Math 322, lecture 14, 26/10/2017

Last time: group actions, examples

Today: p-groups

Let G be a finite group. Lagrange: if $g \in G$, order of g divides $\#G$.

Thm: (Cauchy 1845) Suppose $p \mid \#G$. Then G has an element of order p.

Pf: (induction) Let G be a counterexample of least order. ($p \mid \#G$, G has no element of order p)

Consider class equation. (group action, stabilizer)

$$\#G = \#Z(G) + \sum_{i=1}^{h} [G : Z_G(x_i)],$$

where $\{x_i\}_{i=1}^{h}$ represent non-central conjugacy classes. The centralizers $Z_G(x_i)$ are proper subgroups (x_i are non-central) (subgps) so thm holds for them. They have no elements of order p, so $p \nmid \#Z_G(x_i)$. But $p \mid [G : Z_G(x_i)] \cdot \#Z_G(x_i) = \#G$ (Lagrange's thm)

so $p \mid [G : Z_G(x_i)]$ for each i.

Also $p \mid \#G$, so $p \mid \#Z(G)$. Get $Z(G)$ is non-trivial, and that it's enough to work there.

Let $x \in Z(G)$ be non-trivial, $N = \langle x \rangle$, $\#N = n$.

Case 1: (division into cases) Order of x is divisible by p. Then $x^{n/p}$ has order p. — contradiction!

Case 2: order of x is prime to p ($p \nmid n$). Then $p \mid [Z(G):N]$ where $[Z(G):N] = \#Z(G)/N$ ← quotient groups

but $Z(G)/N$ is a group ($N \trianglelefteq Z(G)$ since $Z(G)$ is commutative) since $N \neq \{e\}$, $\#(Z(G)/N) < \#Z(G) \leq \#G$, so Cauchy's thm holds for $Z(G)/N$ and it has an element $\bar{y}$ of order p

Let $y \in Z(G)$ be any preimage of $\bar{y}$. If $q: Z(G) \to Z(G)/N$ is the quotient map, $q(y) = \bar{y}$. ↑ homomorphisms

Say y has order m. Then $y^m = e \Rightarrow (q(y))^m = e$.

i.e. $\bar{y}^m = e$. But $\bar{y}$ has order p so $p \mid m$, and we are back in case 1. ↑ orders of elements

∎

Cor: Let G be a finite gp, p a prime. TFAE:

(1) Every element $g \in G$ has order p^k for some k (depending on g)

(2) Order of G is a power of p

Pf: (2) $\Rightarrow$ (1) by Lagrange

not (2) $\to \neg(2) \Rightarrow \exists$ prime $q \neq p$ s.t. $q \mid \#G$ and then G has an element of order q, so $\neg(1)$.

Def: Call a gp G a p-group if every element has p-power order.

Recall: If G is a finite p-gp, X finite G-set, then

$\#X = \#\mathrm{Fix}(G) \pmod{p}$ (*)

(3) If $\#G = p^2$, G non-commutative then $\#Z(G) = p$, $G/Z(G) \simeq C_p \times C_p$

Pf: (1) Let G have order p^2, then $\#Z(G) \in \{1, p, p^2\}$ by Lagrange

But $Z(G) \neq \{e\}$ (G is a p-gp) and $\#Z(G) \neq p$ (that would mean $\#G/Z(G) = p^2/p = p$, so $G/Z(G)$ would be cyclic).

so $\#Z(G) = p^2$, i.e. $Z(G) = G$.

Case 1: G has an element of order p^2.

Then $G \simeq C_{p^2}$.

Case 2: Every $g \in G$ has order 1 or p

write $+$ for the operation of G.

for $k \in \mathbb{Z}$, $g \in G$ write $k \cdot g = g + \dots + g$ (k times). Note: $p \cdot g = 0$ (identity element)

Can define $[k]_p \cdot g = k \cdot g$

Ex: $(G, +, \cdot)$ is a vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Cor: As a vsp G is finite so finite dim, dim must be 2.

since $\#\mathbb{F}_p^{\text{2d}} = p^d$, so $G \simeq C_p \times C_p$.

(2) Say $\#G = p^3$, G commutative. Same reasoning:

- if G has element of order p^3, $G \simeq C_{p^3}$
- if every element has order $\leq p$ then $G \simeq (C_p)^3$

Rephrase Cauchy's thm: If $p \mid \#G$ then some (non-triv) subgp of G is a p-gp

Study p-groups.

(Aside: If V v.sp / $\mathbb{F}_p$, then $(V,+)$ is a p-gp. If $\dim_{\mathbb{F}_p} V < \infty$, V is ∞)

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

Pf: Let G act on itself by conjugation. The number of fixed points is $\equiv \#G \pmod p$. But e is a fixed point, so have at least p fixed points.

Lemma: Let G be any gp s.t. $G/Z(G)$ is cyclic. Then G is commutative, $G = Z(G)$.

Pf: Suppose $G/Z(G)$ is generated by image of $g \in G$

This means any $x \in G$ has $X \equiv g^k (Z(G))$ for some k

i.e. $x = g^k z$ for some $k \in \mathbb{Z}$, $z \in Z(G)$

Let $y \in G$ be another element. Then $y = g^l w$ for some $l \in \mathbb{Z}$, $w \in Z(G)$

Then
$$xy = (g^k z)(g^l w) = g^k z g^l w \overset{z \in Z(G)}{=} g^k g^l z w = g^{k+l} \cdot zw$$
$$yx = (g^l w)(g^k z) = g^l w g^k z = g^l g^k z w = g^{l+k} \cdot zw \quad \text{))}$$
$$\uparrow \; w \in Z(G)$$

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

(2) Let G have order p^3, G commutative. Then G is one of

C_{p^3}, $C_{p^2} \times C_p$, $C_p \times C_p \times C_p$