Intro to Algebra W3-2

fat

March 8, 2024

Proof of theorem $4 + 6$.

We first prove that $F(\alpha) = F[\alpha]$. Clearly, $F[\alpha] \subseteq F(\alpha)$. We now prove $F(\alpha) \subseteq F[\alpha]$. Let $f(\alpha)/g(\alpha) \in F(\alpha), g(\alpha) \neq 0$. Let $m(x) = m_{\alpha,F}(x)$. Now since $m(x)$ is irreducible over F and has the property that $p(\alpha) = 0 \Leftrightarrow m(x)|p(x)$. The assumption $g(\alpha) \neq 0$ implies $GCD(g(x), m(x)) = 1$. ($GCD(m(x), h(x))$ is either 1 or $m(x)$ since $m(x)$ is irreducible over F.) Then since $F[x]$ is a PID, $\exists a(x), b(x) \in F[x]$ s.t. $a(x)g(x) + b(x)m(x) = 1$.

$$\Rightarrow a(\alpha)g(\alpha) = 1 \Rightarrow g(\alpha)^{-1} = a(\alpha)$$
$$\Rightarrow \frac{f(\alpha)}{g(\alpha)} = f(\alpha)a(\alpha) \in F[\alpha]$$
$$\Rightarrow F(\alpha) \subseteq F[\alpha]$$

We now prove that

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

Define $\phi : F[x] \to F[\alpha]$ by $f(x) \mapsto f(\alpha)$. It is a surjective ring homomorphism with $ker(\phi) = \{f(x) \in F[x] : f(\alpha) = 0\}(= I_\alpha) = (m(x))$.

$$\Rightarrow F[x]/_{(m(x))} \simeq F[\alpha]$$

We now prove that $\{1, \alpha, ..., \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F, where $n = deg(m(x))$. For $f(\alpha) \in F[\alpha] = F(\alpha), \exists! q(x), r(x) \in F[x]$ s.t.

$$\begin{cases} f(x) = q(x)m(x) + r(x) \Rightarrow f(\alpha) = r(\alpha) \\ r(x) = 0 \text{ or } deg(r(x)) < deg(m(x)) \end{cases}$$

This implies that every element of $F[\alpha]$ can be written as $r(\alpha)$ for some $r(x) \in F[x]$ with $r(x) = 0$ or $deg(r) \leq n-1$. $\Rightarrow \{1, \alpha, ..., \alpha^{n-1}\}$ spans $F[\alpha] = F(\alpha)$. Now if $a_0, ..., a_{n-1}$ are elements of F s.t. $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = 0$. Then $m(x)|(a_0 + a_1x + \ldots + a_{n-1}x^{n-1})$ Thus, $\{1, \alpha, ..., \alpha^{n-1}\}$ is linearly independent over F. $\square$

Example 1. $F = \mathbb{R}, \alpha = i = \sqrt{-1}, m(x) = x^2 + 1$. According to the proof of the theoren, to find $(ai + b)^{-1}$, where $a, b \neq 0$. We shall find $s(x), t(x)$ s.t. $s(x)(ax + b) + t(x)(x^2 + 1) = 1$. Then $(ai + b)^{-1} = s(i)$. We have

$$x^2 + 1 = (a^{-1}x - \frac{b}{a^2})(ax + b) + 1 + \frac{b^2}{a^2}$$

$$\Rightarrow s(x) = \frac{x/a - b/a^2}{+b^2/a^2} = \frac{ax-b}{a^2+b^2}$$

$$(ai+b)^{-1} = s(i) = \frac{ai-b}{a^2+b^2}$$

Remark 1. If α is transcendental over F, then $F(\alpha) \simeq F(x)$.

Proposition 1. α is algebraic over $F \Leftrightarrow [F(\alpha) : F] < \infty$.

Proof.

We have proved $\Rightarrow$ in Theorem 4 + 6. Conversely, assume that $[F(\alpha) : F] = n < \infty$. Consider $1, \alpha, ..., \alpha^n$. Since $\#\{1, \alpha, ..., \alpha^n\} = n + 1 > dim_F(F(\alpha)) = n$, $\exists a_0, ..., a_n \in F$, not all zero s.t. $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. $\Rightarrow \alpha$ is algebraic over F. $\square$

Corollary 1. If K/F is a finite extension, then K/F is an algebraic extension. (The converse is not true in general.)

Theorem 1. Let $L/K/F$. Then $[L : F] = [L : K][K : F]$.

Example 2. Claim $\sqrt{2} \ni \mathbb{Q}(2^{1/3})$.

Proof.

iWe have $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$. Now if $\sqrt{2} \in \mathbb{Q}(2^{1/3})$, then $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(2^{1/3})$ and $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$, which is impossible. $\square$

Proof of Theorem.

Note that if any of the degree is ∞, then both sides are equal to ∞. So we assume that $[L : K] = m, [K : F] = n$ are finite. Let $\{\alpha, ..., \alpha_m\}$ be a basis for L over K, $\{\beta_1, ..., \beta_n\}$ be a basis for K over F.

Claim. $\{\alpha_i\beta_j : i = 1, ..., m, j = 1, ..., n\}$ is a basis for L over F.

Proof.

Given $r \in L$. Since $\{\alpha_1, .., \alpha_n\}$ is a basis for L/K, we have

$$r = \sum_{i=1}^{m} a_i\alpha_i \text{ for some } a_i \in K$$

Then because $\{\beta_1, ..., \beta_n\}$ is a basis for K over F, we have for each i

$$a_i = \sum_{j=1}^{n} b_{ij}\beta_j \text{ for some } b_{ij}$$

$$\Rightarrow r = \sum_{i=1}^{m}(\sum_{j=1}^{n} b_{ij}\beta_j)\alpha_i \in \text{ span of } \{\alpha_i\beta_j\}$$

$$\Rightarrow L \subseteq span\{\alpha_i\beta_j\}$$

Now assume that c_{ij} are elements of F s.t.

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}\alpha_i\beta_j = 0$$

Then

$$0 = \sum_{i=1}^{m}(\sum_{j=1}^{n} c_{ij}\beta_j)\alpha_i$$

Since $\{\alpha_1, ..., \alpha_m\}$ is linearly independent over K. We have $\sum_{j=1}^{n} c_{ij}\beta_j = 0 \ \forall i$. Then since $\{\beta_1, ..., \beta_n\}$ is linearly independent over F, we have $c_{ij} = 0 \ \forall i, j$. ...

$\square$

$\square$