta - \beta\gamma = -1$

- $\alpha = \delta = 0$: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ or $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$
- $\alpha = 1, \delta = -1$: $X = \begin{bmatrix} 1 & x \\ 0 & -1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ x & -1 \end{bmatrix}$ $x \in \mathbb{F}_3$.
- $\alpha = -1, \delta = 1$: $X = \begin{bmatrix} -1 & x \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} -1 & 0 \\ x & 1 \end{bmatrix}$ $x \in \mathbb{F}_3$

Total 16. However, there are only 3 conjugacy classes.

(22.4)

General Lemma. – Let H, N be two groups

$$\alpha, \beta : H \longrightarrow \mathrm{Aut}_{gp}(N) \quad \text{two gp. hom-s.}$$

<u>Assume</u>, there exists $T \in \mathrm{Aut}_{gp}(N)$ s.t.

$$\alpha(h)(n) = T\Big(\beta(h)\big(T^{-1}(n)\big)\Big) \quad \forall\, h \in H,\ n \in N.$$

Then $N \rtimes_\alpha H$ and $N \rtimes_\beta H$ are isomorphic.

Proof. Define

$$\begin{aligned} N \rtimes_\beta H &\xrightarrow{\ f\ } N \rtimes_\alpha H \quad \text{as:} \\ (n, h) &\longmapsto (T(n), h) \end{aligned}$$

Check: f is a group hom.

$$\begin{aligned} f\big((n_1,h_1) \cdot_\beta (n_2,h_2)\big) &= f\big(n_1 \cdot \beta(h_1)(n_2),\ h_1h_2\big) \\ &= \Big(T(n_1) \cdot T\big(\beta(h_1)(n_2)\big),\ h_1h_2\Big) \\ f(n_1,h_1) \cdot_\alpha f(n_2,h_2) &= \big(T(n_1), h_1\big) \cdot_\alpha \big(T(n_2), h_2\big) \\ &= \Big(T(n_1) \cdot \alpha(h_1)\big(T(n_2)\big),\ h_1h_2\Big) \end{aligned}$$

are equal because $\alpha(h)\big(T(n)\big) = T\big(\beta(h)(n)\big) \quad \forall\, h \in H,\ n \in N.$

Now f is clearly an iso., with inverse $(n, h) \mapsto (T^{-1}(n), h)$.

$\square$

(22.5) Back to the end of page 5.

Ex. Verify that all 14 matrices corresponding to the case

$$\alpha + \delta = 0, \quad \alpha\delta - \beta\gamma = -1$$

are conjugate to each other. (say all conj to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$)

(e.g. $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{-1}$.)

So our options for $\alpha : P \longrightarrow \mathrm{Aut}_{gp}(Q)$ $(= GL_2(\mathbb{F}_3))$

are: generator $\longmapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

(up to conjugation) or $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

We get 3 more groups

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \rightsquigarrow \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 = \left\langle x, y_1, y_2 \;\middle|\; \begin{array}{c} x^2 = y_1^3 = y_2^3 = e \\ y_1 y_2 = y_2 y_1 \\ x y_1 x = y_1 \\ x y_2 x = y_2 \end{array} \right\rangle$$

$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \rightsquigarrow$ " change $\bigcirc$ to $x y_1 x = y_1^{-1}$, $x y_2 x = y_2^{-1}$ ".

$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \rightsquigarrow$ " ______ $x y_1 x = y_1$, $x y_2 x = y_2^{-1}$ ".