Problem 1

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

Then $H = G$.

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

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

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

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

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

Idea 2: Note Lagrange's Theorem $|G:N_G(H)| \cdot |H| = \#G$

or $|G:H| \cdot \#H = \#G$

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

so $|H| \leq |N_G(H)| \cdot \#H$, we get:

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

Almost succeed, remains to attach one inequality, make it strict.

Idea 3: $|\bigcup_{i=1}^k A_i| = \sum_{i=1}^k |A_i|$ (finite) holds iff union is disjoint.

But $\bigcup_{g \in G} gHg^{-1}$ 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 $H = G$. 

Lecture 16, 5/14/2015
Back to Sylow of order $p^2$

Recall $G$ of order $p^2$, $p < q$ 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 $q^2 = p^2$)

Suppose $p = \langle a \rangle$, $Q = \langle b \rangle$,

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

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

$ba^e = a^e (a^{-e} b a^e) = b a^e b^{-1} a^{-e}$.

$[k] = \text{class of } k \text{ mod } q$.

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

$a^p b a^p = b^{k^p} = b$ so $k^p = 1 (q)$

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 $G = P \times Q = C_p \times C_q$ is $C_{pq}$.

What about other values of $k$?

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

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

i.e. iff $q = 1 (p)$

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

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

2 handle isom
Observation 2: Define a group $G$ by a structure on $G 	imes G$
by $(i, j) \cdot (k, l) = (i + j, k^{-l} + m j)$
where $k^{-l}$ is inverse to $k$ mod $q$.

(Defining things so that for $a = (i, j), b = (0, j)$, $aba^{-1} = b^k$
P = $\{(i, j)\} \in G$
Q = $\{(0, j)\} \in G$
$
\text{check! } G = P \times Q.$

This is a group: $(i, j), (k, l) = (i + j, k^{-l} + m j)$
$(i, j) \cdot (k, l) = (i', j')$ check

and $(i, j) \cdot (-i, -j) = (0, 0)$

Associativity holds (check!)

The operation is well-defined because if $l' = l$ (mod $p$)
then $k^{-l} = k^{-l'}$ (mod $q$) (because $k^{-l}$ have order $p$ mod $q$)

$k^{-l'} = (k^p)^{\frac{p-l'}{p}} \equiv 1 \text{ (mod q)}$

Is $k$ unique? No! $i, j$ is also a generator of $Z_p \times Z = G$
(if $[i], [j]$) and $a b a^{-1} = b^k$.

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

Interpretation 2: The semidirect products $G \times G$ with $k, k'$ are isomorphic.
Conclusion: replacing \( k \) with \( k_1 \) gives an isomorphic \( G_p \), so \( G_p \) corresponding to \( k, k^2, k^3, \ldots, k^{p-1} \) are same.

Remains to count count solutions to \( k^{p-1} = 1 \pmod{p} \).

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

So bottom line: \( q \neq 1(p) \), only \( q = 3 \) is \( \mathbb{Z}_p \times \mathbb{Z}_3 \) or \( q = 1(p) \) then two \( G_p \times \mathbb{Z}_2 \), \( G_p \times G_2 \).

Example: \( p = 2, q \) odd get \( C_{2q}, D_{2q} = C_2 \times C_2 \).

---

Tools: Cauchy's thm, produced subgps \( P, Q \).
Conjugation action showed \( Q \) normal.
Counting showed \( G = PQ \Rightarrow G = P \times Q \).
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 \( \langle b \rangle \leq C_5 \), say \( aba^{-1} = b^k \), \( k = 1, 2, 3, 4 \). \( b^4 = 1 \).

These define maps \( C_5 \rightarrow C_5 \):
- \( f(1) = 1 \)
- \( f(2) = 2 \)
- \( f(3) = 3 \)
- \( f(4) = 4 \)

\( f \circ \gamma \) (or \( f_{\gamma} \))

\( f_1 = 1d \) \( f_2 \circ f_3 = id \) \( f_2^2(i) = 2(2i) = -i \)

\( f_4 = 1d \) \( f_3^2 = f_4 \) so \( f_3^4 = 1d \).
$P = C_3$, normalize $Q = G$. So $P$ acts on $Q$ by automorphisms.

But $\text{Aut}(Q)$ has no elements of order 3.

So every act $P$ acts trivially, i.e., commutes with $Q$.

And $G$ is commutative.

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

Note $2^3 = 1 (7)$.

So $5^2 - 2 = 23$.

So $(\mathbb{Z}/7\mathbb{Z})^2 \cong C_6$.

So $\mathbb{Z}_2^3$ can act by $[i_1 j_1] \mapsto [2i_1 j_1] = [2i_1][j_1]_2$.

Facts:

1. $\text{Aut}(\mathbb{Z}/n\mathbb{Z}, +) = (\mathbb{Z}/n\mathbb{Z})^\times$.

2. For $p$ prime, $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$.

(also true for $(\mathbb{Z}/p^2\mathbb{Z})^\times$ if $p$ odd)

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