Lecture #3 (Sep 25, 2024)

Today: $\begin{cases} \text{Separable and} \\ \text{normal extensions} \end{cases}$

Notation Given L/K and M/K

- $\mathrm{Hom}_K(L,M) := \{\varphi : L \to M \,;\, \varphi \neq 0_M \text{ and } K\text{-linear}\}$
  field morphisms
- $\mathrm{Aut}_K(L) := \{\varphi \in \mathrm{Hom}_K(L,L) \,;\, \varphi \text{ is bijective}\}$

Definition Given L/K and $S \subset K[x] \setminus K$, we say L is a splitting field for S iff

(i) each $f \in S$ splits over L, and

(ii) $L = K(A)$, where A is the set of all roots of all $f \in S$.

Notation: $L = SF_K(S)$

Definition (Normality)

A field extension L/K is called normal iff $L = SF_K(S)$ for some $S \subset K[x]$

(We also say that L is normal K)

<u>RmK</u> Note that normal $\Rightarrow$ algebraic

Proposition If L/K is algebraic, then TFAE:

(i) L/K is normal

(ii) If $\sigma \in \mathrm{Hom}_K(L, \bar{L})$, then $\sigma(L) = L$.

(iii) If $K \subset F \subset L \subset F'$ are fields and $\sigma \in \mathrm{Hom}_K(F, F')$, then $\sigma(F) \subset L$ and $\exists\, \tilde{\sigma} \in \mathrm{Aut}_K(L)$ s.t. $\tilde{\sigma}|_F = \sigma$

(iv) if $f \in K[x]$ is irreducible and it has a root in L, then f splits over L

(v) given $\alpha \in L$, m_α splits over L

Examples

① Every degree two extension is normal.

② Given $f \in K[x] \setminus \{0\}$,

$SF_K(f)/K$ is normal.

- $\mathbb{Q}(\omega, \sqrt[3]{2})$, $\omega^3 = 1$ is normal $/ \mathbb{Q}$

- $$\underbrace{\mathbb{Q}(\sqrt[4]{2}, i) \overset{\text{normal}}{\supset} \mathbb{Q}(i) \overset{\text{normal}}{\supset} \mathbb{Q}}_{\text{normal}}$$

Question Is $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ normal?

Rmk In general, given $K \subset F \subset L$, if L/K is finite and normal, then so is L/F.

⚠ F/K may not be normal!

$$\mathbb{Q}(\sqrt[3]{2}, \omega) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$$

not normal

③ p a prime, $K = \mathbb{F}_p$

$L = K(\alpha_1, \dots, \alpha_n)$, where $\alpha_i^p \in \mathbb{F}_p$ $\forall i$

Then $L = SF_K(\{m_{\alpha_i}\})$ and L/K is normal.

Definition Let L/K be a field extension, fix $n \geq 0$ and $(\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n) \in L^n$.

We say $(\alpha_1, \dots, \alpha_n)$ and $(\beta_1, \dots, \beta_n)$ are conjugate over K iff for all $f \in K[X_1, \dots, X_n]$

$$f(\alpha_1, \dots, \alpha_n) = 0 \iff f(\beta_1, \dots, \beta_n) = 0$$

Proposition Let L/K be a finite normal extension and $G = \mathrm{Aut}_K(L)$.

Fix $\alpha, \beta \in L$. Then

α and β are conjugate $\iff \beta = \sigma(\alpha)$ for some $\sigma \in G$.

(φ and $\tilde{\varphi}$ are given, $\tilde{\varphi}$ extends φ)

Lemma 1

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\varphi}} & L' \\ \cup & & \cup \\ K & \xrightarrow[\varphi]{} & K' \end{array} \quad \rightsquigarrow \quad K[x] \xrightarrow[\varphi_*]{} K'[x]$$

Given $\alpha \in L$ and $f \in K[x]$

$f(\alpha) = 0 \iff \varphi_* f\left(\tilde{\varphi}(\alpha)\right) = 0$

Lemma 2

L/K is finite & normal $\iff L = SF_K(f)$ for some $f \in K[x] \setminus \{0\}$

proof of proposition

$(\Leftarrow)$ Apply Lemma 1 to

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\varphi} = \sigma} & L \\ \cup & & \cup \\ K & \xrightarrow[\varphi = id]{} & K \end{array}$$

$(\Rightarrow)$ α and β are alg. $/K$ and

$m_\alpha = m_\beta$. Thus, $\exists$ iso. $\varphi: K(\alpha) \to K(\beta)$

$\alpha \mapsto \beta$

Since L/K is finite and normal,
$L = SF_K(f)$ for some $f \in K[x] \setminus \{0\}$ (Lemma 2)

In fact, $L/K(\alpha)$ and $L/K(\beta)$ are also finite and normal and

$$L = SF_{K(\alpha)}(f) = SF_{K(\beta)}(f)$$ check!

Moreover, $f = \varphi_* f$ and we know that $\exists$ an automorphism $\tilde{\varphi} : L \to L$ extending φ:

$$\begin{tikzcd}
SF_{K(\alpha)}(f) = L \arrow[r, "\exists\ \tilde{\varphi}", "\simeq"'] & L = SF_{K(\beta)}(\varphi_* f) \\
f \quad K(\alpha) \arrow[u, hook] \arrow[r, "\simeq", "\varphi"'] & K(\beta) \arrow[u, hook] \quad \varphi_* f = f
\end{tikzcd}$$

given

Definition Let K be a field.

An <u>irreducible</u> polynomial $f \in K[x]$ is separable over K if it has no repeated roots in $SF_K(f)$ ($\Longleftrightarrow$ it splits into <u>distinct</u> linear factors in $SF_K(f)$)

A general $g \in K[x]$ is separable if each of its irred. factors (over K) is separable over K. Otherwise, g is called inseparable.

Definition Let L/K be a field extension.

(i) $\alpha \in L$ is separable over K if $\min_K(\alpha) := m_\alpha$ is separable over K.

If you prefer, you may add α is alg.

(ii) L/K is separable if every $\alpha \in L$ is separable (over K).

(as before, we also say that L is sep. $/K$)

(iii) $L^{sep,K} := \{\alpha \in L^{alg,K} ; \alpha \text{ is separable } /K\}$ is a subfield of L called the sep. closure of K in L.

Examples

① Any alg. ext. of $\begin{cases} \text{a field of char} = 0 \\ \text{a finite field} \end{cases}$

② Let $K = \mathbb{F}_p(\alpha)$ and $f = x^p - \alpha$

Then $L = SF_K(f)$ is NOT separable over K.

Definition Let L/K be an algebraic field extension (here think char $K = p > 0$)

(i) $\alpha \in L$ is purely inseparable over K if $\min_K(\alpha)$ has exactly one root

($\Leftrightarrow \exists n$ s.t. $\alpha^{p^n} \in K$)

(ii) L/K is purely inseperable if every $\alpha \in L$ is purely inseparable $/K$.

Exercises

assume finite

① Given L/K, prove that

$L^{sep,K}$ is a field extension of K.

② Prove that if L/K is finite and separable, then $L = K(\alpha)$ for some $\alpha \in L$.

---

① Any $\alpha \in K$ is algebraic and separable $/K$ $(\min_K(\alpha) = x - \alpha)$

To see $L^{sep,K}$ is a field, it suffices to show

$$\alpha, \beta \in L^{sep,K} \implies K(\alpha, \beta) \subset L^{sep,K}$$

For this, we will use the following lemma:

$$K \subset L \subset \overline{K}$$

Lemma 3

$\alpha \in L$ is separable $\Leftrightarrow$ $M_\alpha : L \to L$ given by $x \mapsto \alpha x$ is diagonalizable (over $\overline{K}$)

Take $\alpha, \beta \in L^{sep, K}$. Then M_α and M_β are simultaneously diagonalizable. That is, we fix a basis &

$\exists P \in GL(n, \overline{K})$, $n = [L : K]$

s.t. $P[M_\alpha]P^{-1}$ & $P[M_\beta]P^{-1}$ are diagonal.

Now, take $x \in K(\alpha, \beta)$. Then

$x = f(\alpha, \beta)$ for some $f \in K[s, t]$

Thus,

$$P[M_x]P^{-1} = f\left(P[M_\alpha]P^{-1}, P[M_\beta]P^{-1}\right)$$

is diagonal

$\boxed{3}$

(2) This is the primitive element theorem

First, note that we may assume

$L = K(\alpha, \beta)$ with $\alpha, \beta \in L$ alg. &

sep. $/ K$ and K infinite

(K finite $\Rightarrow$ L finite $\Rightarrow$ $L = K(\eta)$
where $L^\times = \langle \eta \rangle$)

Now, given $\lambda \in K$ consider

$$\ell_\lambda := \alpha + \lambda\beta \in L$$

Claim For all but finitely many choices of λ we have that $L = K(\ell_\lambda)$.

$$\Updownarrow$$

$$\beta \in K(\ell_\lambda) \iff \min_{K(\ell_\lambda)}(\beta) \text{ has deg } 1$$

Let $f := \min_K(\alpha)$ and $g := \min_K(\beta)$

Let $F := SF_L(\{f, g\})$

Consider

$$h(x) := f(\ell_\lambda - \lambda x) \in \underbrace{K(\ell_\lambda)[x]}_{:= R}$$

Then β is a root of h since

$\alpha = \ell_\lambda - \lambda\beta$.

Thus, $\min_{K(\ell_\lambda)}(\beta)$ divides g and h

So, it suffices to show

$\gcd(g, h)$ has $\deg = 1$ (in R)

for almost all choices of λ.

Since β is separable $/K$

it follows that if gcd has deg ≥ 2, then $\exists\ \beta' \neq \beta \in F$ that is a root of both g and h.

But then $\alpha' = \ell_\lambda - \lambda\beta' = \alpha + \lambda(\beta - \beta')$ is a root of f in F.

Thus, $\lambda = \dfrac{\alpha' - \alpha}{\beta - \beta'}$ $\star$

In short,

$$\left\{ \begin{array}{c} \text{common roots} \\ \text{of } g \ \& \ h \\ \neq \beta \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \lambda\text{'s of the} \\ \text{form } \star \end{array} \right\}$$

So, it suffices to avoid the finitely many "bad choices".

Exercise

Prove that $\mathbb{Q}(i, \sqrt[3]{2}) / \mathbb{Q}$ is finite and separable and $\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(i + \sqrt[3]{2})$ (i.e., $\lambda = 1$ works)