Fri, Oct 24, 2014

Last time: stated 2nd Sylow Thm

proved 1st Sylow Thm

Rmk: We argued

$$\binom{p^e m}{p^e} = \frac{p^e m(p^e m-1)\cdots(p^e m-p^e+1)}{p^e(p^e-1)\cdots(1)}$$

isn't divisible by p. This came down to

$$p^i \mid p^e m - k \implies p^i \mid p^e - k.$$

Why is $i<e$? Since otherwise,

$$k = p^{e+a}\ell \Rightarrow p^e - k = p^e(1-p^a\ell) \leq 0 \text{ if } a \geq 0.$$

More concretely, by defn of binomial coefficient, k has to run from 0 to p^e-1, so k itself must be less than p^e.

So the First Sylow Thm tells us that Sylow p-subgroups exist.

given group G s.t $|G| = p^e m$, $p \nmid m$, $H \subset G$ is a Sylow p-subgroup if $|H| = p^e$.

Thm (Second Sylow Thm)
Fix a finite group G and a prime p dividing $|G|$.

(a) Any two Sylow p-subgroups are conjugate.

(b) For any subgroup $H \subset G$ which is a p-group, $\exists$ a Sylow p-subgroup containing H.

Note that if $\exists$ only one Sylow p-subgroup, it must be normal. Why?

$\forall g \in G$,

$$C_g : G \longrightarrow G$$
$$x \longmapsto gxg^{-1}$$

is a group isomorphism. So it sends subgroups of order k to subgroups of order k. If $\exists$ only one such subgroup H, C_g must take H to H $\forall g \in G$. i.e.,

$$gHg^{-1} = H \quad \forall g \in G.$$

So H is normal.

The Second Sylow Thm tells us the converse is true.

Cor If a Sylow p-subgroup H is a normal subgroup of G, H is the only Sylow p-subgroup of G.

Before we get to the Third Sylow Thm, I want to quickly run a useful fact by you.

We know that semidirect products are recognized as split short exact sequences:

$$H \cong L \rtimes R \iff \exists \text{ split SES } 1 \to L \to H \underset{j}{\overset{i}{\rightleftarrows}} R \to 1$$

So when can we recognize <u>direct</u> products?

<u>Prop'n</u> TFAE (The following are equivalent):

(1) $H \cong L \times R$

(2) $H \cong L \rtimes_\phi R$ where

$\phi: R \to Aut(L)$

is trivial

(3) $\exists$ split SES

$L \to H \underset{j}{\overset{i}{\rightleftarrows}} R$

s.t. $j(R) \trianglelefteq H$

Pf (1) → (3) ⇒ (2) ⇒ (1)

(1) → (3): If $H \cong L \times R$, we have the inclusion

$$i: L \longrightarrow H$$
$$l \longmapsto (l, 1_R)$$

and the projection

$$p: H \longrightarrow R$$
$$(l, r) \longmapsto r$$

both of which you've proven are homomorphisms. (Hmwk).

Then we have a splitting

$$L \xrightarrow{i} H \underset{j}{\overset{p}{\rightleftarrows}} R$$

where $j: R \longrightarrow H$ is
$r \longmapsto (1_L, r)$

the other "inclusion" homomorphism.

Moreow. $j(R) \trianglelefteq H$. Why?

$$(l', r')(1_L, r)(l', r')^{-1} = (l', r')(1_L, r)(l'^{-1}, r'^{-1})$$
$$= (l' 1_L l'^{-1}, r' r r'^{-1})$$
$$= (1_L, r' r r'^{-1}) \in j(R).$$

(3) $\Longrightarrow$ (2)

Let $r \in j(R)$, $\ell \in i(L)$.

Then

$$r\ell r^{-1}\ell^{-1} = \overbrace{\ell' \ell^{-1}}^{\text{since } i(L) \text{ is normal}}$$

$$\in i(L)$$

and

$$r\ell r^{-1}\ell^{-1} = \overbrace{r\, r'}^{\in j(R) \text{ since } j(R) \text{ is normal}}$$

$$\in j(R)$$

So $r\ell r^{-1}\ell^{-1} \in j(R) \cap i(L)$

But $j(R) \cap i(L) = \{1_H\}$ since

j is a splitting.

$$\Rightarrow r\ell r^{-1}\ell^{-1} = 1_H \quad \forall\, \ell, r$$

$$\Rightarrow r\ell r^{-1} = \ell \quad \forall\, \ell, r$$

$$\Rightarrow \phi : R \longrightarrow Aut(L)$$

$$\text{is} \quad r \longmapsto id_L \quad \forall\, r \in R.$$

(2) $\Rightarrow$ (1)

If $\phi(r) = id_L \quad \forall\, r,$

then

$$(\ell_1, r_1)\cdot(\ell_2, r_2) = (\ell_1 \cdot \phi_{r_1}(\ell_2), r_1 r_2)$$

$$= (\ell_1 \ell_2, r_1 r_2)$$

which is the definition of the multiplication on $L \times R$. //

Now we'll state the Third Sylow Thm, which will really help us determine the structures of groups.

Thm (Third Sylow Thm) Let G be a finite group, and p a prime dividing $|G|$. We let $Syl_p(G)$ denote the set of Sylow p-subgroups of G. Then

(1) $|Syl_p(G)|$ divides m

(2) $|Syl_p(G)| \equiv 1 \pmod p$.

Rmk So it relates $|Syl_p(G)|$ to both m and to p.

G acts on $Syl_p(G)$ by conjugation, and 2nd Sylow Thm says this action has a single orbit.

i.e., $|Syl_p(G)| = |G| /$ Stabilizer. G_H for some Sylow p-subgp H.

But $H \subset G_H$, so $|G_H| = p^e \cdot m'$

$$|Syl_p(G)| = p^e m / p^e \cdot m' = m/m' .$$

We'll show that $\forall\ H \in Syl_p(G)$, H is the only fixed pt for conjugation action of H on $Syl_p(G)$. So

$$|Syl_p(G)| = 1 + \sum \Theta$$

$\uparrow$ all divisible by p.

Here's an example application:

Prop If $|G| = 15$, G is cyclic.

Pf Strategy: Determine $Syl_5(G)$, $Syl_3(G)$.

By Third Sylow Thm

(a) $|Syl_5(G)|$ divides 3.

(b) $|Syl_5(G)| \equiv 1 \mod 5$.

(a) $\Rightarrow |Syl_5(G)| = 1$ or 3

(b) $\Rightarrow |Syl_5(G)| = 5$.

$\Rightarrow \exists!$ subgp $H_5 \leq G$ of ordr 5;
H_5 is hence normal.

Likewise,

(c) $|Syl_3(G)|$ divides 5

(d) $|Syl_3(G)| \equiv 1 \mod 3$

$\Rightarrow |Syl_3(G)| = 1$.

$\Rightarrow \exists!$ subgrp $H_3 \leq G$ of ordr 3.
H_3 normal.

Since $\gcd(|H_3|, |H_5|) = \gcd(3,5) = 1$,
$H_3 \cap H_5 = \{1_G\}$.

$\Rightarrow 1 \to H_3 \to G \xrightarrow{j} H_5 \to 1$.

For $p=5$, $|G| = p^e m$
$= 5^1 \cdot 3$.

Since $H_3, H_5 \trianglelefteq G$, $G \cong H_3 \times H_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
by hmwk $\cong \mathbb{Z}/15\mathbb{Z}$

Prop Let $|G| = p \cdot P$
where $p \neq P$ are primes.
Then, if P is the larger prime,

$$G \cong \mathbb{Z}/P\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

Pf By Third Sylow Thm,

(a) $|Syl_P(G)|$ divides p

(b) $|Syl_P(G)| \equiv 1 \bmod P$.

(a) $\Rightarrow$ $|Syl_P(G)| = 1$ or $p < P$.

(b) $\Rightarrow$ $|Syl_P(G)| = 1$ since the only number less than P equal to $1 \bmod P$ is 1.

$\Rightarrow$ $\exists!$ $H_P \subset G$ of order P.

$\Rightarrow$ $H_P \triangleleft G$.

So consider SES

$$1 \to H_P \longrightarrow G \longrightarrow G/H_P \to 1.$$

$|G/H_P| = p$, so it is $\cong$ to $\mathbb{Z}/p\mathbb{Z}$.

$|H_P| = P$, so $\cong$ to $\mathbb{Z}/P\mathbb{Z}$.

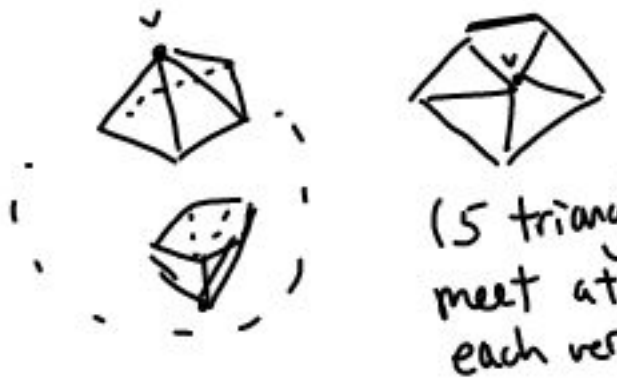
So we have SES

$$1 \to \mathbb{Z}/P\mathbb{Z} \to G \to \mathbb{Z}/p\mathbb{Z} \to 1.$$

By 1st Sylow, splitting j exists. (Since p, P are relatively prime).

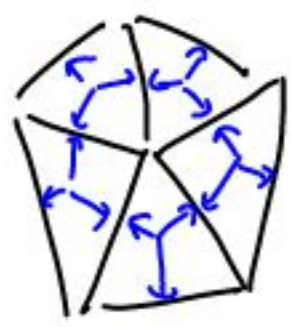
Interlude:

An icosahedron is a (the) regular polyhedron with twenty faces.



(5 triangles meet at each vertex)

If you draw three arrows on every face — every arrow pointing from the center of the face to an edge — we get



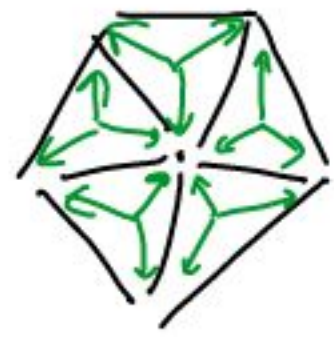
$$\#\text{ arrows} = 3 \cdot F \quad \leftarrow \#\text{ of Faces}$$

$$= 60$$

OTOH, every edge has two arrows pointing at it, so

$$\#\text{ arrows} = 2 \cdot E \quad \leftarrow \#\text{ of edges.}$$

Finally, if you draw an arrow from the center of every face to its vertices, we get



$$\#\text{ arrows} = 3 \cdot F$$

$$\#\text{ arrows} = 5 \cdot V \quad \leftarrow \#\text{ of vertices.}$$

so $V = 12$. Note $V - E + F = 2$.

($V - E + F = 2$ for any polyhedron!)