Lecture 16, 3/11/2015

Q: What's $\mathbb{F}_p$ A: The field with p elements: $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$

Last time: G order p^2 $\Rightarrow$ G commutative, $\cong C_{p^2}$ or $C_p \times C_p$

G order p^3, commutative $\Rightarrow$ $G \cong C_{p^3}$ or $C_{p^2} \times C_p$ or $C_p \times C_p \times C_p$

G order p^3, non-commutative $\Rightarrow$ $Z(G) \cong C_p$, $G/Z(G) \cong C_p \times C_p$
(two isom classes)

Key: $Z(G) \neq \{1\}$ if $|G| = p^n$.

HW: if $|G| = p^n$, $Z(G) \cap N \neq \{1\}$ for $N \trianglelefteq G$ | if $0 \le k \le n$ $\exists N \trianglelefteq G$, $\# N = p^k$.

Today: Study groups of order pq.
($p \neq q$ prime)

① groups of order $6 = 2 \cdot 3$

Examples: C_6, S_3, D_6. Note: C_6 commutative, S_3, D_6 aren't.

In fact, $D_6 \cong S_3$: $D_6 = \mathrm{Aut}(\triangle) \cong S_3$
all vertices are connected

Let's try classifying G of order 6
Method: build group up.

By Cauchy's thm, G has subgps P of order 2, Q of order 3.

The order of $P \cap Q$ is 1 (must be a common divisor of 2, 3 by Lagrange)

Lemma: Suppose $P, Q < G$, $P \cap Q = \{e\}$. Then the map $P \times Q \to PQ$ given by $(x, y) \mapsto xy$ is a bijection.

Pf: Suppose $xy = x'y'$, $x, x' \in P$, $y, y' \in Q$. Then $x^{-1}x' = y(y')^{-1} \in P \cap Q = \{e\}$
then $x = x'$, $y = y'$.

[In fact, for any P, Q get bijection
$$P \times Q \leftrightarrow PQ \times P \cap Q.]$$

Conclusion: since $\#(P \times Q) = 2 \cdot 3 = 6$, $G = PQ$.

Claim: Q is normal.
Short pf: $[G : Q] = 2$.
Long pf: let $\mathcal{C} = \{gQg^{-1} \mid g \in G\}$ be the conjugacy class of Q.
Know: $G = PQ$, so any $g \in G$ has the form $g = xy$, $x \in P$, $y \in Q$
then
$$gQg^{-1} = (xy)Q(xy)^{-1} = x(yQy^{-1})x^{-1} = xQx^{-1}!$$
So: orbit of Q under conjugation by G = orbit under conjugation by P.
Let's say $P = \{1, a\}$. Then $\mathcal{C} = \{Q, aQa^{-1}\}$
either $aQa^{-1} = Q$, then $C = \{Q\}$, Q is normal,
Or, $aQa^{-1} = Q' \neq Q$. In this case, let Q act by conjugation on $\mathcal{C}$.
In an action of Q, the size of any orbit divides $\#Q$.
No orbits of size 3 here, so $\{Q'\}$ is a orbit of size 1, ie.
Q normalizes Q'. Also, $Q \cap Q' \neq Q', Q$ so $Q \cap Q' = \{e\}$
[By HW, QQ' is then a subgp of G of order 9]
By lemma, $\#(QQ') = \#Q \cdot \#Q' = 9 > 6 = \#G$ – that's impossible

Conclusion: G has subgps P, Q, $P \cap Q = \{e\}$, $Q \triangleleft G$.
Thus $G = P \ltimes Q$.
Goal: Get mult. table. So, let $xy, x'y' \in G$: $x, x' \in P$, $y, y' \in Q$.
then $(xy)(x'y') = \underset{\in P}{(xx')} \underbrace{((x')^{-1} y x')}_{\in Q} \cdot y'$

Conclusion: To know mult table enough to know conj. action of P on Q

[HW: for any action of P on Q by gp aut. $\exists$ group $\tilde{G}$, subgps $\tilde{P}, \tilde{Q}$ s.t.: $\tilde{P} \cong P$, $\tilde{Q} \cong Q$, $G = \tilde{P} \ltimes \tilde{Q}$, action by conj of $\tilde{P}$ on $\tilde{Q}$
= " " aut of P on Q]

Here, $P = \{1, a\}$
$Q = \{1, b, b^2\}$ need to understand aba^{-1}.
because (conj. is a hom) $ab^2a^{-1} = (aba^{-1})^2$

What are the possibilities for aba^{-1}? b or b^2.

Case 1: $aba^{-1} = b \iff ab = ba$
so action of P on Q is trivial, P, Q commute, $G \cong P \times Q \cong C_2 \times C_3 \overset{\text{CRT}}{\cong} C_6$

Case 2: $aba^{-1} = b^{-1}$.
$D_{2n} = \langle a, b \mid b^n = e, \ aba^{-1} = b^{-1} \rangle$ so $G \cong D_6$

Classification of groups of order pq

Let $p < q$ be distinct primes, G gp of order pq.
By Cauchy's thm, G has cyclic subgroups P, Q of orders p, q.
$\#(P \cap Q)$ divides $\#P, \#Q$ so $P \cap Q = \{e\}$, $G = PQ$ (setwise)
Let $\mathcal{C} = \{gQg^{-1} \mid g \in G\} = \{xyQ(xy)^{-1} \mid x \in P, y \in Q\} = \{xQx^{-1} \mid x \in P\}$
be the conjugacy class of Q. This has at most p (In fact, either 1 or p elements) ~~let Q act on $\mathcal{C}$ by conjugation.~~
First of all, if there is $Q' \in \mathcal{C}$, $Q' \neq Q$, then $Q \cap Q' = \{e\}$ (subgp of Q, but not Q)
so QQ' has $q^2 > qp$ elements.
So $\mathcal{C} = \{Q\}$, Q is normal in G, $G = P \ltimes Q$.
Let a, b generate P, Q: $P = \{a^0, a^1, .., a^{p-1}\}$, $Q = \{b^0, b^1, .., b^{q-1}\}$
G determined by conj. action of P on Q, enough to know $aba^{-1} \in Q$.

(we need $a^i(b^j)a^{-i}$ for all i,j, but $a^i b^j a^{-i} = (a^i b a^{-i})^j$;

[For any G, map $\gamma_g(x) = gxg^{-1}$ is a hom $G \to G$: $\gamma_g(xy) = gxyg^{-1} =$
$= gxg^{-1}gyg^{-1} = \gamma_g(x)\gamma_g(y)$

so $\gamma_g(b^j) = (\gamma_g(b))^j$.]

Also, $\gamma_{gh} = \gamma_g \circ \gamma_h$: $\gamma_{gh}(x) = g(hxh^{-1})g^{-1}$.

$$a^i x a^{-i} = \underbrace{a(a(\cdot\, a}_{i}(x)\underbrace{a^{-1})\cdots)a^{-1}}_{i}$$

Need to find what aba^{-1} is, but must have: $aba^{-1} = b^k$
for some k mod q.

Q1: What values of k are permitted?

Q2: For each such k, construct G.

Q3: Isom?

Q1: evidently, $k \neq 0$. More than that, $aba^{-1} = b^k$

$a^2ba^{-2} = a(b^k)a^{-1} = (aba^{-1})^k =$
$= (b^k)^k = b^{k^2}$

since $a(b^i)a^{-1} = b^{ik}$
$a^j(b^i)a^{-j} = b^{ik^j} \leftarrow j$

$$a^j(b^i)a^{-j} = b^{i(k^j)}$$

Think additively: $a^j \cdot [i]_q \cdot a^{-j} = [i]_q \cdot [k^j]_q$ (identify Q with $\mathbb{Z}/q\mathbb{Z}$)

for $j = p$, $a^p = e$, must have $[i]_q \cdot [k^p]_q = [i]_q$ so $k^p \equiv 1\ (q)$

Obvious solution: $k = 1$, $aba^{-1} = b$, P, Q commute, $G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$.

Summary: realised G as $\langle a, b \mid a^p = e,\ b^q = e,\ aba^{-1} = b^k \rangle$ where $k^p \equiv 1\ (q)$