Math 422/501 lecture 2
(11/Sept/2020)
F.T. of Arithmetic: \(\mathbb{Z}_p\) has a unique representation as a product \(\prod_{i=1}^n q_i\cdot e_i\),
where \(q_i\) are distinct primes, \(e_i \in \mathbb{Z}_{\geq 1}\).

Today: non-commutative generalization

Course: (1) a bit on groups
(2) fields of extensions
(3) symmetry groups of field extensions

Idea: Know how to make \(G\) from \(H, N\) by:
(1) \(G = H \rtimes N\) (both \(H, N\) normal)
(2) \(G = H \times N\) (\(N\) normal, \(H\) acts on \(N\))

"external" pov: construct \(G\) from \(H, N\)
"internal" pov: \(H, N\) subgroups of \(G\) st: \(G = HN\)
in both cases. \( N \trianglelefteq G/N \)

More generally, if study extensions: \( N \trianglelefteq G \)

hope: \( N, H \) "simpler" than \( G \).

So classify \( G \) by classifying \( N, H \), ways to put them together.

Examples: \( C_2, C_2 \) can be put together to make \( C_2 \times C_2 \times C_2 \)

and \( S_3 = D_6 = C_2 \times C_2 \)

given \( \sigma : H \rightarrow \text{Aut}(N) \), set \( \phi : H \times N \rightarrow H \times N \)

\[ \phi(h, n) = (h \cdot n, n) \]

---

**Def:** A normal series in \( G \) is a sequence

\[ G = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq G_3 \trianglelefteq \cdots \trianglelefteq G_k = \{ e \} \]

**Intuition:** \( G \) is "assembled" from \( G_0/G_1, G_1/G_2, \ldots \)

**Assume:** \( G_i \triangleleft G_{i+1} \).

A normal series refines another if it contains all its terms (e.g. any normal series refines \( G_i \)).
Recall: correspondence theorem gives bijection\[
\{\text{normal subgroups of } G_i\} \leftrightarrow \{\text{subgroups of } G_i/\phi_i^{-1}\}.
\]
so series cannot be refined off the quotients \(G_i/\phi_i^{-1}\), are simple (have no normal subgroups \(\neq e\), \(G\)).

**Def:** A composition series is a normal series with simple factors.

**Examples:** Every finite gp has a composition series.

**Problem:** (1) List all finite simple groups.
(2) List all ways to put them together.

**Def:** The composition factors of \(G\) are the quotients of a composition series.

**Thm:** (Jordan-Hölder) the list of composition factors (with multiplicity) is unique.

**Example:** \(C_{15} \triangleleft C_5 \triangleleft 3e\)? \(C_{15} \triangleleft C_3 \triangleleft 3e\)?

\[
C_{15}/C_5 = C_3 \quad C_{15}/C_3 = C_5
C_5/3e = C_5 \quad C_2/3e = C_2
\]

**Def:** \(G\) is soluble if it has a normal series with abelian quotients.

**Remark:** A finite gp is soluble if its composition factors are abelian.
Example: Every abelian group.

(2) Every $p$-group $P$: composition factors are simple $p$-groups, so $G$ is $C_p$.

(3) $S_n$, $n \geq 3$, not solvable. $S_n \not\cong A_n$. $S_n \no D_2$ is a composition series.

(4) $S_2 = \{e\} \times G$, composition factors are $C_2, G$.

(5) Any group of order 12 is solvable.

Proof: Let $|G| = 12$. Let $P_2$ be set of 2-sylow subgroups.

1. $|P_1| \in \{1, 3\}$ (divides 12, prime to 2).
2. If $P = \{e\} \times P_2$, then $P_2$ normal, order 4, $G/P_2$ order 3.

$P_2$ abelian (either $C_4$ or $C_2 \times C_2$), $G/P_2$ abelian.

If $|P_1| = 3$, conjugation action of $G$ on $P$ is a hom.

$G \rightarrow S_3$ is 1-1, so $|S_3| = 6 < 12$, so $G/P_2 \cong P_2.$

Let $N = \text{Ker} [G]$. Then, $N$ is abelian (subgroup of any $P_2$ in $N$ is $G$).

$G/N$ has order 6. Say $G/N$ has composition series $G/N \supset H \supset \{e\}$.

Then, $G \cong f^{-1}(H) \supset f^{-1}(e) = N \supset \{e\}$ is a normal series with abelian quotients.

\[
N \cong \bigcap_{P_2 \in P_2} \text{Stab}_G(P_2) = \bigcap_{P_2 \in P_2} N_{G}(P_2) = \bigcap_{P_2 \in P_2} P_2 = \{e\} \supset \bigcap_{P_2 \in P_2} P_2 = \{e\} \supset \{e\}.
\]

$[G : N_0(P_2)] = \#P_2 = 2$.

$N_0(P_2) = P_2.$
**Digression:** Say \( G/N \approx H. \) Assume \( N \) is abelian. Then conjugation action of \( G \) on \( N \) descends to \( H \).

Let \( s: H \rightarrow G \) be a "section." (inverse of quotient map)

\( G \) is union of cosets \( \leftrightarrow \) every element of \( G \) has a unique rep'\( n \) \( g = \text{sch}(n) \) for some \( h \in H, n \in N \)

Then \( a_1, a_2 = s(h_1)h_1, s(h_2)h_2 \),
\[
  s(h_1)h_1, s(h_2)h_2 = s(h_1) s(h_2). s(h_1)^{-1} (h_2^n h_1 h_2) . h_2
\]

\( \uparrow \)

\( \text{action of } \) \( H \) \( \uparrow \)

\( x^n \), \( x \) only

\( n \in N \) depends on class \( \phi(x) \mod N \)

\( \) (assume given \( H, N, \phi \), action of \( H \) on \( N \))

also \( s(h_1), s(h_2), s(h_1 h_2), s(h_1 h_2) \cdot f(h_1, h_2) \)

\( \) where \( f: H \times H \rightarrow N \)

so \( s(h_1)h_1, s(h_2)h_2 = s(h_1 h_2) \cdot [f(h_1, h_2)(h_2^n h_1 h_2) . h_2] \)

\( \) bottom line: multi table of \( G \) determined by \( f \).

\( \) (treat \( s(h) \) as formal symbols)

Wlog assume \( s(e) = e \), \( s(h^{-1}) = s(h)^{-1} \).

\( \phi \) Any \( f \) defines a binary op.

\( \) easy to check when \( s(e) = e \) is id, inverses

\( \) real issue: associativity

\( \) op. is associative \( \iff \forall x, y, z \in H: \) \( x \cdot (y \cdot z) = (x \cdot y) \cdot z \)

\( + f(x, y, z) = f(x, y) = 0 \)
Call the set of such $f \in \mathbb{Z}^2(\mathbb{H}; N)$ abelian $g \in \mathbb{N}^{H \times H}$ if we replace $s$ with $s'$ where $s'(h) = s(h) - n(h) m(h) n(h)^{-1}$ and if appropriately get same $g$. Let $s'$ be $g \in \mathbb{Z}^2(\mathbb{H}; N)$, s.t. extension $s' : \mathbb{Z}^2(\mathbb{H}; N) / \mathbb{Z}^2(\mathbb{H}; H) \rightarrow H^2(\mathbb{H}; H) \subseteq H^2(\mathbb{H}; N)$