1.3 Lecture 4: Theorem of the primitive element

Proposition 1.8. *Let $\mathbb{F}$ be a field and let $\overline{\mathbb{F}}$ be an algebraically closed field containing $\mathbb{F}$. Let $\alpha, \beta \in \overline{\mathbb{F}}$ and let $c \in \mathbb{F}$. Let $\alpha_1, \ldots, \alpha_r$ be the roots of $m_{\alpha,\mathbb{F}}(x)$ and let $\beta_1, \ldots, \beta_s$ be the roots of $m_{\beta,\mathbb{F}}(x)$ so that*

$$m_{\alpha,\mathbb{F}}(x) = (x-\alpha_1)\cdots(x-\alpha_r) \qquad \text{and} \qquad m_{\beta,\mathbb{F}}(x) = (x-\beta_1)\cdots(x-\beta_s) \qquad \text{in } \overline{\mathbb{F}}[x],$$

and $\alpha = \alpha_1$ and $\beta = \beta_1$. Assume that

$$c \notin \left\{ \frac{-(\beta-\beta_j)}{(\alpha-\alpha_i)} \mid i \in \{1,\ldots,r\}, j \in \{1,\ldots,s\} \text{ with } (i,j) \neq (1,1) \right\}.$$

then

$$\mathbb{F}(\alpha,\beta) = \mathbb{F}(\alpha + c\beta).$$

Proof.

To show: (a) $\mathbb{F}(\alpha+c\beta) \subseteq \mathbb{F}(\alpha,\beta)$.
(b) $\mathbb{F}(\alpha,\beta) \subseteq \mathbb{F}(\alpha+c\beta)$.

(a) To show: $\alpha + c\beta \in \mathbb{F}(\alpha,\beta)$.

(b) To show: (ba) $\alpha \in \mathbb{F}(\alpha+c\beta)$
(bb) $\beta \in \mathbb{F}(\alpha+c\beta)$.

(ba) To show: $m_{\alpha,\mathbb{F}(\alpha+c\beta)}(x) = x - \alpha$.

Since

$$m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}(\alpha,\beta)[x] \qquad \text{and} \qquad h(x) = m_{\beta,\mathbb{F}}(\beta + c\alpha - cx) \in \mathbb{F}(\alpha,\beta)[x]$$

and

$$m_{\alpha,\mathbb{F}}(\alpha) = 0, \qquad \text{and} \qquad h(\alpha) = 0,$$

then $m_{\alpha,\mathbb{F}(\alpha+c\beta)}(x)$ is a common divisor of $m_{\alpha,\mathbb{F}}(x)$ and $h(x) = m_{\beta,\mathbb{F}}(\beta + c\alpha - cx)$.
As elements of $\overline{\mathbb{F}}[x]$, $m_{\alpha,\mathbb{F}}(x)$ factors as $m_{\alpha\,\mathbb{F}}(x) = (x-\alpha)(x-\alpha_2)\ldots(x-\alpha_r)$ and $h(x)$ factors as

$$h(x) = (\beta + c\alpha - cx - \beta_1)\cdots(\beta + c\alpha - cx - \beta_s).$$

Since $c^{-1}\beta + \alpha - c^{-1}\beta_j \neq \alpha_i$ except when $i = 1$ and $j = 1$ then

$$\gcd(m_{\alpha,\mathbb{F}}(x), h(x)) = x - \alpha.$$

So $m_{\alpha,\mathbb{F}(\alpha+c\beta)}(x) = x - \alpha$.
So $\alpha \in \mathbb{F}(\alpha + c\beta)$. □

Theorem 1.9. *Let $\mathbb{F}$ be a field and let $\mathbb{K}$ be the splitting field of a polynomial $f(x) \in \mathbb{F}[x]$. Then there exists $\gamma \in \mathbb{F}$ such that*

$$\mathbb{K} = \mathbb{F}(\gamma).$$

Proof. Let $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ be the roots of $f(x)$ so that $f(x) = (x-\alpha_1)\cdots(x-\alpha_k)$ in $\mathbb{K}[x]$. Then

$$\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_k).$$

By induction on ℓ, the theorem of the primitive element gives that if $\ell \in \{1,\ldots,k\}$ then there exists $\gamma_\ell \in \mathbb{K}$ such that

$$\mathbb{F}(\alpha_1,\ldots,\alpha_\ell) = \mathbb{F}(\gamma_{\ell-1}, \alpha_\ell) = \mathbb{F}(\gamma_\ell).$$

Let $\gamma = \gamma_k$. □