Lecture 16, 5/11/2015

PS7 Problem 1

Exercize: Let G be a finite group, $H < G$. Suppose $G = \bigcup_{g\in G} gHg^{-1}$. Then $H = G$.

Pf: Need to show $\bigcup_{g\in G} gHg^{-1} \subsetneq G$ (assume $H \neq G$)

Idea 1: try to prove $\left|\bigcup_{g\in G} gHg^{-1}\right| < |G|$.

natural to start with $\left|\bigcup_{g\in G} gHg^{-1}\right| \leq (\#\text{conjugates}) \cdot \# H$.

Recall: #conjugates of $H = [G : N_G(H)]$

so want to show $[G : N_G(H)] \cdot \# H < \# G$

Idea 2: Note Lagrange's Thm: $[G : N_G(H)] \cdot \# N_G(H) = \# G$

or $[G : H] \cdot \# H = \# G$

notice: yes, $H \leq N_G(H)$

so $\# N_G(H) \geq \# H$, we get:

$$\left|\bigcup_{g\in G} gHg^{-1}\right| \leq [G : N_G(H)] \cdot \# H \leq [G : N_G(H)] \cdot \# N_G(H) = \# G$$

Almost succeeded, remains to attack one inequality, make it strict

Idea 3: $\left|\bigcup_i A_i\right| = \sum_{i=1}^{r} |A_i|$ (A_i finite) holds iff union is disjoint

But $\{gHg^{-1}\}$ aren't disjoint - they all contain e, and we're done if at least 2 conjugates. But if H is normal, $\bigcup_{g\in G} gHg^{-1} = H$ and this is G only if $H = G$.

Back to gps of order pq

Recap: G of order pq, $p<q$ primes

Cauchy $\Rightarrow$ subgps P, Q of order p, q respectively.

Q is normal: unique subgp of order q.

(if Q' also has size q then QQ' has size $q^2 > pq$)

suppose $P = \langle a \rangle$, $Q = \langle b \rangle$

then $aba^{-1} = b^k$ and choice of k determines G

($G = PQ$, to multiply $(a^i b^j)(a^\ell b^m)$ have

$$b^j a^\ell = a^\ell(a^{-\ell} b^j a^\ell) = a^\ell \cdot b^{j[k]^{-\ell}}, \quad [k] = \text{class of } k \text{ mod } q.$$

Ended with noting that $a^p = e$, so

$$a^p b (a^p)^{-1} = b^{k^p} = b \qquad \text{so } k^p \equiv 1 \ (q)$$

clearly $k=1$ is a solution, and $C_p \times C_q$ is a gp of order pq.

(if a, b commute then $G = \langle a,b \rangle$ commutes, so $G = P \times Q = C_p \times C_q \cong C_{pq}$.

What about other values of k?

Observation 1: $k^p \equiv 1 \ (q)$ means $[k] \in (\mathbb{Z}/q\mathbb{Z})^\times$ has order p

by Cauchy have such $k \neq 1$ iff $p \mid q-1 = \#(\mathbb{Z}/q\mathbb{Z})^\times$.

i.e. iff $q \equiv 1 \ (p)$

Cor: The only group of order 35 is C_{35} $(7 \not\equiv 1 \ (5))$

Still to do: ① show that if $k^p \equiv 1 \ (q)$ there really is G with $aba^{-1} = b^k$.

② handle isom

Observation 2: define a group ~~by~~ structure on $C_p \times C_q$ by $([i]_p, [j]_q) \cdot ([\ell]_p, [m]_q) = ([i+\ell]_p, [j \cdot \bar{k}^\ell + m]_q)$ where $\bar{k}$ inverse to k mod q.

(defining things so that for $a = ([1],[0])$, $b = ([0],[1])$, $aba^{-1} = b^k$

$P = \{([i],[0])\} \cong C_p$
$Q = \{([0],[j])\} \cong C_q$ $\leftarrow$ check! $G = P \rtimes Q$.

This is a group: $([0],[0]) \cdot ([\ell],[m]) = ([\ell], [0 \cdot \bar{k}^\ell + m]) = ([\ell],[m])$

$([i],[j])([0],[0]) = ([i],[j])$ check

and $([i],[j]) \cdot (-[i], -[j \cdot k^i]) = ([0],[0])$

associativity holds (check!)

The operation is well-defined because if $\ell' \equiv \ell$ (C_p) then $\bar{k}^\ell \equiv \bar{k}^{\ell'}$ (q) (because $k, \bar{k}$ have order p mod q)

$\left[\ \bar{k}^{\ell-\ell'} = (\bar{k}^p)^{\frac{\ell-\ell'}{p}} \equiv 1 \ (q)\right]$

Is k unique? no! $[i]$ is also a generator of $\mathbb{Z}/p\mathbb{Z} = C_p$ (if $[i] \neq [0]$) and $a^i b a^{-i} = b^{k^i}$.

Interpretation 1: k is not unique. If for one choice of a, b have $aba^{-1} = b^k$ then also have choice where $aba^{-1} = b^{k^i}$.

Interpretation 2: The semidirect prods $C_p \rtimes C_q$ with k, k^i are isomorphic

Conclusion: replacing k with k^i gives an isomorphic gps, so gps corresponding to $k, k^2, k^3, \dots, k^{p-1}$ are same

Remains to ~~contat~~ count solutions to $k^p \equiv 1 \ (q)$, ie. to

$$x^p - 1 = 0 \text{ in } \mathbb{Z}/q\mathbb{Z}$$

But a polynomial of degree p over a field has at most p roots!

So bottom line: either $q \not\equiv 1 \ (p)$, only gp is $C_p \times C_q = C_{pq}$

or $q \equiv 1 \ (p)$ then two gps, $C_p \times C_q$, $C_p \ltimes C_q$.

Example: $p = 2$, q odd get C_{2q}, $D_{2q} = C_2 \ltimes C_q$

Tools: Cauchy's thm produced subgps P, Q
conjugation action showed Q normal,
Counting showed $G = PQ \Rightarrow G \cong P \ltimes Q$.
Analysis of actions of P on Q classified possible semidirect products

---

Examine case of $n = 15 = 3 \cdot 5$.

Can a, of order 3, act on C_5?

say $\langle b \rangle \cong C_5$, say $aba^{-1} = b^k$, $k = 1, 2, 3, 4$
$1, 2, -2, -1$

these define maps $C_5 \to C_5$:

$f(1) = 1 \quad f(i) = i \mod 5$

$f(1) = 2 \quad f_2(i) = 2i \mod 5$

$f(1) = 3 \quad f_3(i) = 3i \mod 5$

$f(1) = 4 \quad f_4(i) = -i \mod 5$

$f_1 = \text{id}. \quad f_4 \circ f_4 = \text{id} \quad f_2^2(i) = 2(2i) = -i$

$f_2^4 = \text{id} \quad f_3^2 = f_4 \text{ so } f_3^4 = \text{id}.$

$P = C_3$ normalize $Q = C_5$. So P acts on Q by automorphisms.
But $\mathrm{Aut}(Q)$ has no elements of order 3
so every $a \in P$ acts trivially, i.e. commutes with Q,
and G is commutative

What about $n = 21 = 3 \cdot 7$

note $2^3 \equiv 1 \ (7)$

(note: $5^3 \equiv -1 \ (7)$ so 5 has order 6.
$(5 \equiv -2)$ so $(\mathbb{Z}/7\mathbb{Z})^\times \cong C_6$)

so $[1]_3$ can act by $[i]_7 \mapsto [2i]_7 = [2]_7 [i]_7$

Facts: (1) $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}, +) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

(2) For p prime, $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$
(also true for $(\mathbb{Z}/p^k\mathbb{Z})^\times$ if p odd)

(if ~~H~~ F is a field, $H < F^\times$ is finite, then H is cyclic)