Galois Theory 2.

Algebraic extension:

K/F field extension $\alpha \in K$ is algebraic$/F$ if $\exists$ $p(x) \in K[x]$ $p(x) \neq 0$ such that $p(\alpha) = 0$

Example

- $\sqrt{2}$ is algebraic over $\mathbb{Q}$ root of $x^2 - 2$
- $F \subseteq F(x)$ x is not algebraic over $/F$

why let $p(t) = \sum a_i t^i \in F[t]$ such that

$$p(x) = 0 \Rightarrow \sum a_i x^i = 0 \in F \subseteq F(x)$$
$$\Rightarrow a_i = 0$$

Lemma K/F $\alpha \in K$ algebraic

$$\Leftrightarrow \mathrm{eval}_\alpha : F[x] \longrightarrow K \quad \text{is not injective.}$$
$$p(x) \longmapsto p(\alpha)$$

Proof

$\Leftarrow$ let $f \in \ker \mathrm{eval}_\alpha$ $\Rightarrow$ $f(\alpha) = 0$ $\Rightarrow$ α algebraic
$f \neq 0$

$\Rightarrow$ let $p \in F[x] \setminus \{0\}$ with $p(\alpha) \neq 0$ then $p \in \ker \mathrm{eval}_\alpha \Rightarrow \ker \mathrm{eval}_\alpha \neq 0$.

We say that a fields extension is algebraic if for all $\alpha \in K$ we have that α is algebraic $/F$.

Finitely generated extension

K/F field extension $\alpha \in K$

$$F \subseteq F(\alpha) := \bigcap_{\substack{K \supseteq L \supseteq F \\ \alpha \in L}} L$$

· Universal property: it is the smallest intermediate extension containing α

For all

$$\begin{tikzcd} F \arrow[r, hook] \arrow[dr, hook] & L \arrow[r, hook] & K \\ & F(\alpha) \arrow[u, hook, "\exists!"'] & \end{tikzcd}$$

If $K = F(\alpha)$ we say that K is a simple extension of F and that α is a primitive element for K

(Digression on the theorem of element primitive)

Recursively: K/F : $\alpha_1 \dots \alpha_n \in K$

$$F(\alpha_1 \dots \alpha_n) = F(\alpha_1 \dots \alpha_{n-1})(\alpha_n)$$

is the smallest intermediate extension containing $\alpha_1 \dots \alpha_n$

~~Theorem K/F fini'~~

We say that K/F is finitely generated if $\exists$ finitely many $\alpha_1 \dots \alpha_n \in K$ such that

$$K \simeq K(\alpha_1 \dots \alpha_n)$$

Theorem K/F finite
$\iff$ algebraic & finitely generated

Example

- $\mathbb{Q}(x)/\mathbb{Q}$ fg but not finite
- $\overline{\mathbb{Q}}/\mathbb{Q}$ algebraic but not finite.

Minimal polynomial

Def K/F ~~ext~~ $\alpha \in K$ algebraic the minimal poly of α is the (unique) monic generator of $\ker \mathrm{eval}_\alpha$ it is denoted by $m_{\alpha,F}(x)$

Remark: $F[x]$ PID
$\Rightarrow \ker \mathrm{eval}_\alpha = (p(x))$
If $p(x)$ is monic then $p(x) = m_{\alpha,F}(x)$
otherwise $m_{\alpha,F}(x) = \frac{1}{LC(p)} p(x)$
and $(p(x)) = (m_{F,\alpha}(x))$

Lemma: Given K/F and $\alpha \in K$ algebraic$/F$ we have that $p \in F[x]$ is the minimal polynomial of $\alpha \iff p$ is irreducible, monic and $p(\alpha)=0$

Proof

$\Rightarrow$ • $m_{F,\alpha}$ is monic by definition.

• $m_{F,\alpha} \in \ker \mathrm{eval}_\alpha \Rightarrow m_{\alpha,F}(\alpha) = 0$

• $F[x]/(m_{F,\alpha}) = F[x]/\ker \mathrm{eval}_\alpha \overset{F\Pi}{\subseteq} K$ field

$\Rightarrow$ it is a domain $\Rightarrow (m_{F,\alpha})$ is prime

$\Rightarrow m_{\alpha,F}$ irreducible

$(\Leftarrow)$ Let p monic irreducible with $p(\alpha)=0$

(we want to show that

$\mathrm{Ker}\, \mathrm{eval}_\alpha = (p(x))$)

Certainly $p \in \mathrm{Ker}\, \mathrm{eval}_\alpha \Rightarrow (p(x)) \subseteq \underset{(m_{\alpha,F})}{\mathrm{Ker}\, \mathrm{eval}_\alpha}$

$\Rightarrow m_{\alpha,F} \mid p(x)$ irreducible

$\Rightarrow m_{\alpha,F} \sim p(x)$ but both are monic

Example: minimal poly $\sqrt{2}$

· minimal poly $\sqrt{2}+\sqrt{3}$

Prop K/F $\quad \alpha \in K$

1) If α is algebraic then $F(\alpha) \simeq F[x]/(m_{\alpha,F})$

2) If α is trascendent then $F(\alpha) \simeq F(x)$

Proof

1) α algebraic.

$$\begin{array}{ccc} F[x] & \longrightarrow & K \\ \downarrow & & \\ F[x]/(m_{\alpha,F}) & \simeq \mathrm{Im}\, \mathrm{eval}_\alpha & \overset{?}{\supseteq} K(\alpha) \end{array}$$

this is a subfield of K that contains $\alpha = \mathrm{eval}_\alpha(x)$

$\Rightarrow \mathrm{Im}\, \mathrm{eval}_\alpha \supseteq K(\alpha)$

Conversely let $\beta \in \mathrm{Im}\, \mathrm{eval}_\alpha$ $\quad \beta = \sum a_i \alpha^i \quad a_i \in F$

$\in F(\alpha)$

2) α trascendent

$\mathrm{eval}_\alpha : F[x] \longrightarrow K$

$p \in F[x] \quad p(\alpha) \neq 0 \Rightarrow p(\alpha)$ is invertible

thus we use the universal propert of the field of fractio

$$\begin{tikzcd}
F[x] \arrow[r, "eval_\alpha"] \arrow[d] & K \\
F(x) \simeq Q(F[x]) \arrow[ur, dashed, "\varphi_\alpha \ \exists!"'] &
\end{tikzcd}$$

want $\operatorname{Im} \varphi_\alpha = F(\alpha)$

$\varphi_\alpha(\underset{1}{x}) = eval_\alpha(x) = \alpha \Rightarrow F(\alpha) \subseteq \operatorname{Im} \varphi_\alpha$

On the other side $\beta \in \operatorname{Im} \varphi_\alpha$

$$\beta = \frac{p(\alpha)}{q(\alpha)} \qquad p, q \in F[x] \quad q \neq 0$$

$$= \frac{\sum a_i \alpha^i}{\sum b_i \alpha^i} \in F(\alpha) \qquad \#$$

<u>Example</u>

- $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ we have 3 roots $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2} \in \mathbb{C}$

where ω is a root of x^2+x+1

$\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(\omega\sqrt[3]{2})$ but they are not equal as subfield of $\mathbb{C}$!

Cor: if α, β are roots of the same polynomial then $F(\alpha) \simeq F(\beta)$

<u>Conversely</u>: Suppose that we have an isomorphis[m] α, β algebraic

$\varphi: F(\alpha) \longrightarrow F(\beta)$

Such that $\varphi_{|F} = id$ and $\varphi(\alpha) = \beta$

$$\Rightarrow m_{F,\alpha} \stackrel{?}{=} m_{F,\beta}$$

<u>Proof</u>:

$m_{\alpha F} = \sum a_i x^i$

$m_{\alpha F}(\varphi(\alpha)) = \sum a_i \varphi(\alpha)^i = \sum \varphi(a_i)\varphi(\alpha)^i$

$= \sum \varphi(a_i \alpha^i) = \varphi\left(\sum a_i \alpha^i\right) = \varphi(0) = 0.$

$\Rightarrow m_{\alpha F}(\beta) = 0) \Rightarrow m_{\beta F} \mid m_{\alpha F}$

$\Rightarrow m_{\beta F} = m_{\alpha F}$

Example

$\varphi : \mathbb{Q}(\sqrt{2}) \xrightarrow{\sim} \mathbb{Q}(2+\sqrt{2}) = \mathbb{Q}(\sqrt{2})$

identity $|_{\mathbb{Q}}$ = identity

$\sqrt{2} \longmapsto \sqrt{2} \neq 2+\sqrt{2}$

They have different minimal poly

$x^2-2 \qquad x^2-4x+2$

· Rmk another point of view:

F field $\quad p(x)$ irreducible poly

$F[x]/(p(x))$ is a field extension of

F where p has a root (might not split completely)

$$F \hookrightarrow F[x] \longrightarrow F[x]/(p(x)) \quad \text{injective}$$

$$p(x+(p(x))) = \sum a_i (x+(p(x)))^i$$

$$= \sum p(x) + (p(x)) = 0$$

The proof of the theorem

Lemma finite $\Rightarrow$ algebraic.

Finite $\Rightarrow$ fg

$v_1 \ldots v_n \in K$ basis

$F(v_1 \ldots v_n) = K$

Proof Let $m = [K:F] < \infty \qquad \alpha \in K$

$1, \alpha, \alpha^2 \ldots \alpha^m$ are F-linearly dep

$\exists\, a_i \in F$ not all 0 st

$\sum_0^m a_i \alpha^i = 0 \qquad$ let $p(x) = \sum_0^m a_i x^i$

$p(\alpha) = 0 \quad \alpha$ algebraic

Lemma L/K finite K/F finite $\Rightarrow L/F$ finite and $[L:F]=[L:K][K:F]$

Proof $[L:K]=k$ $\quad v_1 \dots v_k \in K$ basis for L/K

$[K:F]=m$ $\quad w_1 \dots w_m$ —— K/F

$\alpha \in L$

$$\alpha = \sum_i a_i v_i \qquad a_i \in K \qquad a_i = \sum_j b_{ij} w_j$$

$$= \sum_i \left(\sum_j b_{ij} w_j\right) v_i$$

$$= \sum_{i,j} b_{ij}\, w_j \cdot v_i$$

$\Rightarrow \langle w_j \cdot v_i \rangle$ L over F

They are linearly independent

$$\sum \beta_{ij} w_j v_i = 0$$
$$\|$$
$$\sum_i \left(\sum_j \beta_{ij} w_j\right) v_i \Rightarrow \sum_j \beta_{ij} w_j = 0$$
$$\Rightarrow \beta_{ij} = 0$$

- **Lemma** $[F(\alpha):F] = \deg m_{\alpha F}$

Proof: let $d = \deg m_{\alpha F}$

I claim that $1, \alpha \dots \alpha^{d-1}$ gives a basis for $F(\alpha)/F$

- They are li $\quad \sum_0^{d-1} a_i \alpha^i = 0$

$$\Rightarrow p(x) = \sum_1^{d-1} a_i x^i \qquad p(\alpha) = 0$$

but $\deg p(x) < \deg m_{\alpha F}(x)$

$$\Rightarrow p(x) = 0 \quad \Rightarrow a_i = 0$$

- They generate. We use the iso

$$F[x]/(m_{\alpha F}) \simeq F(\alpha)$$

$\cancel{\alpha}$ $\beta \in F(\alpha)$ then $\exists$ $p(x) + (m_{\alpha F}(x))$

such that $\beta = p(\alpha)$

By the Euclidean algorithm we can chose $p(x)$ such that $\deg p \lneq \deg m_{\alpha F}$

$$p(x) = \sum_{1}^{d-1} a_i x^i$$

$$\beta = \sum_{1}^{d-1} a_i \alpha^i$$

Prop: fg + alg $\Rightarrow$ finite.

Proof $K = F(\alpha_1 \dots \alpha_n)$ Induction on n

$\Rightarrow$ they are algeb

① $n=1$ $K = F(\alpha_1)$ $\alpha_1 \in K \Rightarrow$ alg / F

$[K:F] = \deg m_{\alpha_1 F} < \infty$

② suppose that the statement is true for $K = F(\alpha_1 \dots \alpha_n)$ we show that it is true for $K = F(\alpha_1 \dots \alpha_{n+1})$ algebraic

$F(\alpha_1 \dots \alpha_n) \subseteq F(\alpha_1 \dots \alpha_{n+1})$

This is fg + algebraic

$[F(\alpha_1 \dots \alpha_n) : F] = m < \infty$

α_{n+1} is algebraic / F $\Rightarrow$ it is alg / $F(\alpha_1 \dots \alpha_n)$

$\Rightarrow [F(\alpha_1 \dots \alpha_{n+1}) : F(\alpha_1 \dots \alpha_n)] = \deg m_{\alpha_{n+1} F(\alpha_1 \dots \alpha_n)} < \infty$

$\Rightarrow [F(\alpha_1 \dots \alpha_{n+1}) : F]$ is finite

<u>Corollary</u>: K/F α, β algebraic so are $\alpha \pm \beta$ $\alpha\beta$ $\alpha \cdot \beta^{-1}$ if $\beta \neq 0$

$\{\alpha \in K \mid \alpha \text{ algebraic } /F\}$ is a field.

<u>Proof</u> All these are elements of $F(\alpha, \beta)$ which is finite $\Rightarrow$ algebraic.

β algebraic $/F$ $\quad m_{\beta, F} \subseteq F(\alpha)[x]$

it might be reducible

$$[F(\alpha,\beta) : F(\alpha)] \leq \deg m_{\beta F} < \infty$$

$$[F(\alpha) : F] = \cancel{\deg}\, m_{\alpha F} < \infty$$

$$(*) \Rightarrow \boxed{[F(\alpha,\beta) : F] \leq \deg m_{\alpha F} \cdot \deg m_{\beta F} < \infty}$$

$\Rightarrow F(\alpha, \beta)$ algebraic $/F$

<u>Cor</u> $(\deg m_{\alpha F}, \deg m_{\beta F}) = 1 \Rightarrow$

$$[F(\alpha,\beta) : F] = \deg m_{\alpha F} \cdot \deg m_{\beta F}$$

<u>Proof</u>

$[F(\alpha,\beta) : F(\alpha)]$

$$\begin{tikzcd} & F \arrow[dl] \arrow[dr] \arrow[dd] & \\ F(\alpha) \arrow[dr] & & F(\beta) \arrow[dl] \\ & F(\alpha\beta) & \end{tikzcd}$$

$[F(\alpha) : F] \mid [F(\alpha\beta) : F]$ $\rightarrow$ common multiple

$[F(\beta) : F] \mid [F(\alpha,\beta) : F]$

$\geq$ lcm $=$ the product use $(*)$.

Application $\overline{\mathbb{Q}}/\mathbb{Q}$ is not finite.

α_p root of $x^p - 2$ p prime (irreducible)

Suppose that $\overline{\mathbb{Q}}/\mathbb{Q}$ finite

$[\overline{\mathbb{Q}}:\mathbb{Q}] = \prod p_i^{m_i}$ q a prime

q not in the fact

$\alpha_q \in \overline{\mathbb{Q}}$

$q = [\mathbb{Q}(\alpha_q):\mathbb{Q}] \mid [\overline{\mathbb{Q}}:\mathbb{Q}]$.