21.05.2024 ①

Algebra Lect. 35

A. Ram

Solvable groups

Let G be a group. Let $x,y\in G$.

The commutator of x and y is

$$[x,y]=xyx^{-1}y^{-1}.$$

"The axiomatic method has many advantages over honest work"
B. Russell

The derived subgroup of G is

$$[G,G]=\{[x,y]\ |\ x,y\in G\}$$

The group $[G,G]$ is always a normal subgroup of G. The abelianization of G is

$$G^{ab}=\frac{G}{[G,G]}.$$

The derived series of G is

$$G=D^0(G)\supseteq D^1(G)\supseteq \cdots,$$

where $D^{i+1}(G)=[D^iG,D^iG]$.

The group G is solvable if there exists $n\in\mathbb{Z}_{>0}$ such that $D^n(G)=1$.

Alternatively, the group G is solvable if there is a composition series with

$G\supseteq G_1\supseteq\cdots$ with G_i/G_{i+1} abelian.

The group A_5 is the smallest nonsolvable group. All subgroups of S_4 and S_3 and S_2 are solvable.

Solutions of equations

Quadratic: If α is a root of $x^2+bx+c=0$ then

$$\alpha \in \{ -b+\sqrt{b^2-4ac},\ -b-\sqrt{b^2-4ac} \}$$

Cubic: Let α be a root of

$$f(x) = x^3 + a_2 x^2 + a_1 x + a_0.$$

Let $y = x - \frac{1}{3} a_2$. Then

$$f(x) = y^3 + py + q$$

where

$$p = \frac{a_2^2}{3} - \frac{2a_2^2}{3} + a_1 \quad \text{and} \quad q = \frac{a_2^3}{4} - \frac{a_1 a_2}{3} + a_0$$

Then

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

A <u>constructible extension of $\mathbb{Q}$</u> is a field $\mathbb{K} \supseteq \mathbb{Q}$ such that there exist elements $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$ such that $\mathbb{K} \subseteq \mathbb{R}$ and

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha_1, \alpha_2) \subseteq \cdots \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_r) = \mathbb{K}$$

and $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots \alpha_{i-1})$ for $i \in \{1, \ldots, r\}$.

A <u>constructible number</u> is $\alpha \in \mathbb{R}$ such that α is in a constructible extension $\mathbb{K}$ of $\mathbb{Q}$.

A <u>radical extension of $\mathbb{Q}$</u> is a field $\mathbb{K} \supseteq \mathbb{Q}$ such that there exist elements $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$ and $n_1, \ldots, n_r \in \mathbb{Z}_{>0}$ such that

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \cdots \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_r) = \mathbb{K}$$

and $\alpha_i^{n_i} \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ for $i \in \{1, \ldots, r\}$.

A polynomial $f(x) \in \mathbb{Q}[x]$ is <u>solvable by radicals</u> if the splitting field of f over $\mathbb{Q}$ is contained in a radical extension of $\mathbb{Q}$.

$$\begin{array}{c} \mathbb{K} \text{ radical} \\ \cup\!| \\ S_f \\ | \\ \mathbb{Q} \end{array}$$

<u>Theorem</u> Let $f(x) \in \mathbb{Q}[x]$ and let S_f be the splitting field of $f(x)$ over $\mathbb{Q}$

Then

$f(x)$ is solvable by radicals

if and only if

$\mathrm{Aut}_{\mathbb{Q}}(S_f)$ is a solvable group.

<u>Proof</u> $\Leftarrow$: Let $n = \deg(f(x))$,

| Assume $\mathrm{Aut}_{\mathbb{Q}}(S_f)$ is a solvable group.

~~Case 1~~: Let $\omega = e^{2\pi i/n}$.

Then

$$\begin{array}{c} S_f(\omega) \\ | \\ \mathbb{Q}(\omega) \\ | \\ \mathbb{Q} \end{array}$$

and $S_f(\omega)$ is the splitting field of $f(x)$ over $\mathbb{Q}(\omega)$

The map

$$\mathrm{Aut}_{\mathbb{Q}(\omega)}(S_f(\omega)) \longrightarrow \mathrm{Aut}_{\mathbb{Q}}(S_f)$$

$$\sigma \longmapsto \sigma|_{S_f}$$

is injective.

Since $\mathrm{Aut}_{\mathbb{Q}}(S_f)$ is solvable then

$\mathrm{Aut}_{\mathbb{Q}(\omega)}(S_f(\omega))$ is solvable.

Let
$G = \mathrm{Aut}_{\mathbb{Q}(\omega)}(\mathbb{F}(\omega))$.

Since G is solvable then there is a series

$G \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}$ with

G_i a normal subgroup of G_{i-1} and

G_i / G_{i-1} cyclic.

Let
$\mathbb{Q}(\omega) = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r$ be the corresponding fixed fields. Since

G_i is a normal subgroup of G_{i-1}

then

$\mathbb{F}_i$ is a splitting field over $\mathbb{F}_{i-1}$

Since G_i / G_{i-1} is cyclic then

$\mathbb{F}_i$ is the splitting field over $\mathbb{F}_{i-1}$ of a polynomial $x^{n_i} - b_i \in \mathbb{F}_{i-1}[x]$.

So $b_i = \alpha_i^{n_i}$, where $\alpha_i \in \mathbb{F}_i$ and $\mathbb{F}_i = \mathbb{F}_{i-1}(\alpha_i)$.

So $f(x)$ is solvable by radicals.

$\Rightarrow$: Assume that $f(x)$ is solvable by radicals. Let $\mathbb{K}$ be a splitting field of $f(x)\cdot(x^n-1)=g(x)$, where $n=\deg(f(x))$. Then $\mathbb{K}$ is a radical extension

$$\begin{array}{lll}
\mathbb{K}=\mathbb{Q}(\alpha_1,\dots,\alpha_r) & & \{1\} \\
\cup| & & \cap| \\
\mathbb{F}_{r-1}=\mathbb{Q}(\alpha_1,\dots,\alpha_{r-1}) & H & G_{r-1} \\
\cup| & & \vdots \\
\vdots & & \cap| \\
\cup| & & G_1 \\
\mathbb{F}_1=\mathbb{Q}(\alpha_1) & & \cap| \\
\cup| & & G \\
\mathbb{F}_0=\mathbb{Q}(\omega) & & \\
\cup| & & \\
\mathbb{Q} & &
\end{array}$$

$\mathbb{S}_f$

The series $G\supseteq G_1\supseteq\cdots\supseteq G_{r-1}\supseteq\{1\}$ has G_i/G_{i-1} being the $\mathrm{Aut}_{\mathbb{F}_i}(\mathbb{F}_i(\alpha_i))$ which is cyclic since $\mathbb{F}_{i-1}(\alpha_i)$ is the splitting field of $x^{n_i}-b_i\in\mathbb{F}_{i-1}[x]$ over $\mathbb{F}_{i-1}$ and thus

G_i/G_{i-1} is cyclic.

So G is solvable.

Then $H=\mathrm{Aut}_{\mathbb{Q}}(\mathbb{S}_f)\cong\dfrac{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})}{\mathrm{Aut}_{\mathbb{S}_f}(\mathbb{K})}$ is also solvable since a quotient of G is also solvable.