Sylow Theory

By Lagrange, if $H \leq G$ then $|H|$ divides $|G|$.

Fundamental question : Is the opposite true? If m divides $|G|$, does G have a subgroup of order m?

If G is Abelian, then yes!
If G is non-Abelian, the situation is far more complicated...

Ex: S_3 has subgroups of order $1, 2, 3, 6$.

Ex: A subgroup of index 2 is normal, since A_n is simple, A_n has no subgroup of order $n!/4$ for $n \geq 5$.

Can we say any general results?

Cauchy's Theorem: If p is a prime dividing $|G|$, then G has a subgroup H of order p.

Proof:
Consider $X = \{(g_0, g_1, \dots, g_{p-1}) \mid g_k \in G \ \forall\, 0 \leq k < p \text{ and } g_0 g_1 g_2 \cdots g_{p-1} = e\}$.
and consider the equivalence relation

$$(g_0, \dots, g_{p-1}) \sim (h_0, \dots, h_{p-1}) \Leftrightarrow \exists\, r \text{ with } h_k = g_{(k+r) \bmod p}.$$

Note that $|X| = |G|^{p-1}$ and the size of each equivalence class

$$[(g_0, \dots, g_{p-1})] = \{(h_0, h_1, \dots, h_{p-1}) \in X \mid (g_0, \dots, g_{p-1}) \sim (h_0, \dots, h_{p-1})\}$$

is either 1 or p.

Let $(g_{1,0}, \dots, g_{1,p-1}), (g_{2,0}, \dots, g_{2,p-1}), \dots, (g_{r,0}, g_{r,1}, \dots, g_{r,p-1})$ be representatives of distinct equivalence classes of order p and

$(h_{1,0},\dots,h_{1,p-1}),\ (h_{2,0},\dots,h_{2,p-1}),\dots,(h_{s,0},h_{s,1},\dots,h_{s,p-1})$

be representatives of distinct equivalence classes of order 1.

Then

$|G|^{p-1} = |X| = pr + 1s$

Reducing this mod p, we see $s \equiv 0 \mod p$.

Since $[(e,e,\dots,e)]$ has order 1, $s>0$.

Thus $s \geq 2$ and $\exists$ $a \in G$ with $a^p = e$.

It follows $\langle a \rangle \leq G$ has order p $\square$

Simpler question: If p^n divides $|G|$ for p prime, does G have a subgroup of order p^n?

Def: A group G with the property that for some prime p

$\forall\ a \in G\ \exists\ j>0$ with $\operatorname{ord}(a) = p^j$

is called a p-group.

This turns out to be the same as a condition on the order of G.

Theorem: If G is a finite p-group, then $|G| = p^n$ for some $n \geq 0$.

Proof: If $q \neq p$ is a prime with $q \mid |G|$, then by Cauchy's Theorem, G has an element of order q.

$\Rightarrow \Leftarrow$.

$\square$

It turns out that we can generalize Cauchy's Theorem:

First Sylow Theorem: Suppose $|G| = p^n m$ with $\gcd(m,p)=1$.

- G has a subgroup of order p^j $\forall\ 1 \leq j \leq n$.
- every subgroup $H < G$ of order p^j is a normal subgroup of a subgroup of order p^{j+1} for $1 \leq j < n$.

Idea of proof:

By Cauchy's Theorem, can find $H_1 \leq G$ with $|H| = p$.
Now we grow it!

$$N(H_1) = \{ x \in G \mid xH_1x^{-1} = H_1 \}$$

is a subgroup of G containing H_1 and satisfying

- $H \trianglelefteq N(H_1)$
- $[N(H_1) : H_1]$ is divisible by p

So $N(H_1)/H_1$ has a subgroup $\overline{H}_1$ of order p.
The preimage of $\overline{H}_1$ under the quotient map $q_1 : N(H_1) \to N(H_1)/H_1$

$$H_2 = q_1^{-1}(\overline{H}_1)$$

is a group of order p^2. Then continue this process!

The biggest possible p-subgroups play a special role

Def: Let $G = p^n m$ with $\gcd(p, m) = 1$ a subgroup of order p^n is called a Sylow p-subgroup.

Second Sylow Theorem: If P_1 and P_2 are Sylow p-subgroups of G then $\exists$ $a \in G$ with $P_2 = aP_1a^{-1}$.

Proof: Let P_1, P_2 be Sylow p-subgroups of G and define $\sim$ on G/P_1 by

$$xP_1 \sim yP_1 \iff \exists\, z \in P_2 \text{ with } yP_1 = zxP_1.$$

Then the equivalence class

$$[xP_1] = \{ yP_1 \mid xP_1 \sim yP_1 \} = \{ zxP_1 \mid z \in P_2 \}$$

has order dividing $|P_1| = p^n$. Let $x_1P, \dots, x_rP$ be reps. of distinct equiv. classes.

$$|G/P_1| = |[x_1P_1]| + \dots + |[x_rP_1]|$$

and reducing mod p, we see at least

one x_j satisfies $[x_jP_1] = \{x_jP_1\}$.

This means $zx_jP_1 = x_jP_1 \;\; \forall z \in P_2$ so
$x_j^{-1}zx_j \in P_1 \;\; \forall z \in P_2$ so
$x_j^{-1}P_2x_j \subseteq P_1$

Thus $x_j^{-1}P_2x_j = P_1$

$\square$

Consequently, if G has only one Sylow p-subgroup then that subgroup is normal.

Lastly, we have the Third Sylow Theorem:

Third Sylow Theorem: If $n_p = \#$ Sylow p-subgroup of G then $n_p \equiv 1 \mod p$ and $n_p \mid |G|$.

Proof:

Similar flavor to the above

$\square$

Some cool applications:

Lemma: If $P \trianglelefteq G$ and $Q \trianglelefteq G$ and $P \cap Q = \{e\}$ then $PQ \cong P \times Q$.

Proof:

S'pose $P \trianglelefteq G$ and $Q \trianglelefteq G$ and $P \cap Q = \{e\}$.

Then for $x \in P$, $y \in Q$

$$\left.\begin{array}{l} x^{-1}yx \in Q \\ y\,x\,y^{-1} \in P \end{array}\right\}$$

$$Q \ni (x^{-1}yx)y^{-1} = x^{-1}yxy^{-1} = x^{-1}(yxy^{-1}) \in P$$

Thus $x^{-1}yxy^{-1} \in P \cap Q = \{e\}$ so $x^{-1}yxy^{-1} = e$.

Hence $yx = xy \ \forall \ x \in P, y \in Q$.

The map $\psi : P \times Q \to PQ$
$(a, b) \mapsto ab$ is surjective

and

$$\psi((x_1, y_1)(x_2, y_2)) = \psi(x_1x_2, y_1y_2)$$
$$= x_1x_2y_1y_2$$
$$= x_1y_1x_2y_2 \quad = \psi(x_1, y_1)\psi(x_2, y_2)$$

so it's a homomorphism!

$\ker(\psi) = \{(x,y) \in P \times Q \mid xy = e\}$
but if $x \in P, y \in Q$ and $xy = e$, then $y = x^{-1} \in P$
so $y \in P \cap Q \Rightarrow y = x = e$. Thus $\ker(\psi) = \{(e,e)\}$
and ψ is an isomorphism

$\square$

Ex: If $|G| = 99$ then $G \cong \mathbb{Z}_{99}$ or $G \cong \mathbb{Z}_3 \times \mathbb{Z}_{33}$

Proof:
Suffices to show G is Abelian!

$n_{11} = 1$ and $n_3 = 1$. Choose $P \lhd G$ and $Q \lhd G$
with $|P| = 9$, $|Q| = 11$. Then $P \cap Q = \{e\}$ so
$|PQ| = |P| \cdot |Q| = 9 \cdot 11 = 99 \quad \therefore PQ = G$.

By prev. Lemma $G = PQ \cong P \times Q$
P order $9 \Rightarrow P$ Abelian
Q order $11 \Rightarrow Q$ cyclic!

$\square$

Ex: If $|G| = 1645$ then $G \cong \mathbb{Z}_{1645}$.

Proof: $1645 = 5 \cdot 7 \cdot 47$

$n_5 = 1, \quad n_7 = 1, \quad n_{47} = 1$

$\Rightarrow \quad P \trianglelefteq G, \quad Q \trianglelefteq G, \quad R \trianglelefteq G$

with $|P| = 5, \quad |Q| = 7, \quad |R| = 47$

$PQ \trianglelefteq G$ and $PQ \cap R = \{e\}$ so

$G = (PQ)R \cong PQ \times R$

$P \trianglelefteq PQ$ and $Q \trianglelefteq PQ$ and $P \cap Q = \{e\}$ so

$PQ \cong P \times Q$

Thus $G \cong PQ \times R \cong P \times Q \times R \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{47}$

$\cong \mathbb{Z}_{1645}$.

$\square$