04.03.2024
Algebra Lect 4
A. Ram

①

Theorem of the primitive element

Proposition Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and let $\alpha, \beta \in \mathbb{K}$. Assume that $\mathbb{K}$ contains all the roots of

$$m_{\alpha,\mathbb{F}}(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$$

$$m_{\beta,\mathbb{F}}(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_s)$$

and assume $\alpha = \alpha_1$ and $\beta = \beta_1$.
Let $c \in \mathbb{F}$ such that $c \neq 0$ and

$$c \notin \left\{ \frac{-(\beta-\beta_j)}{\alpha-\alpha_i} \;\middle|\; \begin{matrix} i \in \{2,\ldots,r\} \\ j \in \{2,\ldots,s\} \end{matrix} \right\}$$

Then
$$\mathbb{F}(\alpha,\beta) = \mathbb{F}(\alpha + c\beta).$$

Recall:
$\mathbb{F}(\alpha,\beta)$ is the smallest field containing $\mathbb{F}$ and α and β

$\mathbb{F}(\alpha+c\beta)$ is the smallest field containing $\mathbb{F}$ and $\alpha + c\beta$

$$\ker(ev_{\alpha,\mathbb{F}}) = m_{\alpha,\mathbb{F}}(x)\mathbb{F}[x]$$
$$\ker(ev_{\beta,\mathbb{K}}) = m_{\beta,\mathbb{F}}(x)\mathbb{F}[x].$$

<u>Theorem</u> Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$. Let $\mathbb{K}$ be the splitting field of $f(x)$ over $\mathbb{F}$. Then there exists $\gamma \in \mathbb{K}$ such that

$$\mathbb{K} = \mathbb{F}(\gamma)$$

<u>Proof sketch</u> In $\mathbb{K}[x]$,

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$$

and

$$\begin{array}{l}
\mathbb{K} = \mathbb{F}(\alpha_1, \dots \alpha_k) = \mathbb{F}(\gamma_{k-1}, \alpha_k) = \mathbb{F}(\gamma_k). \\
\cup| \\
\mathbb{F}(\alpha_1, \dots, \alpha_{k-1}) = \mathbb{F}(\gamma_{k-2}, \alpha_{k-1}) = \mathbb{F}(\gamma_{k-1}) \\
\cup| \\
\vdots \\
\cup| \\
\mathbb{F}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{F}(\gamma_2, \alpha_3) = \mathbb{F}(\gamma_3) \\
\cup| \\
\mathbb{F}(\alpha_1, \alpha_2) = \mathbb{F}(\gamma_2) \\
\cup| \\
\mathbb{F}(\alpha_1) \\
\cup| \\
\mathbb{F}
\end{array}$$

Let $\gamma = \gamma_k$. /.

<u>Example</u> Let $\zeta = e^{2\pi i/3}$

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{Q}(\sqrt[3]{2},\zeta) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[drr, dash] & \mathbb{Q}(\sqrt[3]{2}\zeta) \arrow[dr, dash] & \mathbb{Q}(\sqrt[3]{2}\zeta^2) \arrow[d, dash] & \mathbb{Q}(\zeta) \arrow[dl, dash] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

$$m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3-2 = (x-\sqrt[3]{2})(x-\sqrt[3]{2}\zeta)(x-\sqrt[3]{2}\zeta^2)$$

$$m_{\zeta,\mathbb{Q}}(x) = x^2+x+1 = (x-\zeta)(x-\zeta^2)$$

Pick $c \in \mathbb{Q}$ such that $c \neq 0$ and

$$c \notin \left\{ \frac{-(\zeta-\zeta^2)}{\sqrt[3]{2}-\sqrt[3]{2}\zeta}, \frac{-(\zeta-\zeta^2)}{\sqrt[3]{2}-\sqrt[3]{2}\zeta^2} \right\}$$

Then $\mathbb{Q}(\sqrt[3]{2},\zeta) = \mathbb{Q}(\sqrt[3]{2}+c\zeta)$.

In particular, $\mathbb{Q}(\sqrt[3]{2},\zeta) = \mathbb{Q}(\sqrt[3]{2}+\zeta)$.

<u>Note:</u> If $\mathbb{K} = \mathbb{F}(\gamma)$ and $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ then $\sigma(\gamma)$ is a root of $m_{\gamma,\mathbb{F}}(x)$.

<u>Because</u> σ fixes $m_{\gamma,\mathbb{F}}(x)$
and γ is a root of $m_{\gamma,\mathbb{F}}(x)$
and σ takes γ to $\sigma(\gamma)$.

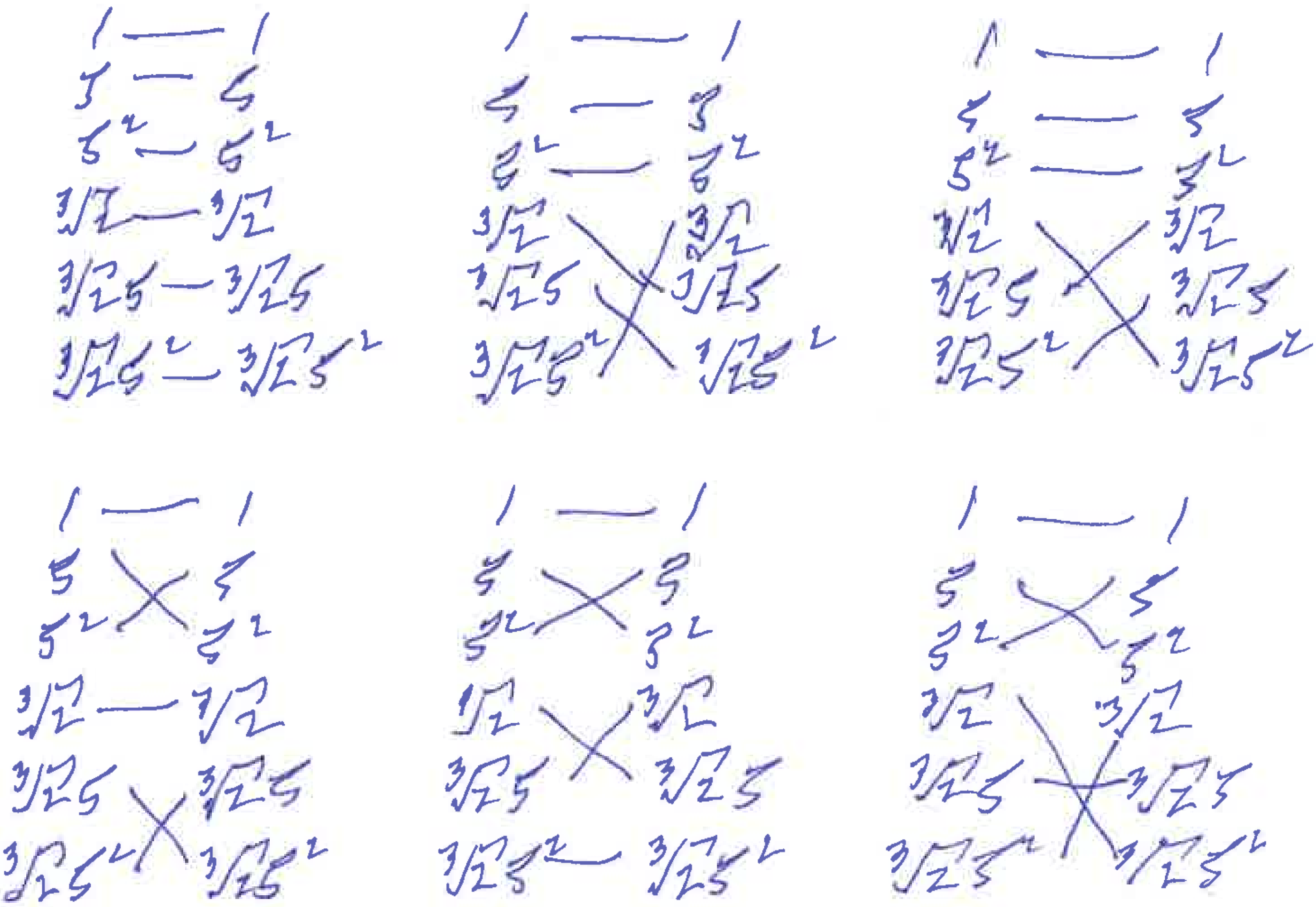
Back to our example

$\mathbb{Q}(\sqrt[3]{2},\zeta)$ has $\mathbb{Q}$-basis $\{1,\zeta,\zeta^2,\sqrt[3]{2},\sqrt[3]{2}\zeta,\sqrt[3]{2}\zeta^2\}$

and

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2},\zeta)) = \{\equiv, \asymp, \bar{\times}, \ast, \ddot{\times}, \times\} = G$$

determined by



Let $\gamma = \sqrt[3]{2}+\zeta$.

What is $m_{\gamma,\mathbb{F}}(x)$?

$G\gamma = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$ where

$\gamma_1 = \gamma = \sqrt[3]{2} + \zeta$, $\quad \gamma_4 = \underline{\times}\,\gamma = \sqrt[3]{2}\zeta + \zeta^2$

$\gamma_2 = \cancel{\times}\,\gamma = \sqrt[3]{2}\zeta + \zeta$, $\quad \gamma_5 = \overline{\times}\,\gamma = \sqrt[3]{2} + \zeta^2$

$\gamma_3 = \times\,\gamma = \sqrt[3]{2}\zeta^2 + \zeta$, $\quad \gamma_6 = \times\,\gamma = \sqrt[3]{2}\zeta^2 + \zeta^2$

Now, all elements of $G\gamma$ are roots of $m_{\gamma,\mathbb{Q}}(x)$

$$\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}+\zeta)) = 6 = \deg(m_{\gamma,\mathbb{Q}}(x))$$

So

$$m_{\gamma,\mathbb{Q}}(x) = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3)(x-\gamma_4)(x-\gamma_5)(x-\gamma_6)$$
$$= x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$$

<u>Galois group of a Galois extension</u>

Let $\mathbb{K} \supseteq \mathbb{F}$ be a Galois extension.
This means that there exists

$$f(x) \in \mathbb{F}[x]$$

such that $\mathbb{K}$ is the splitting field of f over $\mathbb{F}$.

Let $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ so that

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k).$$

and $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_k)$.

Then there exists $\gamma \in \mathbb{F}$ such that

$$\mathbb{K} = \mathbb{F}(\gamma).$$

Then

$$\dim_{\mathbb{F}}(\mathbb{K}) = \deg(m_{\gamma,\mathbb{F}}(x)) = |\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})| = k$$

and elements $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ permute the roots of $m_{\gamma,\mathbb{F}}(x)$,

$$m_{\gamma,\mathbb{F}}(x) = (x-\gamma_1)(x-\gamma_2)\cdots(x-\gamma_k)$$

where $\gamma = \gamma_1$. If $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ then

$$G\gamma = \{\gamma_1, \ldots, \gamma_k\} \text{ and } m_{\gamma,\mathbb{F}}(x) = \prod_{\beta \in G\gamma}(x-\beta).$$

The set $G\gamma$ is the G-orbit of γ.

04.03.2024 ②

Algebra Lect 4

A. Ram

<u>Proof</u> To show: (a) $\mathbb{F}(\alpha+c\beta) \subseteq \mathbb{F}(\alpha,\beta)$

(b) $\mathbb{F}(\alpha,\beta) \subseteq \mathbb{F}(\alpha+c\beta)$

(a) To show: $\alpha+c\beta \in \mathbb{F}(\alpha,\beta)$.

Since $\alpha \in \mathbb{F}(\alpha,\beta)$ and $\beta \in \mathbb{F}(\alpha,\beta)$ and $c \in \mathbb{F}$ then
$\alpha+c\beta \in \mathbb{F}(\alpha,\beta)$.

So $\mathbb{F}(\alpha,\beta) \supseteq \mathbb{F}(\alpha+c\beta)$

(b) To show: (ba) $\alpha \in \mathbb{F}(\alpha,\beta)$

(bb) $\beta \in \mathbb{F}(\alpha,\beta)$

(ba) To show: $m_{\alpha,\mathbb{F}(\alpha,\beta)}(x) = x-\alpha$.

Since

$m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}(\alpha,\beta)[x]$ and $h(x) = m_{\beta,\mathbb{F}}(\beta+c\alpha-cx)$

$h(x) = m_{\beta,\mathbb{F}}(\beta+c\alpha-cx) \in \mathbb{F}(\alpha,\beta)[x]$

and $m_{\alpha,\mathbb{F}}(\alpha) = 0$ and $h(\alpha) = 0$

then $m_{\alpha,\mathbb{F}(\alpha,\beta)}(x)$ is a common divisor of
$m_{\alpha,\mathbb{F}}(x)$ and $h(x)$.

Then

$m_{\alpha,\mathbb{F}}(x) = (x-\alpha_1)\cdots(x-\alpha_r)$

$h(x) = (\beta+c\alpha-cx-\beta_1)\cdots(\beta+c\alpha-cx-\beta_s)$

Since $c^{-1}\beta+\alpha-c^{-1}\beta_j \neq \alpha_i$ except when $i=1$ and $j=1$ then $\gcd(m_{\alpha,\mathbb{F}}(x), h(x)) = x-\alpha$.