Lecture XXX: Solvable groups

Recall We introduced the notion of a composition series of a group G

- Composition series = descending chain of normal subgroups

$$\Sigma: \quad G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \quad \trianglerighteq G_n = \{e\}$$

- Jordan-Hölder series = strict composition series (ie all $\not\trianglerighteq$) & maximal with respect to refinements.

Certain composition series can be constructed via "commutators".

§ 30.1 Commutators:

Definition: Let G be a group and $x, y \in G$. The commutator between x & y is

$$[x,y] := x y x^{-1} y^{-1} \in G$$

Note: $[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = y x y^{-1} x^{-1} = [y,x]$

Definition: Given $A, B \subseteq G$ subsets, $[A,B] := \langle [a,b] : a \in A, b \in B \rangle$

Lemma: If $A, B \trianglelefteq G \Rightarrow [A,B] \trianglelefteq G$. In particular, $[G,G] \trianglelefteq G$

Proof: Given $x = [a,b] = aba^{-1}b^{-1}$ with $a \in A$, $b \in B$ and $g \in G$ we have

$$x[a,b]x^{-1} = x a b a^{-1} b^{-1} x^{-1} = x a x^{-1} x b x^{-1} x a x^{-1} x b^{-1} x^{-1} = [xax^{-1}, xbx^{-1}]$$

$$\left.\begin{array}{l} A \trianglelefteq G \Rightarrow x a x^{-1} \in A \ \forall x \\ B \trianglelefteq G \Rightarrow x b x^{-1} \in B \ \forall x \end{array}\right\} \Rightarrow x[a,b]x^{-1} \in [A,B].$$

In general, any $x \in [A,B]$ has the form $x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$ for $\varepsilon_i = \pm 1$

$x_i = [a_i, b_i]$ with $a_i \in A$, $b_i \in B$ for $i = 1, \ldots, n$

$\Rightarrow g x g^{-1} = (g x_1 g^{-1})^{\varepsilon_1} \cdots\cdots (g x_n g^{-1})^{\varepsilon_n} \in [A,B] \quad \forall g \in G$ since $g x_i g^{-1} \in [A,B]$

Hence, $[A,B] \trianglelefteq G$ $\square$

§ 30.2 Commutator Series:

Alternative name: Derived series.

⚠ The word "derived" has changed its meaning these days. We have things like "derived categories", "derived functors", "derived Algebraic Geometry", etc.
So it is probably better to use "commutator series" for this construction.

Let G be a group. Take $G^{(0)} = G$, $G^{(1)} = [G, G]$, $G^{(2)} = [G^{(1)}, G^{(1)}]$, ...
$G^{(\ell+1)} = [G^{(\ell)}, G^{(\ell)}]$ ....

We obtain a (perhaps infinite) series:

$$\Sigma: \quad G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots\cdots$$

Definition: The series Σ is called the <u>commutator series</u> of G.

⚠ The series Σ may not end in $\{e\}$ even if G is finite.

Lemma: For any group H, the quotient group $H/[H,H]$ by $[H,H] \trianglelefteq H$ is abelian.

It is the largest abelian group which admits a surjective group homomorphism from H.
More precisely, if A is any abelian group and $f: H \longrightarrow A$ is a group homomorphism, then $[H:H] \subset \mathrm{Ker}(f)$ &

$$\begin{tikzcd} H \arrow[r, "f"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & A \\ H/[H,H] \arrow[ur, "\exists ! F"'] & \end{tikzcd}$$

Furthermore, if $A = H/[H,H]$ & $f = \pi$, then $\mathrm{Ker}(f) = [H,H]$.

Proof: Pick $x, y \in H$. We show $[x[H,H], y[H,H]] = e[H,H]$ in $H/[H,H]$. Indeed:

$$x[H,H]\, y[H,H]\, (x[H,H])^{-1} (y[H,H])^{-1} = xyx^{-1}y^{-1}[H,H] = [x,y][H,H] = e[H,H]$$

So $H/[H,H]$ is abelian.

If $f: H \longrightarrow A$ is a group homomorphism & A is abelian, then for any $x, y \in H$ we have $f([x,y]) = [f(x), f(y)] = e$ because A is abelian.
Thus $[x,y] \in \mathrm{Ker}\, f$ $\forall x, y \in H$. Since $\mathrm{Ker}\, f$ is a group, $[H,H] \leq \mathrm{Ker}(f)$.
By the 1st Isomorphism Theorem f factors through $H/[H,H]$, as we wanted. $\square$

Corollary: The associated graded pieces $\left(G^{(\ell)}/G^{(\ell+1)}\right)_{\ell \geq 0}$ of the commutator series are abelian.

§ 30.3 Examples:

① G abelian $\Rightarrow$ $G^{(1)} = [G,G] = \{e\} \Rightarrow G^{(\ell)} = \{e\} \quad \forall \ell$

② $G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \quad a, c \neq 0,\ b \text{ arbitrary} \right\} \subseteq GL_2(\mathbb{C})$

$$\left[\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} \right] = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} \begin{bmatrix} 1/a & -b/(ac) \\ 0 & 1/c \end{bmatrix} \begin{bmatrix} 1/a' & -b'/(a'c') \\ 0 & 1/c' \end{bmatrix}$$

$$= \begin{bmatrix} aa' & ab'+bc' \\ 0 & cc' \end{bmatrix} \begin{bmatrix} 1/aa' & -b'/(aa'c') - b/(acc') \\ 0 & 1/cc' \end{bmatrix} = \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$$

where $d = \dfrac{-b'}{c'} - \dfrac{ba'}{cc'} + \dfrac{ab'}{cc'} + \dfrac{b}{c} = \dfrac{bc' - b'c + ab' - ba'}{cc'}$

Key: any value in $\mathbb{C}$ has this form ($a = a' = 1$, $c = c' = -1$, $b' = 0$, b arbitrary

$d = \frac{1}{1}(-2b) = -2b$ $\quad b$ free)

Conclusion: $G^{(1)} = [G,G] = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \quad x \in \mathbb{C} \right\}$

This is an abelian group $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}$ & $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}$

$\Rightarrow G^{(2)} = [G^{(1)}, G^{(1)}] = \{e\}$

Thus, the composition series of this group is $G^{(0)} = G \trianglerighteq \underset{(\mathbb{C},+)}{\underset{\cong}{G^{(1)}}} \trianglerighteq G^{(2)} = \{e\}$

③ Assume G is simple, non-abelian (Example: A_5, we will see this in a future lecture)

Lemma: If G is a simple, non abelian group, then $G^{(\ell)} = G \quad \forall \ell$. In particular, the commutator series is never ending (in $\{e\}$).

Proof: $[G,G] \trianglelefteq G$ by Lemma § 30.1

But $[G,G] \neq \{e\}$ because G is non-abelian ($\exists\, a, b \in G$ with $ab \neq ba$, ie $e \neq [a;b] \in [G,G]$)

As G is simple, we conclude that $[G,G] = G$.

§ 30.4 Solvable groups:

Definition: We say a group G is <u>solvable</u> if for some $n \geq 0$, we have $G^{(n)} = \{e\}$.

Examples: ① & ② are solvable

A_n for $n \geq 5$ or any simple non-abelian group (as in ③) is not solvable.

The term "solvable" originated in the concept of "solvability by radicals of a polynomial equation". You will learn more about it in Honors Algebra II (Galois Theory), but here is a rough dictionary to illustrate this:

- $ax^2+bx+c=0$ $(a\neq 0)$ can be solved $x = \dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$ in terms of
  - polynomials in a, b, c (eg b^2-4ac)
  - radicals (square roots) (eg $\sqrt{b^2-4ac}$)

The reason for this will turn out to be $\mathbb{Z}/2\mathbb{Z} \simeq S_2$ is solvable

- $S_3 \cong D_6 = \langle r, s \mid r^3 = s^2 = 1,\ srs = r^{-1} \rangle$

$$(1,2,3) \xleftarrow{\varphi} r$$
$$(12) \longleftarrow s$$

$(12)(123)(12) = (213) = (123)^{-1}$, $(123)^3 = 1$, $(1,2)^2 = 1$

$$\begin{cases} \varphi(sr^j) = (12)(123)^j = id & \text{is impossible since } \operatorname{ord}(123)^j = 1 \text{ or } 3 \\ \varphi(r^j) = (123)^j = id \iff j=0. & \operatorname{ord}(12) = 2 \end{cases}$$

$\Rightarrow \varphi$ is injective gp homomorphism. Since $|S_3| = |D_6| = 6 \Rightarrow \varphi$ is an isomorphism

$[D_6, D_6] = ?$ $\quad [s,r] = srs^{-1}r^{-1} = r^{-1}r^{-1} = r^{-2} = r \in G^{(1)}$

$[s^ir^j, s^kr^l] = s^ir^js^kr^l r^{-j}s^{-i}r^{-l}s^{-k}$

4 cases: $i=k=0$ $\quad [r^j, r^l] = e$

$i=1, k=0$ $\quad [sr^j, r^l] = sr^jr^l r^{-j}s^{-1}r^{-l} = sr^ls^{-1}r^{-l} = sr^lsr^{-l} = \underset{\in \langle r\rangle}{r^{-2l}}$

$i=0, k=1$ $\quad [r^j, sr^l] = r^jsr^lr^{-j}r^{-l}s = r^jsr^{-j}s = r^jr^j = \underset{\in\langle r\rangle}{r^{2j}}$

$i=1=k$ $\quad [sr^j, sr^k] = sr^jsr^kr^{-j}s^{-1}r^{-k}s^{-1} = r^{-j}r^kr^{-j}sr^{-k}s = r^kr^k = \underset{\in\langle r\rangle}{r^{2k}}$

$\Rightarrow [D_6, D_6] \subseteq \langle r \rangle$

$\Rightarrow G^{(1)} = \langle r \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ abelian

Conclude: $S_3 \simeq D_3 = G^{(0)} \trianglerighteq G^{(1)} \simeq \mathbb{Z}/3\mathbb{Z} \trianglerighteq G^{(2)} = \{e\}$ is also solvable

This implies that any degree 3 polynomial equation can be solved.

Example: $x^3 - 3Ax + B = 0$ is "solved" $x = r + \frac{A}{r}$ where $r = \left(\dfrac{B \pm \sqrt{B^2-4A^3}}{2}\right)^{1/3}$

Here: $\sqrt{\ }$ & $(\ )^{1/3}$ are the radicals

- S_4 is also solvable (We'll see this in a future lecture).
  Read about solving degree 4 equations if you are interested.
- S_5 (& S_n for all $n \geq 5$) are <u>not</u> solvable. This will imply that a general degree 5 equation has no "explicit solution by radicals" like the ones described above.