Last time: let p be prime and consider a group G of order

$$p^n \cdot r \quad , \quad n \geq 0, \ (p,r)=1$$

Sylow theorem 1: G has a Sylow p-subgroup, i.e.

$$P \leq G \quad \text{s.t.} \quad |P| = p^n$$

Sylow theorem 2: all Sylow p-subgroups of G are conjugate

$\Downarrow$

$\exists$ unique Sylow p-subgroup if and only if it's normal

Sylow theorem 3: let $n_p = \#$ Sylow p-subgroups of G

- $n_p = [G : N_G(P)]$ for any Sylow p-subgroup P
- $n_p \mid r$
- $n_p \equiv 1 \mod p$

Today: use this to classify groups of given order

(p, q will always denote distinct primes in what follows)

THM 1: any group of order p is $\cong \mathbb{Z}/p\mathbb{Z}$

THM 2: suppose $p \nmid q-1$ and $q \nmid p-1$

any group G of order pq is $\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$

↓ true whenever $(p,q)=1$

(what about S_3, which has order $6=2\cdot 3$; however, $2 \mid 3-1$)

Proof: Sylow 3: $n_p \mid q$ and $n_p \equiv 1 \bmod p$ $\Rightarrow$ $n_p = 1$

$n_q \mid p$ $\quad$ $n_q \equiv 1 \bmod q$ $\quad$ $n_q = 1$

Sylow 2: $\exists$ $P \cong \mathbb{Z}/p\mathbb{Z}$ normal Sylow p-subgroup

$Q \cong \mathbb{Z}/q\mathbb{Z}$ normal Sylow q-subgroup

Claim: $P \cap Q = \{e\}$, because any element $g \neq e$ in $P \cap Q$ would have order $\neq 1$ that divides p and q

⇓ injectivity

Claim: $PQ \xleftarrow{\sim} P \times Q$; injective implies $PQ = G$ because $|P \times Q| = pq = |G|$

PQ ← subgroup; $gh \leftarrow (g, h)$

⇓

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong PQ = G$ □

THM 3: any group G of order p^2 is

$$\cong \mathbb{Z}/p^2\mathbb{Z} \quad \text{or} \quad \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Proof: last time $|Z(G)| > 1$; two options

- $|Z(G)| = p^2 \Rightarrow G = Z(G)$ abelian $\Rightarrow G \cong \begin{matrix} \mathbb{Z}/p^2\mathbb{Z} \\ \text{or} \\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \end{matrix}$

- $|Z(G)| = p$; pick $g \in G \setminus Z(G)$

$$Z(G) \leq C_G(g) \leq G$$

cannot be an equality because $g \in C_G(g) \setminus Z(G)$

cannot be an equality because $C_G(g) = G$ means $g \in Z(G)$

Lagrange prohibits subgroups sandwiched between order p and order p^2

□

THM 4: suppose $p \nmid q-1$ and $q \nmid p^2-1$

any group G of order p^2q is $\cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ or

$$\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Proof: like in Thm 2, assumptions ensure $n_p = n_q = 1$

$\overset{\text{Thm3}}{\Rightarrow}$ P, Q normal Sylow p,q-subgroups $\overset{\text{Thm 1}}{\Rightarrow}$

$\mathbb{Z}/p^2\mathbb{Z}$ or
$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

$\cong \mathbb{Z}/q\mathbb{Z}$

we have an injective homomorphism $P \times Q \to PQ$.
because $P \cap Q = \{e\}$, in turn because $(|P|, |Q|) = 1$

Note: $p=2$ and $q=3$, Theorem does not apply.

THM 5: any group G of order 12 is $\cong$ to one of

- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
- A_4
- D_{12}
- the dicyclic group that we will define in proof.

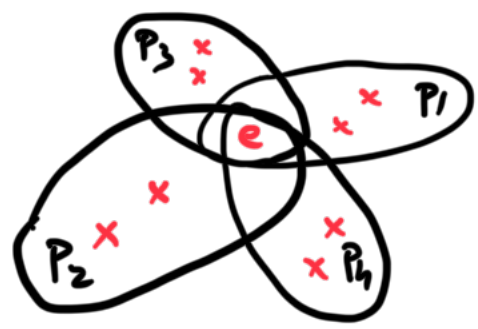
Proof: $12 = 2^2 \times 3$; Sylow 3: $n_3 \equiv 1 \bmod 3$, $n_3 \mid 4$ $\Rightarrow n_3 \in \{1, 4\}$

Option 1: $n_3 = 4$, $\exists\ P_1, P_2, P_3, P_4 \cong \mathbb{Z}/3\mathbb{Z}$

Claim $P_i \cap P_j = \{e\}$ $\forall\ i \neq j$, because if $\exists$
$e \neq g \in P_i \cap P_j$, then $g^2 \in P_i \cap P_j$

$\exists$ at least $2 \times 4 = 8$
elements of order 3 in G

and $P_i = \{e, g, g^{-1}\} = P_j$



Sylow 2: $G \curvearrowright \{P_1, P_2, P_3, P_4\}$ by conjugation

$$g \cdot P_i = g P_i g^{-1}$$

$\Downarrow$

$\exists$ of a homomorphism $G \xrightarrow{f} S_4$

Claim: f is injective because if $f(g) =$ identity

then $g P_i g^{-1} = P_i$, $\forall i$

then $g \in N_G(P_i) = P_i$ $\Rightarrow$ $4 = n_3 = [G : N_G(P_i)] = [G : P_i]$

$\Downarrow$

$g = e$ since $P_i \cap P_j = \{e\}$

Claim: $\mathrm{Im}\, f = A_4 \Longrightarrow G \cong A_4$

All elements of order 3 in S_4 lie in A_4

$\mathrm{Im}\, f$ has at least 8 elements of order 3,

so $(\mathrm{Im}\, f) \cap A_4$ has order ≥ 8

has order $| 12 = |A_4|$

$\Downarrow$

$\mathrm{Im}\, f = A_4$ because $|\mathrm{Im}\, f| = |A_4| = 12$

Option 2: $n_3 = 1 \Rightarrow \exists$ normal Sylow 3-subgroup $P \cong \mathbb{Z}/3\mathbb{Z}$

$$1 \longrightarrow \mathbb{Z}/3\mathbb{Z} \cong P \longrightarrow G \xrightarrow{\pi} G/P \longrightarrow 1$$

$(\pi|_Q)^{-1}$

G/P: order 4, so $\cong \mathbb{Z}/4\mathbb{Z}$ or $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Let Q (which has order 4) be a Sylow 2 subgroup

$\pi|_Q$ is injective because $P \cap Q = \{e\}$ (order 3 ∩ order 4)

$\pi|_Q$ is an isomorphism because $|Q| = |G/P| = 4$

$(\pi|_Q)^{-1}$ is a section $\Rightarrow G \cong P \rtimes G/P$

- How many semidirect products of $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are there?

  - $\mathbb{Z}/4\mathbb{Z} \overset{\text{trivially}}{\curvearrowright} \mathbb{Z}/3\mathbb{Z} \Rightarrow G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
  - $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \overset{\text{trivially}}{\curvearrowright} \mathbb{Z}/3\mathbb{Z} \Rightarrow G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

(however, $\mathbb{Z}/3\mathbb{Z}$ only has two automorphisms: Id and $\chi(k) = -k$)

$\mathbb{Z}/4\mathbb{Z} \hookrightarrow \mathbb{Z}/3\mathbb{Z}$

$k \bmod 4 \rightsquigarrow \chi^k$

$\Rightarrow$ $G =:$ dicyclic group

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathbb{Z}/3\mathbb{Z}$

$(a,b) \rightsquigarrow \chi^a \sigma \chi^b \sigma \chi^{a+b}$

$\Rightarrow$ $G \cong D_{12}$.

↳ prove it yourselves or ask on forum

THM 6: any simple group G of order 60 is $\cong A_5$.

(icosahedral group I of rotations of $\mathbb{R}^3$ which preserve a regular icosahedron is simple of order 60 $\Rightarrow I \cong A_5$

class equation of I is $60 = 1 + 12 + 12 + 15 + 20$

any normal subgroup of I would be a union of conjugacy classes; but there is no such proper union which contains e and its cardinality divides 60)

Proof: Option 1: $\exists\ H < G$ of index $n \in \{2,3,4,5\}$

exclusive or

$\forall\ H < G$ of index ≥ 6

Option 2: $\forall H < G$ has index ≥ 6

Option 1: $G \curvearrowright \{\text{left } H\text{-cosets}\}$

$g \cdot hH = ghH$

$\downarrow$

$f : G \longrightarrow S_n$ is not trivial, because it's transitive

hence $\ker f = \{e\}$ because G is simple

Hence f is injective $\Rightarrow$ $n = 5$ and $G \hookrightarrow S_5$

(order 60 under G, order 120 under S_5)

$[S_5 : G] = 2$; But any subgroup of index 2 (in any group) is normal

$\forall x \in S_5 \setminus G \Rightarrow S_5 = G \sqcup xG = G \sqcup Gx$

$\Downarrow$

$xG = Gx$

$\Downarrow$

G normal

Hence $1 \triangleleft G \triangleleft S_5$ and $1 \triangleleft A_5 \triangleleft S_5$ are both composition series

$\Downarrow$

J-H theorem: $\{G, \mathbb{Z}/2\mathbb{Z}\} \cong \{A_5, \mathbb{Z}/2\mathbb{Z}\}$

$\Downarrow$

$G \cong A_5$

$\forall H < G$ has index ≥ 6

Option 2: any proper subgroup of G has order ≤ 10.

$60 = 2^2 \cdot 3 \cdot 5$; Sylow 3 : $n_2 \equiv 1 \bmod 2$, $n_2 \mid 15$ $\Rightarrow n_2 = 15$

$n_2 = [G : \text{normalizer}] \geq 6$

Let $P_1, \ldots, P_{15}$ be the Sylow 2-subgroups; they have order 4, so must be abelian

Case 1: $\exists\ i \neq j$ s.t. $|P_i \cap P_j| \geq 2$

(since $P_i \cap P_j < P_i$, must have $=$)

$\Rightarrow |P_i \cup P_j| = 6$

pick $e \neq g \in P_i \cap P_j$

$\Rightarrow$

$6 \leq |C_G(g)|$

$4 \mid |C_G(g)|$

$10 \geq |C_G(g)|$

$|C_G(g)| = 8$

impossible since $|C_G(g)| \nmid 60$

Case 2: $\forall\ i \neq j$, $P_i \cap P_j = \{e\}$.

any element in $P_1 \cup \ldots \cup P_{15}$ has order 1, 2 or 4

$\exists$ 46 such elements, including e

Also look at the Sylow 5-subgroups

Sylow 3 : $n_5 \equiv 1 \bmod 5$, $n_5 \mid 12$ $\Rightarrow n_5 = 6$

$n_5 = [G : \text{normalizer}] \geq 6$

$Q_1, \ldots, Q_6 \cong \mathbb{Z}/5\mathbb{Z}$

Claim: $\forall i \neq j \quad Q_i \cap Q_j = \{e\}$; indeed, if $\exists\, e \neq g \in Q_i \cap Q_j$,

then $g^2, g^3, g^4 \in Q_i \cap Q_j$ and so

$$Q_i = \{e, g, g^2, g^3, g^4\} = Q_j$$

↳ must be distinct, as g has order 5

any element in $Q_1 \cup \dots \cup Q_6$ has order 1 or 5

$\exists$ 25 such elements, including e

$$60 < 46 + 25 - 1$$

(46: # elements of order 1, 2, 4; 25: # elements of order 1, 5; −1: # elements of order 1)

Impossible.