Semidirect product:

$N, H, \alpha: H \longrightarrow Aut_{gp}(N) \Rightarrow G := N \rtimes_\alpha H.$

$Aut_{gp}(W) = ?$

if $W = \mathbb{Z}/n\mathbb{Z}$, $Aut_{gp}(W)$ is abelian

$f: W \longrightarrow W$

$1 \longmapsto x \pmod n$ invertible i.e. coprime to n.

$|Aut_{gp}(\mathbb{Z}/n\mathbb{Z})| = \phi(n)$.

$\phi(p_1^{a_1} \cdots p_\ell^{a_\ell}) = \phi(p_1^{a_1}) \cdots \phi(p_\ell^{a_\ell})$, and $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

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

So putting Aut_{gp} around everything works.

So computing $Aut_{gp}(\mathbb{Z}/n\mathbb{Z})$ reduces to computing $Aut(\mathbb{Z}/p^r\mathbb{Z})$.

Assume $r=1$.

<u>Thm</u>: $Aut_{gp}(\mathbb{Z}/p\mathbb{Z})$ is cyclic of size $p-1$.

$$\begin{array}{ccc} f\{1 \mapsto x\} & & Aut_{gp}(\mathbb{Z}/p\mathbb{Z}) \\ \Big\uparrow & & \wr\Vert \\ x & & \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \\ & & \Vert \\ & \text{Notation:} & \mathbb{F}_p^\times \end{array}$$

$\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ as a group under multiplication.

eg: $p=5$, $\mathbb{F}_5^\times = \{1,2,3,4\}$. $2^0 = 1$, $2^1=2$, $2^2=4$, $2^3=3$, $2^4=1$ (mod 5)

order of 2 is 4 $\Rightarrow$ $\mathbb{F}_5^\times$ is cyclic.

$p=7$, $\mathbb{F}_7^\times = \{1,2,3,4,5,6\}$. ord$(2)=3 \neq 6$ bad 2.

$3^0=1$, $3^1=3$, $3^2=2$, $3^3=-1$, ... ord$(3)=6$.

<u>Proof of Thm</u> $\mathbb{F}_p^\times$ is a group w/ $p-1$ elts $\Rightarrow$ $a^{p-1}\equiv 1 \pmod p$ (FLT).

$\mathbb{F}_p^\times$ is abelian let $\overset{\text{exponent}}{m} = \max\{\text{order}(\sigma) \mid \sigma \in \mathbb{F}_p^\times\}$.

We proved $\tau^m = 1$ for all $\tau \in \mathbb{F}_p^\times$.

We have $p-1$ distinct solutions to $X^m \equiv 1 \pmod p$

A poly eqn has #roots $\leq$ degree.

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

Why is # roots of $f(x)=0 \leq$ degree (f)?

Division algorithm works for polynomials

$$X-\alpha \,\overline{\big)\, X^M + a_{M-1}X^{M-1} + \cdots} = f(X).$$

$$f(X) = (X-\alpha)\,q(X) + \overset{\text{remainder, a \#.}}{\beta}$$

hence if α is a root, $\beta=0$, and $f(X) = (X-\alpha)\,q(X)$

for q some poly of degree 1 less than f.

Now induct.

eg $\mathrm{Aut}_{gp}(\mathbb{Z}/25\mathbb{Z})$ is abelian w/ $5\cdot 2^2$ elements.

two possibilities: $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z} \pmod{25} \longmapsto \mathbb{Z} \pmod 5$$

$$G \xrightarrow[\text{gp hom}]{\text{surjective}} \mathbb{F}_5^\times$$

so it can't be the $(\mathbb{Z}/2\mathbb{Z})^2$ possibility.

$$\| $$

$$\mathbb{Z}/25\mathbb{Z} \setminus \{0,5,10,15,20\}$$

(whoever goes to the cyclic generator $2 \in \mathbb{F}_5^\times$ must have order divisible by 4).

<u>Thm (2)</u> If p is an odd prime

$$G = \mathrm{Aut}_{gp}(\mathbb{Z}/p^r\mathbb{Z}) \text{ is cyclic.}$$

pf

$$G = \mathbb{Z}/p^r\mathbb{Z} \setminus \{0, p, 2p, \dots\}$$

$$|G| = \phi(p^r) = p^{r-1}(p-1).$$

$$\left.\begin{array}{ccc} G & \longrightarrow & \mathbb{F}_p^\times \\ x \bmod p^r & \longmapsto & x \bmod p \end{array}\right\} \text{surjective gp. hom}$$

§2.3 #21 $\longrightarrow$ <u>Ex:</u> Order of $(1+p)$ in G is p^{r-1}, so p^{r-1}-sylow subgp is $\mathbb{Z}/p^{r-1}\mathbb{Z}$.

And the surjectivity ~~of~~ of map means some element must have order $p-1$, so

$$\mathrm{Aut}_{gp}(\mathbb{Z}/p^r\mathbb{Z}) \cong \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$$

$$\cong \mathbb{Z}/\phi(p^r)\,\mathbb{Z}$$

meaning

$$\mathrm{Aut}_{gp}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/\phi(n)\,\mathbb{Z} \text{ , as long as } n \text{ is odd.}$$

What if $p=2$? Theorem does not hold.

W	$\mathrm{Aut}_{gp}(W)$
$\mathbb{Z}/2\mathbb{Z}$	$\{id\}$
$\mathbb{Z}/4\mathbb{Z}$	$\{id, 1\mapsto 3\} \cong \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/8\mathbb{Z}$	$\{id, x, y, z\}$, $x^2=y^2=z^2=id$ $\cong (\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

since its $\{1, 3, 5, 7\}$

$$\left.\begin{array}{l} 1^2=1 \\ 3^2=9 \\ 5^2=25 \\ 7^2=49 \end{array}\right\} \equiv 1 \bmod 8.$$

① $x \pmod{2^r} \longmapsto x \bmod 4$

$\mathrm{Aut}_{gp}(\mathbb{Z}/16\mathbb{Z}) \longrightarrow \mathrm{Aut}_{gp}(\mathbb{Z}/4\mathbb{Z})$

EX: 2.3 #22

② Order of 5 is 2^{r-2}.

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

So we know automorphism groups of cyclic groups.

$$\begin{array}{l} \mathbb{Z}/120\mathbb{Z}. \qquad 120 = 2^3 \cdot 3 \cdot 5 \\ \quad \| \\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \end{array}$$

So $\mathrm{Aut}_{gp}\left(\mathbb{Z}/120\mathbb{Z}\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$