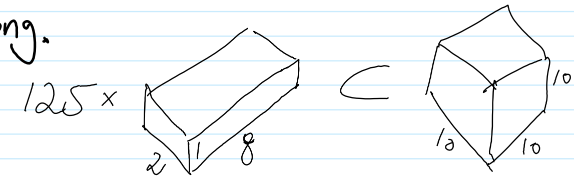
14-1100 Sep 29, hours 10-11: The Sylow theorems

September-27-14 1:18 PM

class photo on web!

Riddle Along.



Today's Menu. Sylow 1 2 3, some classification.

Reminders.

$$G \circlearrowright X \Rightarrow |X| = \sum_i \frac{|G|}{|\mathrm{Stab}_X(x_i)|}$$

$$|G| = |Z(G)| + \sum_i (G : C_G(y_i))$$

G a p-group $\Rightarrow Z(G)$ non-trivial

THE SYLOW THEOREMS. Lovely notation: $p^\alpha \| |G|$

$|G| = p^\alpha m$, p prime, $p \nmid m$; $\mathrm{Syl}_p(G) := \{P < G : |P| = p^\alpha\}$ are "Sylow p-subgroups of G". A "p-subgroup" in general, is any subgroup of G of order a power of p.

Sylow 1 $\mathrm{Syl}_p(G) \neq \emptyset$.

Proof. By induction on $|G|$, if G has a normal subgroup of order p (or p^β) or if G has a subgroup of order divisible by p^α, we are done. The existance of one of the said types follows from the class equation:

$$|G| = |Z(G)| + \sum_i (G : C_G(y_i))$$

Either both are divisible by p, or neither. Do 2^{nd} case first

$$|G| = |Z(G)| + \sum_i (G : C_G(y_i))$$ or [illegible]. Do 2^{nd} case first.

Where $\{y_i\}$ are representatives from the non-central conjugacy classes of G. $\square$

Theorem. If G is a finite Abelian group of order divisible by a prime p, then G contains an element of order p. "Cauchy's Thm" D&F pp 102

Proof. Enough to find an element of order divisible by p; if z is of order $p \cdot n$, z^n would be of order p. Pick $x \in G$, $x \neq 1$. If $p \mid |x|$, we're done. Otherwise $p \mid |G/\langle x\rangle|$, so by induction, $\exists\, y \in G$ s.t. $|\bar{y}| = p$ in $G/\langle x\rangle$. Now use the following claim. $\square$

claim. if $\phi: G \to H$ is a morphism & $y \in G$, then $|\phi(y)| \mid |y|$.

Proof. If $|\phi(y)| = n$, $|y| = m$, $m = nq + r$, then

$$e = \phi(y^m) = \phi(y^{nq})\phi(y^r) = ((\phi(y))^n)^q \phi(y)^r = \phi(y)^r$$

So $r = 0$.

Stronger Sylow 1. If $p^\beta \mid |G|$, then G has a subgroup of order p^β.

Proof. Let $X = \{S \subseteq G : |S| = p^\beta\}$, and write
subset

$|G| = p^{\alpha+\beta} m$ w/ maximal α. By counting & binomial nonsense, $p^\alpha \mid |X|$ yet $p^{\alpha+1} \nmid |X|$.

G acts on X by translations, so there must be $S_0 \in X$ s.t. $p^{\alpha+1} \nmid |G \cdot S_0|$, hence $p^\beta \mid |H = \mathrm{stab}_G(S_0)|$. Yet if $x \in S_0$ then $g \mapsto gx$ is an injection $H \to S_0$, so $|H| \leq |S_0| = p^\beta$, so $|H| = p^\beta$.

Theorem. 1. Sylow p-groups always exist; $\mathrm{Syl}_p(G) \neq \emptyset$.
2. Every p-group is contained in a Sylow-p group.
3. All Sylow-p subgroups of G are conjugate, and $n_p(G) := |\mathrm{Syl}_p(G)| = 1 \bmod p$ & $n_p(G) \mid |G|$

Groups of order 15.

P_5 is normal in G, P_3 is normal in G. Any $y \in P_3$ commutes with P_5 [otherwise, $|y| \mid |\mathrm{Aut}\, P_5| = 4$],

Preliminary Lemma. A group of order p is $\mathbb{Z}/p$.

Aside. $n_p \mid pq \Rightarrow n_p \mid q$, (or $n_p = 1$)
$n_p = 1 \bmod p \Rightarrow q = 1 \bmod p$
$= p \mid q-1$

(**Aside.** $\mathrm{Aut}(\mathbb{Z}/p) = (\mathbb{Z}/p)^*$ so $|\mathrm{Aut}(\mathbb{Z}/p)| = p-1$)

So $G = x^i y^j = y^j x^i$ for generators $x \in P_5$, $y \in P_3$.

Aside. If $G = G_1 \cdot G_2$, $G_1 \cap G_2 = \{e\}$, $[G_1, G_2] = \{e\}$, then $G = G_1 \times G_2$

Aside. $\mathbb{Z}/p \times \mathbb{Z}/q = \mathbb{Z}_{pq}$

So $G_{15} = \mathbb{Z}/15$.

In fact, if $(a,b) = 1$, then $\mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/ab$

Proof. Find s, t s.t. $as + bt = 1$, and write

$$\begin{tikzcd} & \mathbb{Z}/a \arrow[dr, "\cdot b"] & \\ \mathbb{Z}/ab \arrow[ur, "\cdot t"] \arrow[dr, "\cdot s"'] & \times & \mathbb{Z}/ab \\ & \mathbb{Z}/b \arrow[ur, "\cdot a"'] & \end{tikzcd}$$

This also works for order pq, $p<q$ primes, $p \nmid q-1$.

Groups of order 21. P_7 is normal, P_3 might not be

done line (but only 15 & 21, not general $p \cdot q$)

P_3 may act on P_7. If $P_7 = \langle x \rangle$, $P_3 = \langle y \rangle$, we have $x^y = x$, or x^2, or x^4

Aside. $\mathrm{Aut}(\mathbb{Z}/p)$ is cyclic; $\mathrm{Aut}(\mathbb{Z}/7) = \langle x \mapsto x^3 \rangle$

1 3 2 6 4 5

Debt. What does this mean?

This also works for order pq, $p<q$ primes, $p \mid q-1$.