Math 322, lecture 15 31/10/17

Last time: $G/Z(G)$ ~~abelian~~ cyclic $\Rightarrow G$ abelian

G p-gp $\Rightarrow Z(G) \neq \{e\}$ (if G finite)

$\#G = p^2 \Rightarrow G$ abelian, $G \simeq C_{p^2}$ or every element has order $| p$

Continue:

$\#G = p^2$, every element has order $| p$, G commutative

Goal: Show $G \simeq C_p \times C_p$

Pf: let $x \in G$, $x \neq e$. Then x has order p, so $\#\langle x \rangle = p < p^2$

let $y \in G \setminus \langle x \rangle$ (so y has order p as well)

Consider map $f : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$

given by $f([a]_p, [b]_p) = x^a y^b$

recall (study of cyclic gps): if x has order n, map $\mathbb{Z}/n\mathbb{Z} \to \langle x \rangle$, $[a]_n \mapsto x^a$ is an isom.

$\Rightarrow f$ is well-defined.

Also, $f \in \mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})^2, G)$:

$$f([a_1 + a_2], [b_1 + b_2]) = x^{a_1+a_2} y^{b_1+b_2} = x^{a_1} x^{a_2} y^{b_1} y^{b_2}$$

$$= x^{a_1} y^{b_1} x^{a_2} y^{b_2} = f([a_1], [b_1]) \cdot f([a_2], [b_2])$$

G is abelian

f is surjective: $\mathrm{Im}(f) \supset \langle x \rangle$ $(x = f([1], [0]))$.

also $\operatorname{Im}(f) \ni y$ so $\operatorname{Im}(f) \neq \langle x \rangle$.

So $\# \operatorname{Im}(f)$ is a divisor of p^2 larger than p

so $\# \operatorname{Im}(f) = p^2$, ie. $\operatorname{Im}(f) = G$.

$\# C_p^2 = p^2 = \# G$ so by the pigeon hole principle f is injective as well, ie. $G \cong C_p^2$.

<u>Remark:</u> f gives G structure of vsp over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ where $\{x, y\}$ is a basis

But can do this abstractly (define $x + y \overset{\text{def}}{=} x \cdot y$, $[a] \cdot x = x^a$, mult in G)

then invoke linear algebra

fact: every vsp is $\cong \mathbb{F}_p^k$ by choosing basis)

<u>Prop:</u> Let G be abelian of order p^3. Then G is one of C_{p^3}, $C_{p^2} \times C_p$, $C_p \times C_p \times C_p$.

<u>Pf:</u> If G has an element of order p^3, $G \cong C_{p^3}$.

If every element ($\neq e$) has order p, $G \cong C_p \times C_p \times C_p$:

choose $x \in G \setminus \{e\}$, $y \in G \setminus \langle x \rangle$, $z \in G \setminus \langle x, y \rangle$:

$\langle x \rangle$ has order p, by previous construction $\langle x, y \rangle = \{x^a y^b \mid a, b \in \mathbb{Z}/p\mathbb{Z}\}$ has order p^2. Now $(a, b, c) \mapsto x^a y^b z^c$ get isom $(\mathbb{Z}/p\mathbb{Z})^3 \to G$.

Otherwise, there is $x \in G$ of order p^2 but no element has order p^3. Goal: find $y \in G$ of order p s.t.

$$G = \left\{ x^a y^b \;\middle|\; \begin{matrix} a \in \mathbb{Z}/p^2\mathbb{Z} \\ b \in \mathbb{Z}/p\mathbb{Z} \end{matrix} \right\}$$

Argument: choose $y \in G \setminus \langle x \rangle$, "adjust" it to have order p

For this consider map $g \mapsto g^p$. This is a hom $G \to G$ (because G is abelian). Call the image G^p. Then $G^p \neq \{e\}$: x has order p^2, so $x^p \neq e$. Also, $G^p \neq G$: map $g \mapsto g^p$ not injective so not surjective. Kernel contains x^p since $(x^p)^p = x^{p^2} = e$

So what is G^p? Suppose $\#G^p = p^2$.

If $G^p \cong C_{p^2}$ then some $z \in G$ has z^p of order p^2
so z has order p^3: $e = (z^p)^{p^2} = z^{p \cdot p^2} = z^{p^3}$, but G has no such elements

If $G^p \cong C_p \times C_p$, then let x have order p^2 so that $x^p \in G$
Then let $y \in G^p \setminus \langle x^p \rangle$, so that $G^p = \langle x^p \rangle \langle y \rangle$

Then $\langle y \rangle \cap \langle x \rangle = \{e\}$ (any power of x of order p is a power of x^p, and y isn't of that form)

so $\left\{ x^a y^b \;\middle|\; \begin{matrix} a \in \mathbb{Z}/p^2\mathbb{Z} \\ b \in \mathbb{Z}/p\mathbb{Z} \end{matrix} \right\}$ contains $\langle x \rangle$ but differs from it and $G \cong C_{p^2} \times C_p$

Else, $\# G^p = p$. Again, let x have order p^2.

Then $e \neq x^p$ generates G^p.

Let $y \in G \setminus \langle x \rangle$. Consider $y^p \in G^p$: have

$$y^p = (x^p)^j \text{ for some } j.$$

Consider then $y' = y x^{-j}$: $(y')^p = y^p \cdot x^{-jp} = e$ so y' has order p.

Also, $y' \notin \langle x \rangle$: if $y' \in \langle x \rangle$ then $y = y' \cdot x^j$ would also be there

Consider $\left\{ x^a (y')^b \;\middle|\; \begin{matrix} a \in \mathbb{Z}/p^2\mathbb{Z} \\ b \in \mathbb{Z}/p\mathbb{Z} \end{matrix} \right\}$ as before, this is the image of a hom $C_{p^2} \times C_p \to G$

Image contains $\langle x \rangle$ but also y', so is G and we are done.

Groups of order pq

(Convention: q also prime, $q \neq p$)

Question: list groups of order $6 = 2 \cdot 3$:

$$C_6, S_3, D_6, C_2 \times C_3$$

but D_6 = symmetry group of  $\simeq S_3$ since all vertices are connected and $C_2 \times C_3 \cong C_6$ (CRT)

(but $C_6 \not\cong S_3$ because C_6 commutative, S_3 isn't)

we'll show C_6, D_6 only isom classes of order 6.

Pf: Let G have order 6. By Cauchy's thm it has a subgp P of order 2, and a subgp Q of order 3.

Then order of $P \cap Q$ divides the orders of P and Q (Lagrange's thm) so $P \cap Q = \{e\}$

Lemma: Let G be any gp, $P, Q < G$ s.t. $P \cap Q = \{e\}$

Then the ~~map~~ (set) map

$$P \times Q \to PQ$$
$$(x,y) \mapsto xy$$

is a bijection.

Pf: say $xy = x'y'$ then $x^{-1}x' = y \cdot (y')^{-1} \in P \cap Q$

$x, x' \in P$
$y, y' \in Q$

so $x^{-1}x' = y(y')^{-1} = e$

so $x' = x$, $y' = y$.

(in general bijection is $P \times Q \leftrightarrow PQ \times P \cap Q$.)

It follows that $\# PQ = \# P \cdot \# Q = 2 \cdot 3 = 6$, so $PQ = G$.

$$G = \left\{ x^a y^b \;\middle|\; \begin{array}{l} a \in \mathbb{Z}/2\mathbb{Z} \\ b \in \mathbb{Z}/3\mathbb{Z} \end{array} \right\}$$

Claim: Q is normal

Pf: Let $\mathcal{C} = \{gQg^{-1}\}_{g\in G}$ be the conjugacy class of Q.

$$= \{xyQy^{-1}x^{-1} \mid \begin{smallmatrix} x\in P \\ y\in Q \end{smallmatrix}\} = \{xQx^{-1} \mid x\in P\} =$$

$\uparrow$ $G = PQ$ $\qquad$ $\uparrow$ $yQy^{-1} = Q$ if $y \in Q$

$$= \{Q, xQx^{-1}\} \text{ if } P = \{1, x\}$$

Suppose that $Q \neq Q' = xQx^{-1}$. Still have $Q' \cong Q$ &, $\#Q' = 3$

$Q \cap Q'$ is a subgp of $Q \cong C_3$, not Q $(Q \neq Q')$ so must be trivial so $\#QQ' = 3\cdot 3 = 9 > 6 \overset{\#G}{=}$, impossible

We conclude that $Q' = Q$, i.e. Q is normal

$\Rightarrow G = PQ$ where $P \cap Q = \{e\}$, Q is normal

$\Rightarrow G \cong P \ltimes Q$.

Want G exactly. For this let $x, x' \in P$
$y, y' \in Q$.

Then $(x'y')(xy) = \underset{\substack{\cap \\ P}}{(x'x)} \cdot \underset{\substack{\cap \\ Q}}{((x^{-1}y'x)} \cdot y) \leftarrow Q$ is normal

$\Rightarrow$ group operation on G determined by action of P on Q by conjugation - on knowing $x^{-1}y'x$.

Recall $P = \{e, x\}$ where $x \cdot x = e$, $e^{-1} y' e = y'$

Need to know what $x y' x$ is $(x^{-1} = x)$

Write $Q = \{1, y, y^2\}$ now $x^{-1} \cdot 1 x^{-1} = 1$ so only have two possibilities:

(1) $x^{-1} y x = y$, $x^{-1} y^2 x = y^2$

(2) $x^{-1} y x = y^2$, $x^{-1} y^2 x = y$

<u>Case 1:</u> x, y commute, $(x' y')(x y) = (x' x)(y' y)$

$$G \cong C_2 \times C_3 \cong C_6$$