Splitting fields exist

Algebra Lect. 30 A. Raun

Let $F$ be a field and let $f(x) \in F[x]$,

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0.$$

The splitting field of $f$ over $F$ is a pair $(S_f, \iota)$ such that

(a) $S_f$ is a field and $\iota : F \to S_f$ is a field morphism and there exist $\alpha_1, \ldots, \alpha_d \in S_f$ such that

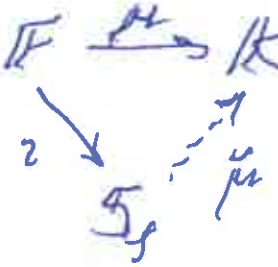
$$f(x) = (x-\alpha_1)\cdots(x-\alpha_d) \text{ in } S_f[x].$$

(b) If $K$ is a field and $\mu : F \to K$ is a field morphism and there exist $\alpha_1, \ldots, \alpha_d \in K$ such that

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_d) \text{ in } S_f[x]$$

then there exists $\tilde{\mu} : S_f \to K$ such that

$$\mu = \tilde{\mu} \circ \iota$$



In English:

The splitting field of $f$ over $\mathbb{F}$ is the smallest field $\mathbb{S}_f$ containing $\mathbb{F}$ such that there exist $\alpha_1, \dots, \alpha_d \in \mathbb{S}_f$ such that

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_d) \text{ in } \mathbb{S}_f[x].$$

The splitting field of the finite set

$$\mathcal{F} = \{f_1(x), \dots, f_s(x)\} \subseteq \mathbb{F}[x]$$

over $\mathbb{F}$ is the splitting field of the single polynomial

$$f(x) = f_1(x) \cdots f_s(x).$$

Since

$$\mathbb{S}_f = \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_d) \text{ then } \dim_{\mathbb{F}}(\mathbb{S}_f) \leq d!$$

## Elementary symmetric functions

Let $z_1, \dots, z_d$ be variables. Then

$$(x-z_1)(x-z_2)\cdots(x-z_d)$$
$$= x^d - e_1(z_1, \dots, z_d)x^{d-1} + e_2(z_1, \dots, z_d)x^{d-2}$$
$$+ \cdots + (-1)^{d-1} e_{d-1}(z_1, \dots, z_d)x + (-1)^d e_d(z_1, \dots, z_d).$$

where

$$e_r(z_1,\dots,z_d) = \sum_{1\le i_1<\dots<i_r\le d} z_{i_1}\cdots z_{i_r}.$$

For example, $(x-z_1)(x-z_2)(x-z_3)$

$$= x^3 - (z_1+z_2+z_3)x^2 + (z_1z_2+z_1z_3+z_2z_3)x - z_1z_2z_3$$

and

$$e_1(z_1,z_2,z_3) = z_1+z_2+z_3,$$

$$e_2(z_1,z_2,z_3) = z_1z_2+z_1z_3+z_2z_3, \quad e_3(z_1,z_2,z_3) = z_1z_2z_3$$

<u>Proposition</u> Let $F$ be a field and let

$$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0 \text{ in } F[x]$$

so that $a_0, a_1, \dots, a_{d-1} \in F$. Let

$$R = F[z_1,\dots,z_d]$$

and let $I$ be a maximal ideal of $R$ containing the set

$$\left\{ \begin{array}{l} e_1(z_1,\dots,z_d) - a_{d-1}, \\ e_2(z_1,\dots,z_d) + a_{d-2}, \\ \vdots \\ e_{d-1}(z_1,\dots,z_d) + (-1)^{d-1}a_1, \\ e_d(z_1,\dots,z_d) + (-1)^d a_0 \end{array} \right\}$$

13.05.2024 (4)

Algebra Lect. 30

A. Ram

Let

$$S_f = \frac{F[z_1, \dots, z_d]}{I}.$$

Then $S_f$ is a field containing $F$ and

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_d) \text{ in } S_f[x]$$

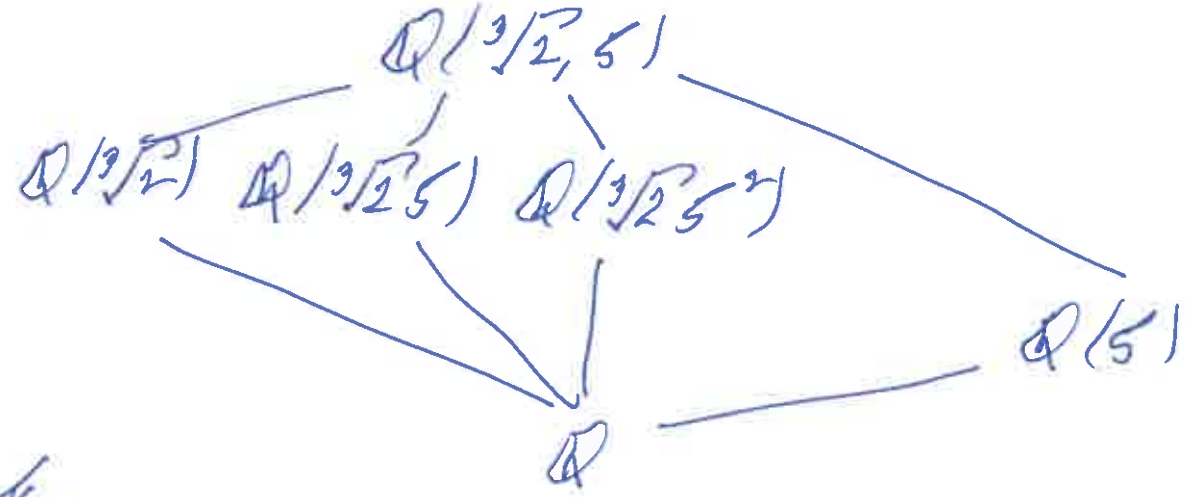
where $\alpha_j$ is the image of $z_j$ in $S_f$

$$F[z_1, \dots, z_d] \longrightarrow S_f = \frac{R}{I}$$

$$z_j \longmapsto \alpha_j = z_j + I.$$

Then $S_f$ is the splitting field of $f$ over $F$.

Example $\zeta = e^{2\pi i/3}$




Then

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

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

13.05.2024 (5)

# Making automorphisms explicit

Algebra Lect. 30

A. Ram

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{5})) = \left\{ \begin{array}{l} \mathbb{Q}(\sqrt{5}) \xrightarrow{id} \mathbb{Q}(\sqrt{5}) \\ \quad \sqrt{5} \longmapsto \sqrt{5} \\ \quad -\sqrt{5} \longmapsto -\sqrt{5}, \end{array} \right. \quad \left. \begin{array}{l} \mathbb{Q}(\sqrt{5}) \xrightarrow{\tau} \mathbb{Q}(\sqrt{5}) \\ \quad \sqrt{5} \longmapsto -\sqrt{5} \\ \quad -\sqrt{5} \longmapsto \sqrt{5} \end{array} \right\}$$

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2},\sqrt{5})) = \left\{ \begin{array}{l} \mathbb{Q}(\sqrt[3]{2},\sqrt{5}) \xrightarrow{id} \mathbb{Q}(\sqrt[3]{2},\sqrt{5}) \\ \quad \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \quad \sqrt[3]{2}\sqrt{5} \longmapsto \sqrt[3]{2}\sqrt{5} \\ \quad \sqrt[3]{2}(\sqrt{5})^2 \longmapsto \sqrt[3]{2}(\sqrt{5})^2 \end{array} \right.$$

$\mathbb{Q}(\sqrt[3]{2},\sqrt{5}) \xrightarrow{\tau} \mathbb{Q}(\sqrt[3]{2},\sqrt{5})$

$\sqrt[3]{2} \longmapsto \sqrt[3]{2}$, $\sqrt[3]{2}\sqrt{5} \longmapsto -\sqrt[3]{2}\sqrt{5}$, $\sqrt[3]{2}(\sqrt{5})^2 \longmapsto \sqrt[3]{2}(\sqrt{5})^2$

$\mathbb{Q}(\sqrt[3]{2},\sqrt{5}) \xrightarrow{\tau^2} \mathbb{Q}(\sqrt[3]{2},\sqrt{5})$

$\sqrt[3]{2} \longmapsto \sqrt[3]{2}$, $\sqrt[3]{2}\sqrt{5} \longmapsto \sqrt[3]{2}\sqrt{5}$, $\sqrt[3]{2}(\sqrt{5})^2 \longmapsto -\sqrt[3]{2}(\sqrt{5})^2$

$\mathbb{Q}(\sqrt[3]{2},\sqrt{5}) \xrightarrow{\sigma} \mathbb{Q}(\sqrt[3]{2},\sqrt{5})$

$\sqrt[3]{2} \longmapsto \sqrt[3]{2}$, $\sqrt[3]{2}\sqrt{5} \longmapsto \sqrt[3]{2}(\sqrt{5})^2$, $\sqrt[3]{2}(\sqrt{5})^2 \longmapsto \sqrt[3]{2}\sqrt{5}$

$\mathbb{Q}(\sqrt[3]{2},\sqrt{5}) \longrightarrow \mathbb{Q}(\sqrt[3]{2},\sqrt{5})$

$\sqrt[3]{2} \longmapsto \sqrt[3]{2}$, $\sqrt[3]{2}\sqrt{5} \longmapsto -\sqrt[3]{2}(\sqrt{5})^2$, $\sqrt[3]{2}(\sqrt{5})^2 \longmapsto -\sqrt[3]{2}\sqrt{5}$

$\mathbb{Q}(\sqrt[3]{2},\sqrt{5}) \longrightarrow \mathbb{Q}(\sqrt[3]{2},\sqrt{5})$

$\sqrt[3]{2} \longmapsto \sqrt[3]{2}$, $\sqrt[3]{2}\sqrt{5} \longmapsto \sqrt[3]{2}\sqrt{5}$, $\sqrt[3]{2}(\sqrt{5})^2 \longmapsto \sqrt[3]{2}(\sqrt{5})^2$

A $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt[3]{2})$ is

$B = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

A $\mathbb{Q}(\sqrt[3]{2})$-basis of $\mathbb{Q}(\sqrt[3]{2}, 5)$ is

$C = \{1, 5\}$ (note that $5^2 = -5 - 1$).

A $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt[3]{2}, 5)$ is

$BC = \{1, \sqrt[3]{2}, \sqrt[3]{4}, 5, \sqrt[3]{2}5, \sqrt[3]{4}5\}$.