Lecture # 2 (Sep 18, 2024)

Today: $\begin{cases} \text{Algebraic extensions } \S 1 \\ \text{algebraic closures } \S 3 \\ \text{splitting fields } \S 2 \end{cases}$

§ 1

Let L/K be a field extension and fix $\alpha \in L$. Consider the morphism of K-algebras

$$\begin{aligned} ev_\alpha : K[X] &\longrightarrow L \\ f &\longmapsto f(\alpha) \end{aligned}$$

and since $K[X]$ is a PID, write

$$\operatorname{Ker}(ev_\alpha) = (m_\alpha).$$

Sometimes called the annihilator of α

Definition α is called algebraic over K if $(m_\alpha) \neq (0)$. Otherwise, α is called transcendental.

Rmk When $K = \mathbb{Q}$, $L = \mathbb{C}$ and $\alpha \in \mathbb{C}$ is algebraic (resp. transcendent) over $\mathbb{Q}$ we often say that α is an algebraic (resp. transcendent) number.

Proposition Given L/K and $\alpha \in L$ as before, we have that α is algebraic over K iff
$$K[\alpha] = \{f(\alpha) \in L \,;\, f \in K[x]\} = \operatorname{im}(ev_\alpha) \simeq K[x]/(m_\alpha)$$
is a f.d.v.s. $/K$, in which case

(i) $K \subset K[\alpha] \leq L$ $\Rightarrow$ $K[\alpha] = K(\alpha)$

subfield

(ii) m_α is irreducible

(iii) $[K[\alpha] : K] = \deg m_\alpha$

(iv) $\{\alpha^i\}_{0 \le i \le \deg m_\alpha - 1}$ gives a basis for $K[\alpha]$ (as K-v.s.)

Definition Let L/K be a field extension and set

$$L^{alg,K} := \{\alpha \in L ; \alpha \text{ is alg. } / K\}$$

We say that the extension L/K is algebraic if $L = L^{alg,K}$. Otherwise, the extension is called transcendental.

<u>Example</u> Every finite field extension L/K is algebraic and finitely generated (as a field) over K.

Exercise

$$K \subsetneq F \leq K(\alpha)$$

α transcendental over K

i.e., $ev_\alpha : K[x] \longrightarrow K[\alpha]$
$f \longmapsto f(\alpha)$

is injective. Let's show α is algebraic over F.

We know that

$$K[x] \simeq \operatorname{im}(ev_\alpha) / \ker(ev_\alpha) \simeq K[\alpha]/(0) = K[\alpha]$$

So, $K(\alpha) = \operatorname{Frac}(K[\alpha]) \simeq \operatorname{Frac}(K[x]) \simeq K(x)$

Since $K \subsetneq F$, $\exists\ f/g \in F(x) \setminus K$

and $f(x) - \frac{f(\alpha)}{g(\alpha)} g(x)$ is a

polynomial in $F[x]$ that has α

as a root.

$F \subset K(\alpha)$ & $F \supsetneq K$

$\exists\ f(\alpha)/g(\alpha) \in F \setminus K$

$\Rightarrow f(x) - \frac{f(\alpha)}{g(\alpha)} g(x) \in F[x]$

Proposition Given a field extension L/K, $L^{alg,K} \leq L$. This subfield is called the algebraic closure of K in L.

(relative alg. closure)

If $L^{alg,K} = K$, we say that K is alg. closed in L.

<u>Proof</u> To show that $L^{alg,K}$ is a field it suffices to show that given $0 \neq \alpha, \beta \in L^{alg,K}$ the extension $K \subset K(\alpha, \beta)$ is algebraic since $\alpha + \beta, -\alpha, \alpha\beta, \alpha^{-1}$ all lie in $K(\alpha, \beta)$.

Now, $K \subset K(\alpha)$ is finite since α is algebraic $/K$

and $K(\alpha) \subset K(\alpha, \beta)$ is finite since β is alg. $/ K(\alpha)$

(alg. $/K \Rightarrow$ alg. $/K(\alpha)$)

but then $K \subset K(\alpha, \beta)$ is finite,

hence algebraic. ⊠

§2 Splitting fields

Let K be a field and fix $f \in K[x]$.
(of deg n)

Definition A field extension L/K is called a splitting field of f if L is the smallest field containing K with the property that in $L[x]$ f factors as a product of linear terms.

Remark/proposition: Given $f \in K[x]$, a splitting field exists, and it is unique up to iso., namely $L = K(\alpha_1, \dots, \alpha_n)$,

where $\alpha_1, \dots, \alpha_n$ are the roots of f.
So, given f, we let $L_f := K(\alpha_1, \dots, \alpha_n)$ denote its splitting field.

Remark/proposition In general, we have that $[L_f : K]$ divides $n!$.

why?

Exercises

1) Prove that if $n > 1$ and $K = \mathbb{C}$ or $n > 2$ and $K = \mathbb{F}_p$, then $[L_f : K] \neq n!$

2) For each n, construct $f \in \mathbb{Q}[x]$ of degree n such that $[L_f : \mathbb{Q}] = n!$

Some examples

① $\alpha \in K$, $\alpha \notin K^{\times 2}$

Then $K(\sqrt{\alpha}) = L_f$ for $f(x) = x^2 - \alpha$.

Thus, $[L_f : K] = 2$

② fix a prime p, ζ s.t. $\zeta^p = 1$ $(\zeta \neq 1)$

and $f(x) = x^p - 1 \in \mathbb{Q}[x]$, then

$L_f = \mathbb{Q}(\zeta)$. Now,

$[L_f : \mathbb{Q}] = \deg m_\zeta = p - 1$

since $m_\zeta = x^{p-1} + x^{p-2} + \dots + 1$

(m_ζ is an irred. factor of $f / \mathbb{Q}$)

What happens if we replace $\mathbb{Q}$ by $\mathbb{F}_p$?

③ fix a prime p and

$f(x) = x^p - x - \alpha \in \mathbb{F}_p[x]$, $\alpha \neq 0$.

Let β be a root of f (not necessarily in $\mathbb{F}_p$)

Then $L_f = \mathbb{F}_p(\beta)$ since the other roots are $\beta+1, \beta+2, \dots, \beta+p-1$

In fact, since $\alpha \neq 0$ we know $\beta \notin \mathbb{F}_p$.

Now, because $x^p - x - \alpha$ is irred.,

$m_\beta = f$ and $[L_f : \mathbb{F}_p] = p$

§ 3 Algebraically closed fields and algebraic closures

Proposition / definition ☆

Given a field F, the following conditions are all equivalent.

(i) $f \in F[x] \Rightarrow \exists\, \alpha \in F$ s.t. $f(\alpha) = 0$

(ii) $f \in F[x] \Rightarrow f$ splits in $F[x]$

(iii) $f \in F[x]$ irred. $\Rightarrow \deg f = 1$

(iv) F'/F algebraic $\Rightarrow [F' : F] = 1$
finite

If any (hence all) of these holds, then F is called **algebraically closed**.

Definition Given a field K, an algebraic closure of K, denoted $\overline{K}$, is an algebraic extension of K which is algebraic closed.

<u>RmK</u> Given K, $\overline{K}$ exists and it is unique up to iso. (proof in Milne's notes Chapter 6)

<u>RmK</u> Given L/K with L algebraically closed, we have that $L^{alg,K}$ is itself algebraically closed, and $L^{alg,K} = \overline{K}$.

So, to Prop/def ★, we can add:

(v) given L/F, $F = L^{alg,F}$

⚠ $\mathbb{A} = \mathbb{C}^{alg,\mathbb{Q}} = \overline{\mathbb{Q}} \neq \mathbb{C}$

$\mathbb{C}/\mathbb{Q}$ is <u>not</u> algebraic