7. Splitting fields (Chapter 16.1)

F-field

Definition 7.1. Let $f(x) \in F[x]$ with $\deg(f) \geq 1$. An extension field E of F is called a *splitting field* of $f(x)$ over F if:
(1) $f(x)$ factors into linear factors $f(x) = c(x-a_1)\cdots(x-a_n)$ in $E[x]$, and
(2) if $F \subseteq K \subsetneq E$ are field extensions, then $f(x)$ does not factor into linear factors in $K[x]$.

Remark 7.2. Let $f(x) \in F[x]$.
(1) A splitting field of f always exist. Let $a_1, \dots, a_n \in \overline{F}$ be the roots of f in the algebraic closure $\overline{F}$ of F. Then $F(a_1, \dots, a_n)$ is a splitting field of f.
(2) Let E be a splitting field of $f(x)$ satisfying $E \subseteq \overline{F}$. Write
$$f(x) = c(x-a_1)\cdots(x-a_n) \quad \text{in } E[x].$$
Then $F(a_1, \dots, a_n) \subseteq E$ and clearly f factors into linear factors in $F(a_1, \dots, a_n)[x]$. We conclude that $E = F(a_1, \dots, a_n)$.
(3) We have $f(a_i) = 0$ for every $1 \leq i \leq n$. Hence each a_i is algebraic over F. Since $E = F(a_1, \dots, a_n)$ is finitely generated, we conclude that $[E:F] < \infty$ and so $F \subseteq E$ is algebraic by Theorem 5.8.

Example 7.3. (1) $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Both $\mathbb{Q}[x]/(x^2-2)$ and $\mathbb{Q}(-\sqrt{2}, \sqrt{2}) = \mathbb{Q}(\sqrt{2})$ are splitting fields of $f(x)$. We will see that they are isomorphic.
(2) A splitting field of $x^2+1 \in \mathbb{R}[x]$ is $\mathbb{R}(-i, i) = \mathbb{C}$.
(3) A splitting field of $x^2+1 \in \mathbb{Q}[x]$ is $\mathbb{Q}(-i, i) = \mathbb{Q}(i)$.

(4) We compute in $\mathbb{C}[x]$:

$$x^4-3=(x^2-\sqrt{3})(x^2+\sqrt{3})=(x-3^{1/4})(x+3^{1/4})(x-i3^{1/4})(x+i3^{1/4}).$$

Hence a splitting field of x^4-3 over $\mathbb{Q}$ is $\mathbb{Q}(3^{1/4}, i3^{1/4})=\mathbb{Q}(3^{1/4}, i)$.
Notice that x^4-3 is irreducible over $\mathbb{Q}$ by Eisenstein criterion for $p=3$. Hence $[\mathbb{Q}(3^{1/4}):\mathbb{Q}]=4$ by Theorem 4.6. Moreover we have that $i\notin\mathbb{Q}(3^{1/4})$ and that the minimal polynomial of i over $\mathbb{Q}(3^{1/4})$ is x^2+1. Hence $[\mathbb{Q}(3^{1/4}, i):\mathbb{Q}(3^{1/4})]=2$. We conclude that

$$[\mathbb{Q}(3^{1/4}, i):\mathbb{Q}]=[\mathbb{Q}(3^{1/4}, i):\mathbb{Q}(3^{1/4})][\mathbb{Q}(3^{1/4}):\mathbb{Q}]=2\cdot 4=8.$$

On the other hand, a splitting field of x^4-3 over $\mathbb{R}$ is $\mathbb{R}(3^{1/4}, i3^{1/4})=\mathbb{R}(i)=\mathbb{C}$.

Let $f(x)\in F[x]$ with $\deg(f)\geq 1$. Remark 7.2 tells us that if there is a unique splitting field of $f(x)$ inside the algebraic closure $\bar{F}$ of F. However, we may be able to find another splitting field of F, not necessarily lying inside $\bar{F}$. The following theorem tells us that even then there is a unique splitting field of F over F, up to an F-isomorphism.

<u>Theorem 7.4.</u> Let E and K be two splitting fields of $f(x)\in F[x]$ over F. Then $\exists$ an F-isomorphism $\sigma: E\to K$.

<u>Proof.</u> Consider the field extensions $F\subseteq E\subseteq\bar{E}$. Let $a_1,\dots,a_n\in\bar{E}$ be the roots of $f(x)$ in $\bar{E}$. By Remark 7.2 we obtain that $E=F(a_1,\dots,a_n)$ and that $F\subseteq E$ is algebraic. Since $E\subseteq\bar{E}$ is also algebraic by definition, we obtain that $F\subseteq\bar{E}$ is algebraic by Lemma 6.8. Since $\bar{E}$ is algebraically closed, we conclude that $\bar{E}$ is an algebraic closure of F.
Similarly, we obtain that $K=F(b_1,\dots,b_m)$ where $b_1,\dots,b_m\in\bar{E}$ are

the roots of $f(x)$ in $\bar{K}$ and that $\bar{K}$ is an algebraic closure of F. By Theorem 6.6 there exists an F-isomorphism $\varphi: \bar{E} \to \bar{K}$. We claim that $\sigma = \varphi|_E$ is an F-isomorphism $E \to K$. Since $\sigma|_F = \varphi|_F = id_F$ and σ is a nonzero ring homomorphism between fields, it is enough to show that $\text{im}\,\sigma = K$. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. For $1 \le i \le n$ we have $f(\alpha_i) = 0$ and so

$$0 = \sigma(f(\alpha_i)) = \sigma(a_0 + a_1\alpha_i + \cdots + a_n\alpha_i^n) = \sigma(a_0) + \sigma(a_1)\sigma(\alpha_i) + \cdots + \sigma(a_n)\sigma(\alpha_i)^n$$
$$= a_0 + a_1\sigma(\alpha_i) + \cdots + a_n\sigma(\alpha_i)^n = f(\sigma(\alpha_i))$$

and so $\sigma(\alpha_i) \in \bar{E}$ is a root of $f(x)$. Hence $\sigma(\alpha_i) \in \{\beta_1, \ldots, \beta_n\}$ and since σ is injective, σ gives a bijection

$$\{\alpha_1, \ldots, \alpha_n\} \xleftrightarrow{1:1} \{\beta_1, \ldots, \beta_n\}.$$

Since φ is an F-isomorphism, we obtain $\sigma(f(\alpha_1, \ldots, \alpha_n)) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$ (exercise). Then $\text{im}\,\sigma = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = f(\beta_1, \ldots, \beta_n) = K$, as required. □

Example 7.5(1) (June 2015, Problem 2a) Find the splitting field E of $f(x) = x^3 - 2$ over $\mathbb{Q}$. What is $[E:\mathbb{Q}]$?

The roots of f in $\mathbb{C}$ are $2^{1/3}$, $\alpha 2^{1/3}$, $\alpha^2 2^{1/3}$, where $\alpha = e^{\frac{2\pi i}{3}}$. So

$$E = \mathbb{Q}(2^{1/3}, \alpha 2^{1/3}, \alpha^2 2^{1/3}) = \mathbb{Q}(2^{1/3}, \alpha).$$

We compute

$$[\mathbb{Q}(2^{1/3}, \alpha) : \mathbb{Q}] = [\mathbb{Q}(2^{1/3}, \alpha) : \mathbb{Q}(2^{1/3})] \cdot [\mathbb{Q}(2^{1/3}) : \mathbb{Q}] \quad (*)$$

Since f is irreducible over $\mathbb{Q}$ (Eisenstein criterion for $p=2$) and monic, we conclude that f is the minimal polynomial of $2^{1/3}$ over $\mathbb{Q}$. Then $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$, with a $\mathbb{Q}$-basis of $\mathbb{Q}(2^{1/3})$ given by $\{1, 2^{1/3}, 2^{2/3}\}$.

On the other hand, α is a root of $x^3 - 1 = (x-1)(x^2+x+1)$, and so it is a root of $x^2+x+1 \in \mathbb{Q}(2^{1/3})[x]$. Since x^2+x+1 has no roots in $\mathbb{Q}(2^{1/3})$, it is the minimal polynomial of α over $\mathbb{Q}(2^{1/3})$. Then $[\mathbb{Q}(2^{1/3}, \alpha) : \mathbb{Q}(2^{1/3})] = 2$, with a $\mathbb{Q}(2^{1/3})$-basis of $\mathbb{Q}(2^{1/3}, \alpha)$ given by $\{1, \alpha\}$.

By $(*)$ we conclude that $[\mathbb{Q}(2^{1/3}, \alpha) : \mathbb{Q}] = 2 \cdot 3 = 6$, with

a $\mathbb{Q}$-basis of $\mathbb{Q}(2^{1/3},\alpha)$ given by $\{1, 2^{1/3}, 2^{2/3}, \alpha, \alpha 2^{1/3}, \alpha 2^{2/3}\}$.

(2) Let $p \geq 3$ be prime and $f(x) = x^p - 1 \in \mathbb{Q}[x]$. Then

$$f(x) = (x-1)(1 + x + \cdots + x^{p-1}) = (x-1)\Phi_p(x),$$

where $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ (Example 3.11(2)). Notice that $\zeta_p = e^{\frac{2\pi i}{p}}$ is a root of $\Phi_p(x)$. Moreover, for $x \neq 1$ we have $\Phi_p(x) = \frac{x^{p-1}}{x-1}$. For $j \geq 0$ we have $\zeta_p^j = 1 \Rightarrow e^{\frac{2\pi i j}{p}} = 1 \Rightarrow p \mid j$ and so for $1 \leq j \leq p-1$ we have

$$\Phi_p(\zeta_p^j) = \frac{(\zeta_p^j)^p - 1}{\zeta_p^j - 1} = \frac{\zeta_p^{pj} - 1}{\zeta_p^j - 1} = 0.$$

Hence $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ are all roots of Φ_p. We claim that $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ is a complete and irredundant set of roots of f. Since $\deg(f) = p$, it is enough to show that $1 \leq j \neq k \leq p \Rightarrow \zeta_p^j \neq \zeta_p^k$. Assume $j > k$. Then $\zeta_p^j = \zeta_p^k \Rightarrow \zeta_p^{j-k} = 1 \Rightarrow p \mid j-k$, a contradiction. Hence the splitting field of f is

$$\mathbb{Q}(1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}) = \mathbb{Q}(\zeta_p),$$

and $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$ (Example 4.7(3)).

(3) Let $q(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$. By Example 4.7(2) q is irreducible. Let α be a root of q in its splitting field. Then by polynomial division we obtain

$$x^3 + 2x + 1 = (x - \alpha)(x^2 + \alpha x + (\alpha^2 + 2))$$

Using the quadratic formula we find that $\alpha + 2$ and $\alpha + 1$ are roots of $x^2 + \alpha x + (\alpha^2 + 2)$. Hence

$$q(x) = (x - \alpha)(x - (\alpha + 1))(x - (\alpha + 2))$$

and so $\mathbb{Z}_3(\alpha)$ is the splitting field of q. Then $[\mathbb{Z}_3(\alpha) : \mathbb{Z}_3] = \deg(q) = 3$, and for an explicit description of $\mathbb{Z}_3(\alpha)$ see Example 4.7(2).