Wed, Oct 22, 2014

Last time we saw the power of counting:

Prop'n If G is a p-group ($|G| = p^e$ for some $e \geq 1$) and $|X|$ is not divisible by p, then any action of G on X has a fixed pt.

I said we'd milk the counting strategy for all it's got. I stated (w/o) proof:

Thm (First Sylow Thm) If p divides $|G|$, then G has a Sylow p-subgroup.

Recall: A Sylow p-subgroup $H \subset G$ is a subgp for which

$$|H| = p^e.$$

Here, p^e is the highest power of p dividing $|G|$. So if

$$|G| = p^e m,$$

then $\gcd(p, m) = 1$.

Ex Let

$$G = S_7 \times \mathbb{Z}/14\mathbb{Z}.$$

Then

$$|G| = 7! \times 14$$
$$= 7^2 \times 5 \times 3^2 \times 2^5.$$

The First Sylow Theorem guarantees that this group will have

- A subgroup of order 49
- A " " " 5
- " " " 9
- " " " 32.

Ex Could you find a subgroup of order 16 in S_7?

Let's try proving this theorem.

What should our strategy be?

Counting.

The better question is: Count what?

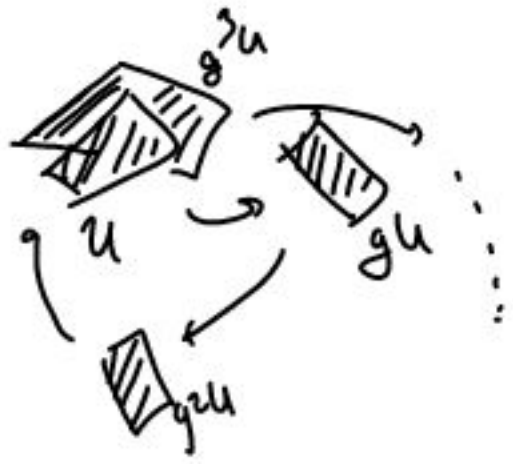
Pf (of First Sylow Thm). (Following Artin §7.7)

Let X be the set of all subsets of G of order p^e.

Then G acts on X as follows:

If $U \in X$ (so U is a subset of G of size p^e) then

$$gU = \{gh \mid h \in U\}.$$



Ex If $G = S_4$, let $U = \{(13), (2134)\}$

Then

(13) $U = \{1_{S_4}, (2134)\}$.

(1432) $U = \{(1243), 1_{S_4}\}$.

etc.

Going on w/ the proof,

$$|X| = \sum_{\text{orbits } \mathcal{O}} |\mathcal{O}|.$$

Claim 1: p doesn't divide $|X|$.

With this in mind (I'll prove the claim soon), what do we know?

$\exists$ at least one $\mathcal{O}$ for which p doesn't divide $|\mathcal{O}|$. Let $U \in \mathcal{O}$, so U is some subset of X, w/ order p^e.

Claim 2: The stabilizer of U has order divisible $|U|$.

A lot of subsets flying around, but now we're done. Let $H \subset G$ be the stabilizer of U. Then

$$|\mathcal{O}_U| = |G|/|H|.$$

But

$$|G| = p^e m = |Q_u| \cdot |H|$$

not divisible by p

divides $|U| = p^e$, so is a power of p.

Thus

$$|H| = p^e. \;//$$

Let's prove these claims!

Pf of Claim 1: The number of subsets of order p^e in a set not divisible by p. Well, we have

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

(p^e products in the numerator; p^e products in the denominator)

Note if p divides a numerator term $p^e m - k$, it also divides $p^e - k$ in the denominator, and the same # of times! Why? If

$$k = p^i l, \quad p \nmid l.$$

$$p^e m - k = p^i (p^{e-i} m - l)$$

$$p^e - k = p^i (p^{e-i} - l).$$

Note i<e, else $p^e - k$ would be negative!

So $\frac{p^e m - k}{p^e - k}$ is NOT divisible by p.

Recall: $\binom{a}{b}$ = ways to choose b unordered things from a collection of size a. So

$$\binom{a}{b} = \frac{a!}{b!\,(a-b)!}.$$

Claim 2: $U \subset G$ a subset.

Then stabilizer has order dividing $|U|$.

Pf. If U is fixed by H, then $U = \bigcup_{u \in U} Hu$, and U is partitioned into cosets.

$$U = \coprod Hu.$$

So $|U| = |H| + \cdots + |H|$. //