

Last time: classified gps of order p^2

Sylow Thms

G a finite gp, $|G| = p^e m$ with $e \geq 1$ an int. and $p \nmid m$.

A Sylow p subgp of G is a subgp H of G with order p^e .

Thm 1 If G has size $p^e m$ with $e \geq 1$ & $\gcd(p, m) = 1$, then G contains a subgp H of order $|H| = p^e$.

Cor Suppose $p \mid |G|$. Then $\exists x \in G$ with $\text{ord}(x) = p$.

Pf: Let $H \leq G$ be a Sylow p subgp. Then $|H| = p^e$.

HW question $\Rightarrow H$ contains elt of order p .

$y \in H$ arbitrary w/ $y \neq 1$. Then $\text{ord}(y) = p^r$ for some r .

$x = y^{p^{r-1}}$ has order p .

Thm 2 G a finite gp w/ $p \mid |G|$.

a) The Sylow p subgps of G are all conjugate

b) Every p -subgp of G is contained in some Sylow p -subgp

Cor: If there is just one Sylow p subgp of G , then it must be normal

Thm 3 $|G| = p^e m$ with $\gcd(p, m) = 1$. Let s denote the number of Sylow p subgps. Then

- s divides m
- $s \equiv 1 \pmod{p}$.

Cor Suppose $|G| = pq$ with p, q distinct primes and $p > q$.

Then $G \cong C_p \rtimes C_q$.

Pf: Let H be a Sylow p subgp

Let K be a Sylow q subgp

The # of Sylow p subgps is $\equiv 1 \pmod{p}$ and it divides q .

$\Rightarrow$ # of Sylow p subgp is 1 $\Rightarrow H$ is normal.

• Now $H \cap K = \{1\}$ b/c any $e \in H$ in intersection has order dividing p and q .

• Moreover mult: $H \times K \rightarrow G$ is bijective

b/c it's injective b/c $H \cap K = \{1\}$ and both sides have size pq .

$\Rightarrow G = H \rtimes K$, $\phi: K \rightarrow \text{Aut}(H)$ (action of K on H)
by conjugation

$\cong C_p \rtimes C_q$.

What are the possible actions of C_q on C_p ?

Propⁿ $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Pf: Suppose $r \in (\mathbb{Z}/n\mathbb{Z})^\times$. Define

$$\phi_r : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

as $\phi_r(k) = r \cdot k$.

ϕ_r is a gp homom: $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$

because $\phi_r(k_1 + k_2) = r(k_1 + k_2) = rk_1 + rk_2 = \phi_r(k_1) + \phi_r(k_2)$

Also, ϕ_r is an isom: $r \in (\mathbb{Z}/n\mathbb{Z})^\times \Rightarrow \exists s \in (\mathbb{Z}/n\mathbb{Z})^\times$ with
 $rs \equiv 1 \pmod n$.

Then $\phi_s \circ \phi_r = \phi_r \circ \phi_s : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ is the identity map

Conversely, suppose $\phi \in \text{Aut}(\mathbb{Z}/n\mathbb{Z})$.

Then $\phi(1) = r$ for some $r \in \mathbb{Z}/n\mathbb{Z}$.

ϕ gp hom $\Rightarrow \phi(k) = r \cdot k \quad \forall k \in \mathbb{Z}/n\mathbb{Z}$.

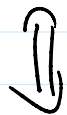
ϕ bijective $\Rightarrow \exists s \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\phi(s) = 1$.

But, $\phi(s) = rs \equiv 1 \pmod n$
 $\Rightarrow r \in (\mathbb{Z}/n\mathbb{Z})^\times$.

$$\Rightarrow r \in (\mathbb{Z}/n\mathbb{Z})^\times$$

Finally, the bijection $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is a group hom.

$C_m \leq C_n$ by gp homom's



$$\phi: C_m \rightarrow \text{Aut}(C_n) = (\mathbb{Z}/n\mathbb{Z})^\times$$

$$\{1, y, y^2, \dots, y^{m-1}\}$$

Cor There is a bijective correspondence between

$$\left\{ \begin{array}{l} \text{actions of} \\ C_m \text{ on } C_n \\ \text{by gp homom's} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{elts } r \in (\mathbb{Z}/n\mathbb{Z})^\times \\ \text{with } r^m \equiv 1 \pmod{n} \end{array} \right\}$$

Pf: If $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $r^m \equiv 1 \pmod{n}$, then

$$C_m \leq C_n \text{ via } \underbrace{y^j}_{\in C_m} \star \underbrace{(k)}_{\in \mathbb{Z}/n\mathbb{Z}} = r^j k.$$

Ex. $C_7 \not\leq C_3$ with $\phi: C_3 = \{1, y, y^2\} \rightarrow \text{Aut}(\mathbb{Z}/7\mathbb{Z}) = (\mathbb{Z}/7\mathbb{Z})^\times$

$$\text{as } \phi(y) = 2$$

$$\cdot \text{ Also: } \phi(y) = 4$$

Pr: $\phi(y) = 4$

- Cor
- Every gp of order 15 is cyclic
 - There are two iso classes of gps of order 6, namely S_3 and $C_3 \times C_2 \cong C_6$
 - There are two iso classes of gps of order 21, namely $C_7 \times C_3 \cong C_{21}$ and $C_7 \rtimes_{\phi} C_3$ with ϕ as in the example above.

Pf: a) G a gp of order 15.
 $G \cong C_5 \rtimes_{\phi} C_3$

However: $\underbrace{\phi: C_3 \rightarrow \text{Aut}(C_5)}_{\text{size 3}} = \underbrace{(\mathbb{Z}/5\mathbb{Z})^{\times}}_{\text{has size 4}}$

must be trivial

$$\Rightarrow G \cong C_5 \times C_3 \cong C_{15}$$

b) G a gp of order 6
 $G \cong C_3 \rtimes_{\phi} C_2$

$$\phi: C_2 \rightarrow \text{Aut}(C_3) = \underbrace{(\mathbb{Z}/3\mathbb{Z})^{\times}}_{\text{cyclic of order 2}}$$

- If ϕ is trivial, $G \cong C_3 \times C_2$
- If ϕ is nontrivial $G \cong C_3 \rtimes_{\phi} C_2 \Rightarrow G \cong S_3$.

Recall: $D_n \cong S_n$, also $D_n \cong C_n \rtimes C_2$

Recall! $D_3 \cong S_3$, also $D_n \cong C_n \rtimes C_2$

c) G has order 21. Then $G \cong C_7 \rtimes C_3$

$$\phi: C_3 = \{1, \gamma, \gamma^2\} \rightarrow (\mathbb{Z}/7\mathbb{Z})^\times$$

Possible ϕ 's $\phi(\gamma) \equiv 1$ i.e. ϕ trivial

$$\phi(\gamma) \equiv 2$$

$$\phi(\gamma) \equiv 4$$

First case, ϕ trivial, gives $G \cong C_7 \times C_3 \cong C_{21}$

Claim: Find two ϕ 's give same gpf

Pf: Define $\gamma' = \gamma^2$ in C_3 .

$$\text{Then } C_3 = \{1, \gamma, \gamma^2\} = \{1, \gamma', (\gamma')^2\}.$$

$$\text{If } \phi(\gamma) = 4 \text{ then } \phi(\gamma') = \phi(\gamma^2) = 2$$

$$\Rightarrow C_7 \rtimes_{\phi} \{1, \gamma, \gamma^2\} \cong C_7 \rtimes_{\phi'} \{1, \gamma', (\gamma')^2\}$$

$\text{w/ } \phi(\gamma) = 4 \qquad \phi'(\gamma') = 2$

□