Lecture 14, 29/10/2015

Summary thus far:

① <u>Basic examples</u>: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, S_n, $GL_n(\mathbb{R})$
modular arithmetic, CRT, $sgn: S_n \to \{\pm 1\}$

② <u>Basic definitions</u>: gp, subgp, hom, Ker, Im, cosets, G/H,
<u>& constructions</u> quotient gp G/N, isom thms, generators

③ <u>Basic tools</u>: group actions, conjugation, orbits + stabilizers.

<u>Next</u>: study finite groups.

<u>Today</u>: <u>p-groups</u>

<u>Start</u>: partial converse to Lagrange.
Fix group G of order $n<\infty$

<u>Thm</u>: (Cauchy) Let $p|n$ be prime. Then G has an element of order p

<u>Pf</u>: Let G be a minimal counterexample

For any proper subgp of $H<G$, H does not have an element of order p

So, by minimality of G, $p \nmid \#H$. But $p | \#G = \#H \cdot [G:H]$ ← Lagrange

so $p | [G:H]$ for all proper subgps

Consider the <u>class equation</u>: $\#G = \#Z(G) + \sum_x [G:Z_G(x)]$ ← sum over non-central classes

Here $p | \#G$ by assumption, $p | [G:Z_G(x)]$
since x not central
$\Leftrightarrow Z_G(x) \neq G$.

So $p | \#Z(G)$. so $Z(G)=G$, i.e. G is abelian.

$G \neq \{e\}$ ($p \mid n$), so there is $x \in G \setminus \{e\}$ let $N = \langle x \rangle$.

Two cases: (1) suppose $p \mid \#N$. Then N, being cyclic, has an element of order p ($\mathbb{Z}/m\mathbb{Z}$ has $[\frac{m}{p}]_m$)

(2) suppose $p \nmid \#N$. Then $p \mid \# G/N$, where this a group since N is normal (G is abelian)

But order of G/N is smaller than order of G.

So there is $\bar{y} \in G/N$ of order p, $\bar{y} = yN$, $y \in G$.

Consider order of y. Suppose y has order k

have $\bar{y} = q(y)$, $q: G \to G/N$ is the quotient map.

Then $\bar{y}^k = (q(y))^k = q(y^k) = q(e) = e_{G/N}$

so $p \mid k$. Then $y^{k/p}$ has order p.

$\boxtimes$

Corollary: Order of G is a power of p iff order of every $g \in G$ is a power of p

(Neccessity is Lagrange's thm: every divisor of p^k is a power of p)

Def: Call G a p-group if every $g \in G$ has order p^k for some $k \geq 0$

Saw: G finite then G p-group iff $\#G = n = p^k$ for some $k \geq 0$.

Observation: If G is a finite p-group every subgp has prime-power index.

So if G acts on finite set X, since

$$\# X = \sum_{O(x) \in G \setminus X} [G : \mathrm{Stab}_G(x)] = \underbrace{\# \mathrm{Fix}(G)}_{\text{orbits of size 1}} + \underbrace{\sum_{O(x) \in G \setminus X} [G : \mathrm{Stab}_G(x)]}_{\text{non-trivial orbits}}$$

~~So~~ But $p \mid [G : \mathrm{Stab}_G(x)]$ if x not fixed by G,

so $\quad \# X \equiv \# \mathrm{Fix}(G) \quad (p)$

Thm: Let G be a finite p-group. Then $Z(G) \neq \{e\}$

Pf: By observation, applies to conjugation in G
(i.e. to class equation)

$$\# Z(G) \equiv \# G \equiv 0 \quad (p)$$

but $1 \not\equiv 0 \ (p)$.

Remark: Since $Z(G) \triangleleft G$, can use arguments by induction, using $G/Z(G)$

Lemma: Suppose $G/Z(G)$ is cyclic. Then $G = Z(G)$

Pf: Let $y \in G$ be such that $\bar{y} = yZ(G)$ generates $G/Z(G)$

Then every $g \in G$ is of the form $y^k z$ for $k \in \mathbb{Z}$, $z \in Z(G)$

reason: $\exists z : g = y^k z \iff g \equiv y^k \pmod{Z(G)} \iff \bar{g} = \bar{y}^k$ in $G/Z(G)$

there is such k since $G/Z(G) = \langle \bar{y} \rangle$.

Finally, $(y^k z) \cdot (y^l z') = y^k z y^l z' \underset{\substack{\uparrow \\ z \in Z(G)}}{=} y^k y^l z z' = y^{k+l} z z'$

while $(y^l z')(y^k z) = \qquad = y^{l+k} z' z$

(Ex: X generates G mod $N \iff X, N$ generate G)

Prop: (1) Let G have order p^2. Then $G \simeq C_{p^2}$ or $C_p \times C_p$.

(2) Let G be abelian, of order p^3. Then $G \simeq$ one of C_{p^3}, $C_p \times C_p \times C_p$, $C_{p^2} \times C_p$

(3) Let G be non-abelian, of order p^3. Then $Z(G) \simeq C_p$ and $G/Z(G) \simeq C_p \times C_p$

Pf; (1) Say $\#G = p^2$. $\#Z(G) \in \{1, p, p^2\}$

$\#Z(G) \neq 1$ by thm. if $\#Z(G) = p$, then $\#G/Z(G) = p^2/p = p$

but this would make $G/Z(G) \simeq C_p$ which is impossible!

Conclusion: $G = Z(G)$. If G has an element of order p^2,

$G \simeq C_{p^2}$ Otherwise every $g \in G$ has order 1 or p

Let $x \in G$ have order p. Let $y \in G \setminus \langle x \rangle$. Then y also has order p.

Consider subgps $\begin{cases} A = \langle x \rangle \\ B = \langle y \rangle \end{cases}$. These are normal

disjoint: $A \cap B$ has size 1 or p

but not p since $A \neq B$.

Then $\underset{\displaystyle AB}{\overset{\displaystyle G}{\cup\!\!|}} \simeq A \times B$ ~~because~~ but $\#AB = p^2 = \#G$, so $G = A \times B$.

$\simeq C_p \times C_p$

(3) $\#G = p^3$, G non-commutative. Then $\#Z(G) \in \{1, p, p^2, p^3\}$

but not $1, p^3, p^2$. (not p^2 since $\#G/Z(G) \neq p$)

so $\#Z(G) = p$, $G/Z(G)$ has order p^2 so it's $C_p \times C_p$

(can't be C_{p^2} which is cyclic)

(2) $\#G = p^3$, G commutative.

(a) if G has element of order p^3, $G \simeq C_{p^3}$

(b) if G has no elements of order p^3, but has x of order p^2

let $A = \langle x \rangle$. ..

(c) if every not-id element has order p, proceed as in (1):

find x of order p, $A = \langle x \rangle$, $y \in G \setminus A$, $B = \langle y \rangle$.

Then $AB \simeq C_p \times C_p$. Take $z \notin AB$. Then $\langle z \rangle \simeq C_p$, disjoint from AB

Get: $(AB) \cdot C \cong (AB) \times C = A \times B \times C$ has order p^3