Lecture XXVI: Computing $\mathrm{Aut}_{Gp}(G)$ II

Recall: Last time we showed $\mathrm{Aut}_{Gp}(\mathbb{Z}/m\mathbb{Z})$ can be reduced to the case when $m = 0, 1$ or a prime power.

Proposition: Fix $m \in \mathbb{N}$, $m \geq 2$ & let $m = p_1^{a_1} \cdots p_k^{a_k}$ be its prime factorization. ($p_1, \ldots, p_k$ distinct primes, $a_1, \ldots, a_k \in \mathbb{N}$). Then:

$$\mathrm{Aut}_{Gp}\left(\mathbb{Z}/m\mathbb{Z}\right) \simeq \prod_{i=1}^{k} \mathrm{Aut}_{Gp}\left(\mathbb{Z}/p_i^{a_i}\mathbb{Z}\right)$$

via Ψ :

$$\prod_{i=1}^{k} \mathrm{Aut}_{Gp}\left(\mathbb{Z}/p_i^{a_i}\mathbb{Z}\right) \longrightarrow \mathrm{Aut}_{Gp}\left(\mathbb{Z}/m\mathbb{Z}\right) \simeq \mathrm{Aut}_{Gp}\left(\mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}\right)$$

$$\underline{f} = (f_1, \ldots, f_k) \longmapsto \left(\Psi(\underline{f}) : (x_1, \ldots, x_k) \longmapsto (f_1(x_1), \ldots, f_k(x_k))\right)$$

Theorem 1 $\quad \mathrm{Aut}_{Gp}\left(\mathbb{Z}/p\mathbb{Z}\right) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

Q: What happens for $\mathrm{Aut}_{Gp}\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ for $r \geq 2$?

A $\left|\mathrm{Aut}_{Gp}\left(\mathbb{Z}/p^r\mathbb{Z}\right)\right| = \varphi(p^r) = p^{r-1}(p-1)$ $\quad \left(\#\{x \in \mathbb{Z}/p^r\mathbb{Z} \;\; \gcd(x,p) = 1\}\right)$

Why? Division algorithm $\Rightarrow x = pq + s$ $\quad s \in \{1, \ldots, p-1\}$ ($\neq 0$ because $p \nmid x$), $\quad q \in \{0, 1, \ldots, p^{r-1}\}$

So $x \longleftrightarrow (q, s)$ is 1-to-1 correspondence $\quad \#q = p^{r-1}$ & $\#s = p-1$.

We have 2 different answers, depending on the parity of p.

§26.1 Case 1: p odd:

Example: $G := \mathrm{Aut}_{Gp}\left(\mathbb{Z}/5^2\mathbb{Z}\right)$ $\quad p = 5$ $\quad r = 2$

$\varphi(25) = 5^1 \cdot (5-1) = 20 = \mathbb{Z}/25\mathbb{Z} \setminus \{0, 5, 10, 15, 20\}$ $\Rightarrow$ G is abelian & order $= 20$

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

$\mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ $\quad (\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z})$ $\quad 2 \mid 10$.

Q: Which one is it? **A:** It's the first one!

Reason: $\exists$ $G \longrightarrow \mathbb{Z}/5\mathbb{Z} \setminus \{0\} = \mathbb{F}_5^* (\simeq \mathbb{Z}/4\mathbb{Z})$ surjective sp homomorphism

$\sigma_x \longmapsto x \pmod 5$

$(x \bmod 25)$ $\quad 5 \nmid x$

$\Rightarrow \mathrm{Aut}_{Gp}\left(\mathbb{Z}/_{5^2\mathbb{Z}}\right) \simeq \mathbb{Z}/_{5\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \simeq \mathbb{Z}/_{20\mathbb{Z}}$ is cyclic

Theorem 2: If p is an odd prime, then $\mathrm{Aut}_{Gp}\left(\mathbb{Z}/_{p^r\mathbb{Z}}\right)$ is cyclic of order $p^{r-1}(p-1)$

Proof: $W := \mathrm{Aut}_{Gp}\left(\mathbb{Z}/_{p^r\mathbb{Z}}\right) = \{\sigma_x : \mathbb{Z}/_{p^r\mathbb{Z}} \longrightarrow \mathbb{Z}/_{p^r\mathbb{Z}} \;:\; x \in \mathbb{Z}/_{p^r\mathbb{Z}},\ \gcd(x,p)=1\}$

$1 \longmapsto x \pmod{p^r}$

$= \mathbb{Z}/_{p^r\mathbb{Z}} \setminus \{0, p, 2p, \ldots, (p^{r-1}-1)p\}$

is abelian and has order $p^{r-1}(p-1)$.

- W has a Sylow p-subgroup of order p^{r-1}, $H \leq \left(\mathbb{Z}/_{p^r\mathbb{Z}}\right)^*$

Claim: $H \simeq \mathbb{Z}/_{p^{r-1}\mathbb{Z}}$

Pf/ Using the Binomial Theorem, we show:

(1) $(1+p)^{p^{r-1}} \equiv 1 \pmod{p^r}$

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

Since $\mathrm{ord}(1+p) \mid p^{r-1}$ this will prove $\mathrm{ord}(1+p) = p^{r-1}$ so H is cyclic

- **Let's show (1):** The Binomial Theorem gives $(1+p)^{p^{r-1}} = 1 + \sum_{k=1}^{p^{r-1}} \binom{p^{r-1}}{k} p^k$

We show $p^r \mid \binom{p^{r-1}}{k} p^k \quad \forall k = 1, \ldots, p^{r-1}$.

We write $k = p^j m \quad p \nmid m \quad 0 \leq j \leq p^{r-1}$

$\Rightarrow p^k \binom{p^{r-1}}{k} = p^k (p^{r-1}) \dfrac{(p^{r-1}-1)!}{(p^j m)!(p^{r-1}-p^j m)!} = p^k \, p^{r-1-j} \dfrac{}{m} \binom{p^{r-1}-1}{p^j m - 1}$

This expression lies in $\mathbb{Z}$ & $p \nmid m \Rightarrow m \mid \binom{p^{r-1}-1}{p^j m - 1}$

$\Rightarrow p^k \binom{p^{r-1}}{k} = p^{r-1-j+k} \underbrace{\frac{1}{m}\binom{p^{r-1}-1}{p^j m - 1}}_{\in \mathbb{Z}}$

Thus, $p^r \mid p^k \binom{p^{r-1}}{k}$ if $p^r \mid p^{r-1-j+k} = p^{r-1-j+p^j m}$

$\Leftrightarrow r \leq r-1-j+p^j m \Leftrightarrow 1+j \leq p^j m$ for $0 \leq j \leq p^{r-1}$, $p \nmid m$

We show: $1+j \leq p^j m$ for $0 \leq j \leq p^{r-1}$, $p \nmid m$ by induction on j.

- Base Case: $j = 0 \overset{1 \leq m}{\leq} m$ ✓

- Inductive Step: $p^{j+1}m = p(p^j m) \underset{IH}{\geq} p(1+j) = p+pj \geq 2+2j \geq j+2$. ✓

- Let's show (2): By the same method, we write $(1+p)^{p^{r-2}} = 1+\binom{p^{r-2}}{1}p + \sum_{k=2}^{p^{r-2}}\binom{p^{r-2}}{k}p^k$

$$= 1+p^{r-1} + \sum_{k=2}^{p^{r-2}}\binom{p^{r-2}}{k}p^k$$

We show $p^r \mid \binom{p^{r-2}}{k}p^k \quad \forall k = 2,3,\dots,p^{r-2}$ as above.

We write $k = p^j m \quad p \nmid m \quad 0 \leq j \leq p^{r-2} \quad (j,m) \neq (0,1)$.

$$\Rightarrow p^k\binom{p^{r-2}}{k} = p^{p^j m}\binom{p^{r-2}}{p^j m} = p^{p^j m}p^{r-2-j}\underbrace{\frac{\perp}{m}\binom{p^{r-2}-1}{p^j m-1}}_{\in \mathbb{Z}}$$

Thus, $p^r \mid p^{r-2-j+p^j m}$ if $r \leq r-2-j+p^j m \iff 2+j \leq p^j m$

We show: $2+j \leq p^j m$ if $0 \leq j \leq p^{r-2}$, $p \nmid m$ & $(j,m) \neq (0,1)$ by induction on j

- Base Cases: $j=0 \Rightarrow m \geq 2 = 2+0$ ✓
  $j=1$ & $m=1$: $2+1 \leq p$ True because p is ODD ← Here we are using p is ODD.

- Inductive Step: $j \geq 0$. We treat 2 cases

If $m \geq 2$ $\quad p^{j+1}m = p(p^j m) \underset{\substack{(IH)\\(j,m)\neq(0,1)}}{\geq} p(2+j) = 2p+pj \geq 4+j > j+2$ ✓

If $m=1 \Rightarrow j \geq 1$ since $(j,m)=(0,1)$ is not allowed.

Thus, $p^{j+1}m = p(p^j m) \underset{\substack{IH\\(j,m)\neq(0,1)}}{\geq} p(2+j) > j+2$ ✓

Since $1+p^{r-1} \neq 0 \bmod p^{r-1}$, we get $(1+p)^{p^{r-2}} \equiv 1+p^{r-1} \neq 0 \ (\bmod p^r)$ □

Note: Item (2) is only True for p odd

$$\Rightarrow W \simeq \mathbb{Z}/p^{r-1}\mathbb{Z} \times \underbrace{\prod_{i=1}^{k} S_i}_{=:Q}$$

S_i sylow p_i-subgroups with $\prod_{i=1}^{k}|S_i| = (p-1)$

↳ Here we are using that p is odd.

by Theorem 1 §20.1.

- $\exists \ G \xrightarrow{\Psi} \mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ surjective homomorphism

$\sigma_x \longmapsto x \bmod p$

$x \bmod p^r$
$p \nmid x$

This map restricted to $\mathbb{Z}/p^{r-1}\mathbb{Z} = H \leq W$ is Trivial because $H = \langle 1+p \rangle$

$\ker \Psi = \{\sigma_x \mid x \equiv 1 \pmod p\} = W \cong \mathbb{Z}/p^{r-1}\mathbb{Z}$ & $\ker \Psi \cap Q = \{e\}$ for coprimality reasons.

$\Rightarrow \Psi|_Q : Q := \prod_{i=1}^{k} P_i \hookrightarrow \mathbb{F}_p^*$ is an injective gp homomorphism.

Since these groups have the same size, we conclude that $\prod_{i=1}^{k} P_i \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Thus $W \cong \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{Z}/p^{r-1}(p-1)\mathbb{Z}$ as we wanted. □

§26.2 Case 2: $p = 2$:

Note: $\varphi(2^r) = 2^{r-1}$ $\forall r \geq 1$

We first look at some examples:

Examples: (1) $\mathrm{Aut}_{Gp}(\mathbb{Z}/2\mathbb{Z}) = \mathbb{F}_2^* = \{1\}$ by Theorem 1. (cyclic!)

(2) $\mathrm{Aut}_{Gp}(\mathbb{Z}/4\mathbb{Z}) = \{1, 3\} \cong \mathbb{Z}/2\mathbb{Z}$ (mult mod 4) (cyclic!)

(3) $\mathrm{Aut}_{Gp}(\mathbb{Z}/8\mathbb{Z}) = \{1, 3, 5, 7\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (mult mod 8), $\langle 3 \rangle$, $\langle 5 \rangle$

$3^2 = 5^2 = 7^2 \bmod 8$

$3 \cdot 5 = 7 \bmod 8$

Not cyclic!

(4) $\mathrm{Aut}_{Gp}(\mathbb{Z}/16\mathbb{Z}) = \{1, 3, 5, 7, 9, 11, 13, 15\}$ (mult mod 16)

Let's compute the order of these elements:

x	1	3	5	7	9	$11 = -5$	$13 = -3$	$15 = -1$
$\mathrm{ord}\, x$	1	4	4	2	2	4	4	2

We get $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\langle 15 \rangle$, $\langle 5 \rangle$ → cyclic group of size 2^{r-2}

$5^2 = 9 = 3^2$, $5^3 = 13 = -3$, $5^4 = -15 = 1 \pmod{16}$

comes from $x \pmod{16} \longmapsto x \pmod 4$

Theorem 3: $\forall r \geq 3$: $\mathrm{Aut}_{Gp}(\mathbb{Z}/2^r\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$

Proof: We claim $\mathbb{Z}/2^{r-2}\mathbb{Z} \hookrightarrow W = \mathrm{Aut}_{Gp}(\mathbb{Z}/2^r\mathbb{Z})$ by $1 \longmapsto 5$.

Claim 1: $\operatorname{ord}_W(5) = 2^{r-2}$

Pf/ We use the Binomial Theorem to show that

(1) $5^{2^{r-2}} = (1+2^2)^{2^{r-2}} \equiv 1 \pmod{2^r}$

(2) $5^{2^{r-3}} = (1+2^2)^{2^{r-3}} \not\equiv 1 \pmod{2^r}$

Once we've established (1) & (2) we are done since $\operatorname{ord}(5) \mid \operatorname{ord}(W) = 2^{r-1}$.

- **Let's show (1):** The Binomial Theorem gives $(1+2^2)^{2^{r-2}} = 1 + \sum_{k=1}^{2^{r-2}} \binom{2^{r-2}}{k} 2^{2k}$.

We claim $2^r \mid \binom{2^{r-2}}{k} 2^{2k} \quad \forall\, k \in \{1, \dots, 2^{r-2}\}$

Write $k = 2^j m$ with $0 \le j \le 2^{r-2}$, $m \in \mathbb{Z}_{\ge 1}$, $2 \nmid m$.

Then $2^{2k}\binom{2^{r-2}}{k} = 2^{2^{j+1}m} \dfrac{2^{r-2}}{2^j m} \dfrac{(2^{r-2}-1)!}{(2^j m - 1)!\,(2^{r-2}-2^j m)!} = 2^{2^{j+1}m}\, 2^{r-2-j} \dfrac{1}{m}\binom{2^{r-2}-1}{2^j m - 1}$

Now: $\binom{2^{r-2}}{k} = 2^{r-2-j}\,\dfrac{1}{m}\binom{2^{r-2}-1}{2^j m - 1} \in \mathbb{Z}$, $r-2-j \ge 0$ & $\gcd(m,2)=1$

This forces $\dfrac{1}{m}\binom{2^{r-2}-1}{2^j m - 1} \in \mathbb{Z}$

$\Rightarrow 2^{r-2-j+2^{j+1}m} \mid \binom{2^{r-2}}{k} 2^{2k}$

It's enough to check $r \le r-2-j+2^{j+1}m$, or equiv $\boxed{2 \le 2^{j+1}m - j}$.

We show: $2 \le 2^{j+1} - j \quad \forall\, j \ge 0$ by induction on j

- Base Case: $j=0$ $\quad 2 \overset{?}{\le} 2^1 - 0 = 2$ ✓
- Inductive Step: $2^{(j+1)+1} - (j+1) = 2^{j+2} - j - 1 = 2\underbrace{(2^{j+1}-j)}_{\ge 2 \text{ by (IH)}} + \underbrace{j-1}_{\ge -1} \ge 4 - 1 = 3 \ge 2$ ✓

- **Let's show (2):** We use the same strategy as with 1.

$$(1+2^2)^{2^{r-3}} = 1 + \sum_{k=1}^{2^{r-3}} \binom{2^{r-3}}{k} 2^{2k} = 1 + \binom{2^{r-3}}{1} 2^2 + \sum_{k=2}^{2^{r-3}} \binom{2^{r-3}}{k} 2^{2k}$$

We claim $2^r \mid \binom{2^{r-3}}{k} 2^{2k} \quad \forall\, k \in \{2, \dots, 2^{r-3}\}$

We write $k = 2^j m$ with $0 \le j \le 2^{r-3}$, $m \in \mathbb{Z}_{\ge 1}$, $2 \nmid m$ but $(j,m) \ne (0,1)$

Then $2^{2k}\binom{2^{r-3}}{k} = 2^{2^{j+1}m}\, 2^{r-3-j} \underbrace{\dfrac{1}{m}\binom{2^{r-3}-1}{2^j m - 1}}_{\in \mathbb{Z} \text{ because } 2 \nmid m} = 2^{2^{j+1}m - j + r - 3} \underbrace{\dfrac{1}{m}\binom{2^{r-3}-1}{2^j m - 1}}_{\in \mathbb{Z}}$

$\in \mathbb{Z}$

$\Rightarrow 2^{2^{j+1}m - j + r - 3} \mid 2^{2k}\binom{2^{r-3}}{k}$

It's enough to show $r \le 2^{j+1}m - j + r - 3$, or equivalently $3 \le 2^{j+1}m - j$ if $(j,m) \neq (0,1)$

We show: (A) $3 \le 2^{j+1} - j$ for $j \ge 1$ $(m=1)$ & (B) $3 \le 2^{j+1}3 - j$ for $j \ge 0$ $(m \ge 3)$

(A) • Base case: $j=1$ $\quad 3 = 2^2 - 1$ ✓

• Inductive step: $2^{j+2} - (j+1) = 2\underbrace{(2^{j+1} - j)}_{\ge 3 \text{ by (IH)}} + \underbrace{j-1}_{\ge -1} \ge 2 \cdot 3 - 1 = 5 \ge 3$ ✓

(B) • Base case: $j=0$ $\quad 3 \overset{?}{\le} 2^1 3 - 0 = 6$ ✓

• Inductive step: $2^{j+2}3 - (j+1) = 2\underbrace{(2^{j+1}3 - j)}_{\ge 3 \text{ by (IH)}} + \underbrace{j-1}_{\ge -1} \ge 6 - 1 = 5 \ge 3$ ✓

Conclude: $(1+2^2)^{2^{r-3}} = 1 + 2^{r-3}2^2 = 1 + 2^{r-1} \pmod{2^r}$

$\Rightarrow (1+2^2)^{2^{r-3}} \neq 1 \pmod{2^r}$, as we wanted. □

$\Rightarrow \left| W / \langle 2^{r-2} \rangle \right| = \frac{2^{r-1}}{2^{r-2}} = 2$

• If W is not cyclic, then $\exp(W) = 2^{r-2}$ and we are done by the structure Theorem of finite abelian 2-groups. The missing 2-subgroup factor will be $\mathbb{Z}/2\mathbb{Z}$ for cardinality reasons.

Claim 2: W is not cyclic.

Pf/ We argue by contradiction. If W were cyclic, then $W \simeq \mathbb{Z}/2^{r-1}\mathbb{Z}$ (with + notation), for size reasons. In particular $(\mathbb{Z}/2^{r-1}\mathbb{Z}, +)$ has a unique element of order 2, namely 2^{r-2}. We show W has 2 elements of order 2, thus producing the desired contradiction.

• One of them is $\sigma_{-1} \in W$ $\quad (x \mapsto -x \bmod 2^r)$

• The second one is $5^{2^{r-3}}$ because $\operatorname{ord}(5) = 2^{r-2}$.

Since $5^{2^{r-3}} \equiv 1 + 2^{r-1} \pmod{2^r} \neq -1 \pmod{2^r}$ because $2^r \nmid (2 + 2^{r-1})$

Indeed $2^r > 2+2^{r-1} \iff 2^{r-1} > 1+2^{r-2} \iff 2^{r-2} > 1$ This is true since $r \geq 3$

Thus, we found 2 elements of order 2 in W Contradiction!

□