Intro to Algebra 2 W4-1

fat

March 13, 2024

Theorem 1 (Theorem 17)**.** An extension K/F is finite $\Leftrightarrow$ K is generated by a finite number of algebraic elements over F. More precisely the field generated by a finite number of algebraic elements $\alpha_1, ..., \alpha_k$ of degrees $n_1, ..., n_k$ has degree $\leq n_1 \cdots n_k$ over F.

Proof.

($\Rightarrow$) Assume that $[K : F] < \infty$. If $K = F$, nothing to be done. If $K \neq F$, then $\exists \alpha_1 \in K \setminus F$ (α_1 algebraic over F since K/F is algebraic.). We have $K - F(\alpha_1) - F$. By theorem 14, $[K : F] = [K : F(\alpha_1)][F(\alpha_1) : F] \neq 1$ since $\alpha_1 \notin F$. $\Rightarrow [K : F(\alpha_1)] < [K : F]$. If $K = F(\alpha_1)$, we are done. If $K \neq F(\alpha_1)$, then $\exists \alpha_2 \in K \setminus F(\alpha_1)$. By the same argument, we have $[K : F(\alpha_1)(\alpha_2)] < [K : F(\alpha_1)]$. In this way, we get a sequence $\alpha_1, \alpha_2, ...$ with $[K : F(\alpha_1, ..., \alpha_k)] < [K : F(\alpha_1, ..., \alpha_{k-1})] < \cdots < [K : F]$. Since $[K : F] < \infty$, this implies that $\exists \alpha_1, ..., \alpha_k \in K$ such that $[K : F(\alpha_1, ..., \alpha_k)] = 1$, i.e. $K = F(\alpha_1, ..., \alpha_k)$.

($\Leftarrow$) We'll prove the case $k = 2$, i.e. that

$$[F(\alpha_1, \alpha_2) : F] \leq [F(\alpha_1) : F][F(\alpha_2) : F]$$

We have $F(\alpha_1, \alpha_2) - F(\alpha_1) - F$. By theorem 14, $[F(\alpha_1, \alpha_2) : F] = [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F]$. Thus, it suffices to prove that

$$[F(\alpha_1, \alpha_2) : F(\alpha_1)] \leq [F(\alpha_2) : F]$$

Now by theorem 4+6,

$$\text{L.H.S.} = \deg m_{\alpha_2, F(\alpha_1)}(x)$$

$$\text{R.H.S.} = \deg m_{\alpha_2, F}(x)$$

Observe that $m_{\alpha_2, F(\alpha_1)}(x) | m_{\alpha_1, F}(x)$. (Recall that $m_{\alpha_2, F(\alpha_1)}(x)$ has the property that $f(x) \in F(\alpha_1)[x]$ has a root $\alpha_2 \Leftrightarrow m_{\alpha_2, F(\alpha_1)}(x) | f(x)$. Here $m_{\alpha_2, F}(x) \in F[x] \subseteq F(\alpha_1)[x]$ and has α_2 as a root.)

$$\deg m_{\alpha_2, F(\alpha_1)}(x) \leq \deg m_{\alpha_2, F}(x)$$

$$\Rightarrow [F(\alpha_1, \alpha_2) : F] \leq [F(\alpha_1) : F][F(\alpha_2) : F]$$

□

Corollary 1 (Corollary 18)**.** α, β are algebraic over F. Then $\alpha\beta, \alpha \pm \beta, \alpha/\beta (\beta \neq 0)$ are all algebraic. In particular, given an extension field K over F, the subset of elements of K that are algebraic over F forms a subfield of K.

Proof.

Suppose that α, β are algebraic over F. Then by theorem 17, $[F(\alpha, \beta) : F] \leq [F(\alpha) : F][F(\beta) : F] < \infty$. $\Rightarrow \alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta)$ are algebraic over F. □

Definition 1. The subfield in the corollary is called the **algebraic closure** of F in K.

Theorem 2. Let $L - K - F$. If $L/K, K/F$ are both algebraic, then L/F is also algebraic.

Proof.

Let $\alpha \in L$. We need to show that α is algebraic over F, i.e.

$$[F(\alpha) : F] < \infty$$

Since L/K is algebraic, α is a zero of some polynomial $f(x) = a_n x^n + \cdots + a_0 \in K[x]$. We have

$$[F(a_n, ..., a_0)(\alpha) : F(a_n, ..., a_0)] \leq \deg f = n$$

since α is a root of $f(x) \in F(a_n, ..., a_0)[x]$.

$$[F(\alpha) : F] \leq [F(a_n, ..., a_0, \alpha) : F] = [F(a_n, ..., a_0)(\alpha) : F(a_n, ..., a_0)][F(a_n, ..., a_0) : F]$$

by theorem 14. Moreover by theorem 17

$$\text{R.H.S.} \leq n \prod_{i=0}^{n} [F(a_i) : F] < \infty$$

$\Rightarrow \alpha$ is algebraic over F. Thus every element o L is algebraic over F, i.e. L/F is algebraic. □

Definition 2. Let K_1, K_2 be subfields of K. Then the **composite** of K_1, K_2, denoted by K_1K_2 is defined to be the smallest subfield of K containing both K_1 and K_2.

Remark 1. Note that if

$$K_1 = F(\alpha_1, ..., \alpha_m)$$

$$K_2 = F(\beta_1, ..., \beta_n)$$

then $K_1K_2 = F(\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_n)$.

Proposition 1 (Proposition 21)**.** Let K_1, K_2 be 2 finite extension fields of F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

Moreover, if $\text{GCD}([K_1 : F], [K_2 : F]) = 1$, then the equality holds.

Proof.

Suppose that $\{\alpha_1, ..., \alpha_m\}$ is a basis for K_1 over F, $\{\beta_1, ..., \beta_n\}$ a basis for K_2 over F.

Claim. $\{\alpha_i\beta_j\}$ spans K_1K_2 over F. (Then $[K_1K_2 : F] \leq |\{\alpha_i\beta_j\}| = mn$.)

Proof of claim.

Clearly we have $K_1 = F(\alpha_1, ..., \alpha_m), K_2 = F(\beta_1, ..., \beta_n)$. Then $K_1K_2 = F(\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_n)$. Now by theorem 4+6

$$F(\alpha_1) = F[\alpha_1]$$

$$F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2) = F(\alpha_1)[\alpha_2] = F[\alpha_1, \alpha_2]$$

$$\Rightarrow F(\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_n) = F[\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_n]$$

That is, every element of K_1K_2 can be written as a linear sum of products $f_j(\alpha_1, ..., \alpha_m)g_j(\beta_1, ..., \beta_n)$ over F where $f_j(\alpha_1, ..., \alpha_m)$ is a monomial in $\alpha_1, ..., \alpha_m$, $g_j(\beta_1, ..., \beta_n)$ is a monimial in $\beta_1, ..., \beta_n$. Now $f_j(\alpha_1, ..., \alpha_m) \in K_1$ so it can be written as a lineaer sum in α_i over F. Same works with $g_j(\beta_1, ..., \beta_n)$. $\Rightarrow f_j(\alpha_1, ..., \alpha_m)g_j(\beta_1, ..., \beta_n)$ is equal to a linear sum in $\alpha_i\beta_k$. $\Rightarrow \{\alpha_i\beta_k\}$ spans K_1K_2 over F. $\square$

Now observe that

$$[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$$

$$\Rightarrow [K_1 : F] | [K_1K_2 : F]$$

Likewise

$$[K_2 : F] | [K_1K_2 : F]$$

$$\Rightarrow \text{LCM}([K_1 : F], [K_2 : F]) | [K_1K_2 : F]$$

When $\text{GCD}([K_1 : F], [K_2 : F]) = 1$, we have $\text{LCM}([K_1 : F], [K_2 : F]) = [K_1 : F][K_2 : F]$. So $[K_1 : F][K_2 : F] \le [K_1K_2 : F] \le [K_1 : F][K_2 : F] \Rightarrow =$ holds. $\square$

13.3

Skipped

13.4 Splitting fields and algebraic closures

Definition 3. Let $f(x) \in F[x]$ An extension field K over F is called a **splitting field** for $f(x)$ if

(1) $f(x)$ splits completely (into linear factors) over K, i.e. K contains every root of $f(x)$.

(2) No proper subfield of K containing F has property (1).

Example 1.

- $x^2 + 1 \in \mathbb{Q}[x]$ has splitting field $\mathbb{Q}(i)$.
- $x^3 - 2 \in \mathbb{Q}[x]$ has splitting field $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}) = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$.
- $x^n - 1 \in \mathbb{Q}[x]$ has splitting field $\mathbb{Q}(e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, ..., e^{-\frac{2\pi i}{n}}) = \mathbb{Q}(e^{\frac{2\pi i}{n}})$

Theorem 3 (Theorem 25+26)**.** Given $f(x) \in F[x]$ a splitting field for $f(x)$ exists. Moreover, its degree over F is $\le n!$, where $n = \deg f$.

Proof.

We'll prove by induction on $n := \deg f$. When $n = 1, f(x) = ax - b$, where $a, b \in F, a \neq 0$. So f has a unique root $b/a \in F$. $\Rightarrow F$ is a splitting field for f. Assume the statement holds up to $\deg f = n - 1$. Now let $f(x)$ be a polynomial of $\deg n$ in $F[x]$. Let $g(x)$ be an irreducible factor of $f(x)$. By theorem 3, g has a root α in $E = F[x]/(g(x))$, which is an extension field of F with $[E : F] = \deg g \leq \deg f = n$. Now we have $f(x) = (x - \alpha)h(x)$ for some polynomial $h(x) \in E[x]$. Since $\deg h = n - 1$, by the induction hypothesis a splitting field E' exists for $h(x)$ with $[E' : E] \leq (n-1)!$ and $[E' : F] = [E' : E][E : F] \leq n!$. $\Rightarrow f$ splits completely in E'. Take K be the smallest subfield of E' containing F and all roots of $f(x)$. Then K is a splitting field for $f(x)$. It satisfies

$$[K : F] \leq [E' : F] \leq n!$$

$\square$