Lecture 21

(21.0) Recall: we have the following method of constructing semidirect products

Input: H, N = 2 groups
$\alpha: H \longrightarrow \mathrm{Aut}_{gp}(N)$
a group hom.

Output: $N \rtimes H$
$= \{(n,h) \mid n \in N, h \in H\}$
$(n_1, h_1) \cdot (n_2, h_2)$
$= (n_1 \alpha(h_1)(n_2), h_1 h_2)$

This brought into focus the importance of understanding $\mathrm{Aut}_{gp}(W)$ of a group W.

By defn $\mathrm{Aut}_{gp}(W)$ consist of all isomorphisms $f: W \xrightarrow{\cong} W$.

Lemma: W cyclic $\Rightarrow$ $\mathrm{Aut}_{gp}(W)$ is abelian.

Proof: Fix a generator $\sigma \in W$. Then any gp hom $f: W \to W$ is completely determined by $x = f(\sigma) \in W$.

$W = \mathbb{Z}/m\mathbb{Z}$ (written additively) $\quad f: W \to W$
$1 \longmapsto x \pmod m$

is an iso. if and only if $\exists\ y \in W$ s.t. $xy \equiv 1 \pmod m$
$(\ \| \ f(y))$

i.e. $\gcd(x, m) = 1$.

Moreover group operation:

$$W \xrightarrow{f_x} W \xrightarrow{f_y} W$$
$$1 \longmapsto x \longmapsto yx = xy$$

by $f_{xy} = f_{yx}$

hence abelian $\square$

(21.1) $\mathrm{Aut}_{gp}\left(\mathbb{Z}/n\mathbb{Z}\right) = ?$

So far we know that it has $\varphi(n) = \#\{x \mid x \in \{1,\dots,n-1\},\ \gcd(x,n)=1\}$ (Euler's φ fn.) elements, and that it is abelian.

- Writing $n = p_1^{a_1} \cdots p_\ell^{a_\ell}$, we get ($p_1,\dots,p_\ell$ distinct primes. $a_1,\dots,a_\ell \geq 1$.)

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_\ell^{a_\ell}\mathbb{Z}$$

As there are no non-trivial group hom-s between $\mathbb{Z}/p_i^{a_i}\mathbb{Z}$ & $\mathbb{Z}/p_j^{a_j}\mathbb{Z}$ for $i \neq j$, we obtain first reduction.

$$\mathrm{Aut}_{gp}\left(\mathbb{Z}/n\mathbb{Z}\right) \cong \prod_{i=1}^{\ell} \mathrm{Aut}_{gp}\left(\mathbb{Z}/p_i^{a_i}\mathbb{Z}\right)$$

Recall: for Euler's φ-function: $\varphi(p_1^{a_1}\cdots p_\ell^{a_\ell}) = \varphi(p_1^{a_1})\cdots\varphi(p_\ell^{a_\ell})$

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{a_1} \times \dots \times \mathbb{Z}/p_\ell^{a_\ell}$

$(f_1(x_1),\dots,f_\ell(x_\ell)) \longleftarrow (x_1,\dots,x_\ell) : (f_1, f_2, \dots, f_\ell)$

So, it is enough to answer : $\mathrm{Aut}_{\text{ab gp}}\left(\mathbb{Z}/p^r\mathbb{Z}\right) = ?$

where p is a prime and $r \geq 2$.

(21.2) Theorem. $\mathrm{Aut}_{gp}\left(\mathbb{Z}/p\mathbb{Z}\right)^{*}$ is cyclic. (as an additive gp.)

(ie. $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, as a mult. gp. $\cong \mathbb{Z}/(p-1)\mathbb{Z}$.)

notation $\mathbb{F}_p^{\times}$ below

e.g.

$p = 5$; $\mathbb{F}_5^{\times} = \{1, 2, 3, 4\}$

$2^0 = 1$; $2^1 = 2$; $2^2 = 4$; $2^3 = 3$; $2^4 = 1$ (modulo 5)

so order of 2 in $\mathbb{F}_5^{\times} = 4 = \#(\mathbb{F}_5^{\times})$, hence cyclic.

$p = 7$; $\mathbb{F}_7^{\times} = \{1, 2, 3, 4, 5, 6\}$

$2^0 = 1$; $2^1 = 2$; $2^2 = 4$; $2^3 = 1$ (mod 7)

$\text{order}_{\mathbb{F}_7^{\times}}(2) = 3 = \frac{1}{2}\left|\mathbb{F}_7^{\times}\right|$ so it cannot be taken as a generator.

$3^0 = 1$; $3^1 = 3$; $3^2 = 2$; $3^3 = 6 = -1$ in $\mathbb{F}_7$

$\Rightarrow$ order(3) $= 6 = \left|\mathbb{F}_7^{\times}\right|$ hence 3 can be taken as a generator of the multiplicative group $\mathbb{F}_7^{\times}$.

Recall: $a^{p-1} \equiv 1 \pmod p$ for every $a \in \mathbb{F}_p^{\times}$

just because $x^{|G|} = e \quad \forall\, x \in G$.

(order(x) divides $|G|$)

(21.3) Proof of Theorem (21.2).-

As $\mathbb{F}_p^\times$ is an abelian group; if we set m = exponent of $\mathbb{F}_p^\times$

(i.e., $m = \max\{s \mid s = \text{order of } \sigma \text{ for some } \sigma \in \mathbb{F}_p^\times\}$)

then $\tau^m = 1 \quad (\forall\ \tau \in \mathbb{F}_p^\times)$

i.e. we have $p-1$ distinct solutions (modulo p)

of the congruence equation

$$X^m \equiv 1 \pmod{p}. \qquad (*)$$

see (21.6) below.

But | number of solns. of a polynomial equation of degree m $\leq m$ |

$\Rightarrow p-1 \leq m \leq p-1 \Rightarrow m = p-1.$

Hence $\mathbb{F}_p^\times$ has an element of order $p-1$, proving that it is cyclic.

(21.4) Back to $\underset{gp}{Aut}\left(\mathbb{Z}/p^r\mathbb{Z}\right)$.

Recall: $\varphi(p^r) = p^{r-1}(p-1)$. Let us first assume $p \neq 2$.

φ ↑ Euler's fn.

e.g. $G := \mathrm{Aut}_{gp}\left(\mathbb{Z}/5^2\mathbb{Z}\right)$ $\quad p = 5,\ r = 2.$

$5(5-1) = 20$ elements $= \mathbb{Z}/25\mathbb{Z} \setminus \{0, 5, 10, 15, 20\}$

$5(5-1) = 5 \cdot 2^2$

We already know $G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \left(\cong \mathbb{Z}/20\mathbb{Z}\right)$

or $\mathbb{Z}/5\mathbb{Z} \times \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \quad \left(\cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right)$

But $x \pmod{25} \longmapsto x \pmod 5$ is a surjective gp. hom. $G \longrightarrow \left(\mathbb{Z}/5\mathbb{Z}\right)^\times \setminus \{0\}$

$= \mathbb{F}_5^\times \left(\cong \mathbb{Z}/4\mathbb{Z}\right)$ by Thm. 21.2.

so we conclude that we must be in the first case; i.e. $\mathrm{Aut}_{gp}\left(\mathbb{Z}/5^2\mathbb{Z}\right)$ is a cyclic group.

Cor. of Theorem (21.2): If p is an odd prime, then $\mathrm{Aut}_{gp}\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ is a cyclic gp. of size $p^{r-1}(p-1)$.

(21.5) $p = 2$; $r \geq 2$. $\quad \varphi(2^r) = 2^{r-1}$.

Small cases: $W = \mathbb{Z}/2\mathbb{Z}$ $\quad \mathrm{Aut}_{gp}(W) = \{\mathrm{id}\}$

$W = \mathbb{Z}/2^2\mathbb{Z}$ $\quad \mathrm{Aut}_{gp}(W) = \{1, 3\} \ (\cong \mathbb{Z}/2)$ mult. mod 4.

$W = \mathbb{Z}/8\mathbb{Z}$ $\quad \mathrm{Aut}_{gp}(W) = \{1, 3, 5, 7\}$

$3^2 = 9 \equiv 1 \pmod 8$

$5^2 = 25 \equiv 1 \ (\text{"})$

$7^2 = 49 \equiv 1 \ (\text{"})$

$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ NOT cyclic!

$W = \mathbb{Z}/16\mathbb{Z}$ $\quad \mathrm{Aut}_{gp}(W) = \{1, 3, 5, 7, 9, 11, 13, 15\}$

x / $\mathrm{ord}(x)$	3	5	7	9	11 (=−5)	13 (=−3)	15
	4	4	2	2	4	4	2

so we get $\boxed{\mathbb{Z}/2\mathbb{Z}} \times \mathbb{Z}/4\mathbb{Z}$.

$\mathbb{Z}/4\mathbb{Z}$: cyclic group of size 2^{r-2}

$\boxed{\mathbb{Z}/2\mathbb{Z}}$: we can always get by reducing modulo 4

Ex. $\mathrm{Aut}_{gp}\left(\mathbb{Z}/2^r\mathbb{Z}\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ $(\forall r \geq 2)$.

Hint: use binomial theorem to show that:

$(1+2^2)^{2^{r-2}} \equiv 1 \pmod{2^r}$ but $(1+2^2)^{2^{r-3}} \not\equiv 1 \pmod{2^r}$

(5) so order $(5) = 2^{r-2}$. (ex. # 22 of 2.3 of textbook)

(21.6) # Solutions of $f(X) = 0$ $\leq$ degree (f).

Reason: Euclidean division works for polynomials. If we try, we can divide $f(X)$ by $X - \alpha$ for any number α.

By division algorithm, we end up writing

$$f(X) = (X-\alpha)\, q(X) + \beta$$

(β: remainder.)

So $f(\alpha) = 0$ iff $f(X) = (X-\alpha)\, q(X)$ ($\deg q = \deg(f) - 1$)

By Induction - # of solns. to $f(X) = 0$

$\leq$ 1 + # (solns. to $q(X) = 0$)

$\leq$ 1 + degree (q) = degree (f).