Intro to Algebra 2 W6-1

fat

March 28, 2024

Quiz: Next Wed., April 3.

Midterm: Fri., April 12.

Including Chap 9, 13 (excluding 9.6, 13.3) and Section 14.1

Proof of Theorem 41*, continued.*

We have shown that if p is a prime not dividing n then $f(\zeta_n^p) = 0$, where $f(x) = m_{\zeta_n,\mathbb{Q}}(x)$. The same argument also shows that for any primitive n-th root ζ_n^k of unity (k,n) and any prime $p \nmid n$, ζ_n^k, ζ_n^{kp} have the same minimal polynomial over $\mathbb{Q}$. $\Rightarrow \forall a \in \mathbb{Z}, (a,n) = 1$, if $a = p_1 \cdots p_k$, then $\zeta_n, \zeta_n^{p_1}, \zeta_n^{p_1 p_2}, ..., \zeta_n^{p_1 \cdots p_k} = \zeta_n^a$ have the same minimal polynomial over $\mathbb{Q}$.

$$\Rightarrow f(x) = \prod_{a=1,(a,n)=1}^{n} (x - \zeta_n^a) = \Phi_n(x)$$

$\Rightarrow \Phi_n(x)$ is irreducible over $\mathbb{Q}$. □

Remark 1. In the proof of Theorem 41, we claimed that $f(x), g(x)$ are both in $\mathbb{Z}[x]$, where $f(x) = m_{\zeta_n,\mathbb{Q}}(x), f(x)g(x) = \Phi_n(x)$.

Explanation: By Gauss's lemma, $\exists r, s \in \mathbb{Q}^\times$ such that $rf(x), sg(x) \in \mathbb{Z}[x]$ and $\Phi_n(x) = (rf(x))(sg(x))$. Observe that $rs = 1$. Considering the leading coeffcients of $rf(x), sg(x) \in \mathbb{Z}[x]$, we see that $r, s \in \mathbb{Z} \Rightarrow r = s = \pm 1 \Rightarrow f(x), g(x) \in \mathbb{Z}[x]$.

Galois Theory

Recall that if $\alpha \in \bar{F}$, then (by Theorem 4+6 of Chap 13)

$$F[\alpha] = F(\alpha) \simeq {}^{F[x]}/_{(m_{\alpha,F}(x))}$$

Suppose that β is another root of $m_{\alpha,F}(x)$, then we also have

$$F[\beta] = F(\beta) \overset{(1)}{\simeq} {}^{F[x]}/_{(m_{\beta,F}(x))} \overset{(2)}{=} {}^{F[x]}/_{(m_{\alpha,F}(x))} \overset{(3)}{\simeq} F(\alpha) = F[\alpha]$$

Take an element $a_0 + a_1\beta + \cdots + a_n\beta^n$ as an example,

$$a_0 + a_1\beta + \cdots + a_n\beta^n \overset{(1)}{\to} a_0 + a_x + \cdots + a_n x^n + (m_{\beta,F}(x))$$

$$\overset{(2)}{\to} a_0 + a_1 x + \cdots + a_n x^n + (m_{\alpha,F}(x)) \overset{(3)}{\to} a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

From this, we see that if α, β have the same minimal polynomial over F, then the function $\phi_{\alpha,\beta} : F(\alpha) = F[\alpha] \to F[\beta] = F(\beta)$ defined by

$$\phi_{\alpha,\beta} = a_0 + a_1\alpha + \cdots + a_n\alpha^n \mapsto a_0 + a_1\beta + \cdots + a_n\beta^n$$

is an isomorphism. Moreover, we have $\phi_{\alpha,\beta}|_F = \mathrm{id}_F$. (i.e. $\phi_{\alpha,\beta}(a) = a \quad \forall a \in F$.)

Example 1.

1. $F = \mathbb{R}, \alpha = i = \sqrt{-1}, m_{\alpha,\mathbb{R}}(x) = x^2 + 1$. The polynomial $x^2 + 1$ has another root $-i$. The discussion above shows that $\phi_{i,-i} : \mathbb{R}(i) = \mathbb{C} \to \mathbb{C} = \mathbb{R}(-i)$ defined by $a + bi \mapsto a - bi$, $a, b \in \mathbb{R}$ is an isomorphism from $\mathbb{C}$ to itself.

2. $F = \mathbb{Q}, \alpha = \sqrt[3]{2}, m_{\alpha,\mathbb{Q}}(x) = x^3 - 2$. The roots of $m_{\alpha,\mathbb{Q}}(x)$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{2}\zeta^2$, where $\zeta = e^{2\pi i/3}$. Then $\phi_{\alpha,\alpha\zeta} : a_0 + a_1\alpha + a_2\alpha^2 \mapsto a_0 + a_1\alpha\zeta + a_2(\alpha\zeta)^2$ is an isomorphism from $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\zeta)$.

Definition 1. If $\alpha, \beta \in \bar{F}$ have the same minimal polynomial over F, then we say they are **conjugates** over F.

Remark 2. $i, -i$ are conjugates over $\mathbb{R}$, but not conjugates over $\mathbb{C}$ sine the minimal polynomials over $\mathbb{C}$ are $x - i, x + i$.

The discussion above shows that if $\alpha, \beta \in \bar{F}$ are conjugates over F, then $\phi_{\alpha,\beta}$ is an isomorphism from $F(\alpha)$ to $F(\beta)$ such that $\phi_{\alpha,\beta}|_F = \mathrm{id}_F$. Conversely,

Proposition 1. Assume that $\alpha \in \bar{F}$ and ϕ is an isomorphism from $F(\alpha)$ to a subfield of $\bar{F}$ such that $\phi|_F = \mathrm{id}_F$. Then $\phi(\alpha)$ is a conjugate of α over F. (so $\phi = \phi_{\alpha,\beta}$.)

Proof.

Assume that $m_{\alpha,F}(x) = a_n x^n + \cdots + a_n$. We have

$$0 = \phi(0) = \phi(m_{\alpha,F}(\alpha)) = \phi(a_n\alpha^n + \cdots + a_0)$$

$$= \phi(a_n)\phi(\alpha)^n + \cdots + \phi(a_0) = a_n\phi(\alpha)^n + \cdots + a_0 = m_{\alpha,F}(\phi(\alpha))$$

$\Rightarrow \phi(\alpha)$ is a conjugate of α over F.

□

The discussion above shows that there is a 1-1, onto correspondence between {the conjugates of α over F (including α)} and {isomorphism ϕ from $F(\alpha)$ to a subfield of $\bar{F}$ such that $\phi|_F = \mathrm{id}_F$}.

Notation: Let $E \leq \bar{F}$. We let $\mathrm{Emb}(E/F)$ ={isomorphisms ϕ from E to subfields of $\bar{F}$ such that $\phi|_F = \mathrm{id}_F$}. We also let $\{E : F\} = |\mathrm{Emb}(E/F)|$. Recall that the number of distinct roots of $m_{\alpha,F}(x)$ = separable degree of $m_{\alpha,F}(x)$. (If char$F = 0$, then $m_{\alpha,F}(x)$ is separable. If char$F = p$, then by Prop 38 of Chap 13, $\exists! k \geq 0$, and a separable $g(x) \in F[x]$ such that $m_{\alpha,F}(x) = g(x^{p^k})$. Then separable degree of $m_{\alpha,F}(x)$ is $\deg g$.) Moreover, if $g(x) = (x - \beta_1)\cdots(x - \beta_d)$, then

$$m_{\alpha,F}(x) = g(x^{p^k}) = (x^{p^k} - \beta_1)\cdots(x^{p^k} - \beta_d) = (x^{p^k} - \alpha_1^{p^k})\cdots(x^{p^k} - \alpha_d^{p^k})$$
$$= ((x - \alpha_1)\cdots(x - \alpha_d))^{p^k}$$

where $\alpha_j \in \bar{F}$ satisfy $\alpha_j^{p^k} = \beta_j$. $\Rightarrow$ number of distinct roots of $m_{\alpha,F}(x) = \deg g(x) =$ separable degree of $m_{\alpha,F}(x)$. Thus, in the case of $E = F(\alpha)$,

$$\{F(\alpha) : F\} = \deg_s m_{\alpha,F}(x) \leq \deg m_{\alpha,F}(x) = [F(\alpha) : F]$$

Theorem 1. If $F \leq K \leq E$ are finite extensions, then

$$\{E : F\} = \{E : K\}\{K : F\}$$

Proof. Skipped. $\square$

Corollary 1. If E/F is a finite extension, then $\{E : F\} \leq [E : F]$.

Definition 2. (1) We say $\alpha \in \bar{F}$ is **separable** over F if $m_{\alpha,F}(x)$ is separable, i.e. if $\{F(\alpha) : F\} = [F(\alpha) : F]$.

(2) Let $E \leq \bar{F}$. We say E is a **separable extension** of F if $\forall \alpha \in E$, α is separable over F. (In the case E/F is a finite extension, this is equivalent to $\{E : F\} = [E : F]$.)

(3) Let $E \leq \bar{F}$. If $\forall \alpha \in E$, $m_{\alpha,F}(x)$ has only 1 distinct root in $\bar{F}$ (i.e. α has only 1 conjugate), then we say E/F is **purely inseparable**. For example, $F = \mathbb{F}_2(t), E = F(\sqrt{t})$. Then $m_{\sqrt{t},F}(x) = x^2 - t$ has only 1 distinct root $\Rightarrow \{F(\sqrt{t}) : F\} = 1 \Rightarrow F(\sqrt{t})/F$ is purely inseparable. (If $\alpha \in F(\sqrt{t})$ has 2 distinct conjugates over F, then $\{F(\alpha) : F\} = 2$, which is absurd since we already know $\{F(\alpha) : F\} = 1$.)

Theorem 2. If $\alpha, \beta \in \bar{F}$ are separable over F, then $F(\alpha, \beta)$ is a separable extension of F. In particular, $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ are all separable over F.

Proof.

We want to show $\{F(\alpha, \beta) : F\} = [F(\alpha, \beta) : F]$. We have

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

So it suffices to show that $\{F(\alpha, \beta : F\} = [F(\alpha, \beta) : F]$. Now $\{F(\alpha, \beta) : F(\alpha)\} = \deg_s m_{\beta,F(\alpha)}(x) =$ number of distinct roots of $m_{\beta,F(\alpha)}(x)$. Now $m_{\beta,F(\alpha)}(x) | m_{\beta,F}(x)$. By assumption that β is separable over F, $m_{\beta,F}(x) = m_{\beta,F(\alpha)}(x)$ has no repeated roots. $\Rightarrow \beta$ is separable over $F(\alpha)$ and $\{F(\alpha, \beta) : F(\alpha)\} = [F(\alpha, \beta) : F]$. $\square$

Corollary 2. Given $E \leq \bar{F}$, the set $E_s = \{\alpha \in \bar{E} : \alpha \text{ is separable over } F\}$ is a subfield of E.

Definition 3. E_s is called the **separable closure** of F in E and $\deg_s E/F := [E_s : F]$ is called the **separable degree** of E over F, $\deg_i E/F := [E : E_s]$ is the **inseparable degree**.

Remark 3. E/E_s is purely inseparable.