Solutions to David A.Cox "Galois Theory"

Richard Ganaye

October 12, 2021

5 Chapter 5

5.1 NORMAL AND SEPARABLE EXTENSIONS

Ex. 5.1.1 *Show that a splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega, \sqrt[3]{2}), \omega = e^{2\pi i/3}$.*

Proof. The roots of $x^3 - 2$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$. A splitting field of $x^3 - 2$ over $\mathbb{Q}$ is thus $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) \subset \mathbb{C}$.

As $\omega, \sqrt[3]{2} \in \mathbb{Q}(\omega, \sqrt[3]{2})$, and as $\mathbb{Q}(\omega, \sqrt[3]{2})$ is a field, $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ are elements of $\mathbb{Q}(\omega, \sqrt[3]{2})$. Since $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$,

$$\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) \subset \mathbb{Q}(\omega, \sqrt[3]{2}).$$

Moreover $\omega = \omega\sqrt[3]{2}/\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ et $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$. As $\mathbb{Q}(\omega, \sqrt[3]{2})$ is the smallest subfield of $\mathbb{C}$ containing these two elements,

$$\mathbb{Q}(\omega, \sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}).$$

These two subfields are identical.

Conclusion : a splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega, \sqrt[3]{2})$. $\square$

Ex. 5.1.2 *Prove that $f \in F[x]$ splits completely over F if and only if F is the splitting field of f over F.*

Proof. Suppose that $f \in F[x]$ splits completely over F:

$$f = a(x - x_1) \cdots (x - x_n),\ x_i \in F, i = 1, \ldots, n.$$

The roots of f are so $x_1, \ldots, x_n$, with possibly some repetitions. As $x_i \in F,\ i = 1, \ldots, n$, $F(x_1, \ldots, x_n) = F$. By Definition 5.1.1, a splitting field of f over F is $F(x_1, \ldots, x_n)$.

Conversely, suppose that a splitting field of f over F is F. Let $x_1, \ldots, x_n$ the roots of f in this splitting field of f. As this field is F, $x_1, \ldots, x_n \in F$, thus

$$f = a(x - x_1) \cdots (x - x_n),\ x_i \in F,\ i = 1, \ldots, n.$$

So f splits completely over F. $\square$

Ex. 5.1.3 *Prove that an extension $F \subset L$ of degree 2 is a splitting field.*

Proof. Suppose that $[L : F] = 2$. Then $F \subsetneq L$, so there exists $\alpha \in L$ such that $\alpha \notin F$.

As $\alpha \notin F$, $F \subsetneq F(\alpha)$, thus $[F(\alpha) : F] > 1$. Since $F(\alpha) \subset L$, $[F(\alpha) : F] \leq 2$, hence $[F(\alpha) : F] = 2$, so $F(\alpha) = L$. Let f be the minimal polynomial of α over F. Then $\deg(f) = [F(\alpha) : F] = 2$, so $f = x^2 + ax + b,\ a, b \in F$.

Since $\alpha \in L$ is a root of $x^2+ax+b \in F[x] \subset L[x]$, there exists a polynomial $q(x) \in L[x]$ such that $x^2 + ax + b = (x - \alpha)q(x)$, where $\deg(q) = 1$ and q is monic. Therefore there exists $\beta \in L$ such that $q(x) = x - \beta$. So $f = (x - \alpha)(x - \beta)$ splits completely over L, and since $\beta \in L$, $L = F(\alpha) = F(\alpha, \beta)$. L is a splitting field of f.

Conclusion: Every quadratic extension L of a field F is a splitting field (so is a normal extension). $\square$

Ex. 5.1.4 *Find the splitting field of $x^6 - 1 \in \mathbb{Q}[x]$.*

Proof. The set of roots of x^6-1 in $\mathbb{C}$ is $S = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$, where $\zeta = e^{2i\pi/6} = e^{i\pi/3} = -\omega^2$. As $\omega^3 = 1$,

$$S = \{1, -\omega^2, \omega, -1, \omega^2, -\omega\}.$$

the splitting field of $x^6 - 1$ over $\mathbb{Q}$ (included in $\mathbb{C}$) is so $\mathbb{Q}(1, -\omega^2, \omega, -1, \omega^2, -\omega) = \mathbb{Q}(S)$.

As $S \subset \mathbb{Q}(\omega)$, $\mathbb{Q}(S) \subset \mathbb{Q}(\omega)$. Conversely, $\omega \in S$, thus $\mathbb{Q}(\omega) \subset \mathbb{Q}(S)$.

Conclusion : the splitting field of $x^6 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega)$. $\square$

Ex. 5.1.5 *We showed in Section 4.1 that $f = x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$. Show that $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is the splitting field of f over $\mathbb{Q}$.*

Proof. Recall the computing of Exercise 4.1.8(b) :

$$\begin{aligned}
f &= (x - \sqrt{2} - \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} + \sqrt{3}) \\
&= [(x - \sqrt{3})^2 - 2][(x + \sqrt{3})^2 - 2] \\
&= (x^2 - 2\sqrt{3}x + 1)(x^2 - 2\sqrt{3}x + 1) \\
&= (x^2 + 1)^2 - (2\sqrt{3}x)^2 \\
&= x^4 - 10x^2 + 1
\end{aligned}$$

The splitting field of f over $\mathbb{Q}$ is thus

$$K = \mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}).$$

As $\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then

$$K \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Moreover,

$$\begin{aligned}
\sqrt{2} &= \frac{1}{2}\left[(\sqrt{2} + \sqrt{3}) - (-\sqrt{2} + \sqrt{3})\right] \in K, \\
\sqrt{3} &= \frac{1}{2}\left[(\sqrt{2} + \sqrt{3}) - (\sqrt{2} - \sqrt{3})\right] \in K,
\end{aligned}$$

thus

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset K.$$

So $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Moreover, the Example 4.3.9 shows that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(Or a direct proof is given in section 4.2, since $\sqrt{2} = \frac{1}{2}(\alpha^3 - 9\alpha)$, where $\alpha = \sqrt{2} + \sqrt{3}$, and $\sqrt{3} = \alpha - \sqrt{2}$, so $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.)

Conclusion: the splitting field of $x^4 - 10x^2 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. □

Ex. 5.1.6 *Let $f \in \mathbb{Q}[x]$ be the minimal polynomial of $\alpha = \sqrt{2 + \sqrt{2}}$*

(a) Show that $f = x^4 - 4x^2 + 2$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

(b) Show that $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$.

Proof. (a) Let $\alpha = \sqrt{2 + \sqrt{2}}$.

Then $\alpha^2 = 2 + \sqrt{2}, \alpha^2 - 2 = \sqrt{2}, (\alpha^2 - 2)^2 - 2 = 0, \alpha^4 - 4\alpha^2 + 2 = 0$.

So α is a root of

$$f = x^4 - 4x^2 + 2.$$

The computing of the roots in $\mathbb{C}$ of f gives (cf Ex. 4.3.2) :

$$\begin{aligned} f(\beta) = 0 &\iff (\beta^2 - 2)^2 = 2 \\ &\iff \beta^2 = 2 + \varepsilon\sqrt{2},\ \varepsilon \in \{-1, 1\} \\ &\iff \beta = \varepsilon'\sqrt{2 + \varepsilon\sqrt{2}},\ \varepsilon, \varepsilon' \in \{-1, 1\} \\ &\iff \beta \in \left\{\sqrt{2 + \sqrt{2}}, -\sqrt{2 + \sqrt{2}}, \sqrt{2 - \sqrt{2}}, -\sqrt{2 - \sqrt{2}}\right\}. \end{aligned}$$

Thus

$$f = \left(x - \sqrt{2 + \sqrt{2}}\right)\left(x + \sqrt{2 + \sqrt{2}}\right)\left(x - \sqrt{2 - \sqrt{2}}\right)\left(x + \sqrt{2 - \sqrt{2}}\right). \quad (1)$$

We show that f is irreducible over $\mathbb{Q}$. The Schönemann-Eisenstein Criterion, with $p = 2$ applies to the polynomial $f = x^4 - 4x^2 + 2 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ $(2 \nmid a_4 = 1, 2 \mid a_3 = 0, 2 \mid a_2 = -4, 2 \mid a_1 = 0, 2 \mid a_0 = 2, 2^2 \nmid a_0 = 2)$. f is so irreducible over $\mathbb{Q}$.

Consequently, f of degree 4, is the minimal polynomial of $\alpha = \sqrt{2 + \sqrt{2}}$ over $\mathbb{Q}$, so,

$$\left[\mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\right) : \mathbb{Q}\right] = 4.$$

(b) The splitting field of f over $\mathbb{Q}$ is

$$K = \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}, -\sqrt{2 + \sqrt{2}}, \sqrt{2 - \sqrt{2}}, -\sqrt{2 - \sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}, \sqrt{2 - \sqrt{2}}\right).$$

Let $\alpha = \sqrt{2 + \sqrt{2}}, \gamma = \sqrt{2 - \sqrt{2}}$. Then $K = \mathbb{Q}(\alpha, \gamma)$.

Note that $\alpha\gamma = \sqrt{4 - 2} = \sqrt{2}$

Moreover $\alpha^2 = 2 + \sqrt{2}, \gamma^2 = 2 - \sqrt{2}$, thus $\alpha^2 - \gamma^2 = 2\sqrt{2} = 2\alpha\gamma$.

$$\alpha^2 - \frac{2}{\alpha^2} = 2\alpha\gamma.$$

So

$$\gamma = \frac{1}{2}\left(\alpha - \frac{2}{\alpha^3}\right) \in \mathbb{Q}(\alpha).$$

Consequently $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \gamma)$ is the splitting field of f over $\mathbb{Q}$. The splitting field of $x^4 - 4x^2 + 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2+\sqrt{2}})$, of degree 4 over $\mathbb{Q}$.

Note: With Sage, we obtain $\gamma = \frac{1}{2}\left(\alpha - \frac{2}{\alpha^3}\right) = \alpha^3 - 3\alpha$, and the factorization

$$x^4 - 4x^2 + 2 = (x - \alpha)(x + \alpha)(x - \alpha^3 + 3\alpha)(x + \alpha^3 - 3\alpha).$$

□

Ex. 5.1.7 *Let $f = x^3 - x + 1 \in \mathbb{F}_3[x]$.*

(a) Show that f is irreducible over $\mathbb{F}_3$.

(b) Let L be the splitting field of f over $\mathbb{F}_3$. Prove that $[L : \mathbb{F}_3] = 3$.

(c) Explain why L is a field with 27 elements.

Proof. (a) Let $f = x^3 - x + 1 \in \mathbb{F}_3[x]$.

As $\deg(f) = 3$, to prove the irreducibility of$f$, it is sufficient to show that f has no root in $\mathbb{F}_3$. This is the case, since every element α of $\mathbb{F}_3$ is a root of $x^3 - x$ (little Fermat's theorem), so $\alpha^3 - \alpha + 1 = 1 \neq 0 :\ f(0) = f(1) = f(2) = 1$.

$f = x^3 - x + 1$ is irreducible over $\mathbb{F}_3$.

(b) Let L the splitting of f over $\mathbb{F}_3$, and α a root of f in L. As the characteristic of $\mathbb{F}_3$ is 3,

$$\begin{aligned} f(x+1) &= (x+1)^3 - (x+1) + 1 \\ &= (x^3 + 1) - (x+1) + 1 \\ &= x^3 - x + 1 \\ &= f(x) \end{aligned}$$

Consequently, $\alpha, \alpha+1, \alpha+2$ are the distinct roots of f, since $0, 1, 2$ are distinct in $\mathbb{F}_3$:

$$f(x) = (x - \alpha)(x - \alpha - 1)(x - \alpha - 2).$$

As $\alpha + 1, \alpha + 2 \in \mathbb{F}_3(\alpha)$,

$$L = \mathbb{F}_3(\alpha, \alpha+1, \alpha+2) = \mathbb{F}_3(\alpha).$$

$f = x^3 - x + 1$ being the minimal polynomial of α, $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = \deg(f) = 3$.

In conclusion, $L = \mathbb{F}_3(\alpha)$ is the splitting field of $x^3 - x + 1$ over $\mathbb{F}_3$. Its degree is 3 over $\mathbb{F}_3$. As a vector space over $\mathbb{F}_3$, its dimension is 3, so $L \simeq \mathbb{F}_3^3$, so its cardinality is $3^3 = 27$.

□

Ex. 5.1.8 *Let n be a positive integer. Then the polynomial $f = x^n - 2$ is irreducible over $\mathbb{Q}$ by the Schönemann-Eisenstein Criterion for the prime 2.*

(a) Determine the splitting field L of f over $\mathbb{Q}$.

(b) Show that $[L : \mathbb{Q}] = n(n-1)$ when n is prime.

Proof. (a) The set of the roots of $x^n - 2 \in \mathbb{Q}[x]$ is $S = \{\zeta^k \sqrt[n]{2},\ k = 0, \cdots, n-1\}$, where $\zeta = e^{2i\pi/n}$: the splitting field L of $x^n - 2$ over $\mathbb{Q}$ is so $\mathbb{Q}(S)$.

As $\zeta = \zeta \sqrt[n]{2} / \sqrt[n]{2} \in \mathbb{Q}(S)$, $L = \mathbb{Q}(\zeta, \sqrt[n]{2})$.

(b) Suppose that n is prime.

As $f = x^n - 2$ is irreducible over $\mathbb{Q}$, f is the minimal polynomial of $\sqrt[n]{2}$ over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = \deg(f) = n$.

As n is prime, $1 + x + \cdots + x^{n-1}$ is irreducible over $\mathbb{Q}$, thus $[\mathbb{Q}(\zeta) : \mathbb{Q}] = n - 1$.

$$\begin{tikzcd}
 & L = \mathbb{Q}(\sqrt[n]{2}, \zeta) & \\
\mathbb{Q}(\sqrt[n]{2}) \arrow[ur] & & \mathbb{Q}(\zeta) \arrow[ul] \\
 & \mathbb{Q} \arrow[ul, "n"] \arrow[ur, "n-1"'] &
\end{tikzcd}$$

From the Tower Theorem,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[n]{2})][\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n\,[L : \mathbb{Q}(\sqrt[n]{2})]$$
$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta)][Q(\zeta) : \mathbb{Q}] = (n-1)[L : \mathbb{Q}(\zeta)] \qquad (2)$$

Thus $n \mid [L : \mathbb{Q}]$ and $n - 1 \mid [L : \mathbb{Q}]$.

As $n, n-1$ are relatively prime,

$$n(n-1) \mid [L : \mathbb{Q}]. \qquad (3)$$

Moreover, the minimal polynomial p of $\sqrt[n]{2}$ over $\mathbb{Q}(\zeta)$ divides $x^n - 2 \in \mathbb{Q}[x] \subset \mathbb{Q}(\zeta)[x]$, thus $[L : \mathbb{Q}(\zeta)] = \deg(p) \le n$. By (2), $[L : \mathbb{Q}] \le n(n-1)$, and by (3) $n(n-1) \mid [L : \mathbb{Q}]$, thus

$$[L : \mathbb{Q}] = n(n-1).$$

□

Ex. 5.1.9 *Let $f \in F[x]$ have degree $n > 0$, and let L be the splitting field of f over F.*

(a) Suppose that $[L : F] = n!$. Prove that f is irreducible over F.

(b) Show that the converse of part (a) is false.

Proof. (a) Let $f \in F[x], \deg(f) = n > 0$, and L be the splitting field of f over F.

Suppose that f is reducible over F. We show then that $[L : F] < n!$.

In this case, $f = gh$, where $1 \le k = \deg(g) \le n-1$ (then $\deg(h) = n-k$).

The roots $\alpha_1, \cdots, \alpha_k$ of g, and the roots $\beta_1, \cdots, \beta_{n-k}$ of h, are the roots of f. They are thus in L, and

$$L = F(\alpha_1, \cdots, \alpha_k, \beta_1, \cdots, \beta_{n-k}).$$

Let $K = F(\alpha_1, \cdots, \alpha_k)$. This is the splitting field of g over F. Theorem 5.1.5 shows that $[K : F] \le k!$.

As $L = K(\beta_1, \cdots, \beta_{n-k})$ is the splitting field of h over K, the same theorem shows that $[L : K] \le (n-k)!$.

Hence

$$[L : F] = [L : K]\ [K : F] \le k!(n-k)!.$$

If $1 \le k \le n-1$,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \prod_{i=0}^{k-1} \frac{n-i}{k-i} > 1,$$

thus, for the same values of k,

$$k!(n-k)! < n!.$$

Consequently $[L : F] < n!$. In particular $[L : F] \neq n!$. The contraposition gives thus

$$[L : F] = n! \ \Rightarrow f \text{ is irreducible over } F.$$

(b) We give a counterexample of the converse : by Exercise 5, $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is the splitting field of the irreducible polynomial $f = x^4 - 10x^2 + 1$, but $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4 \neq 4! = 24.$

$\square$

Ex. 5.1.10 *Let $F \subset L$ be the splitting field of $f \in F[x]$, and let K be a field such that $F \subset K \subset L$. Prove that $K \subset L$ is the splitting field of some polynomial in $K[x]$.*

Proof. If $F \subset K \subset L$, and if L is the splitting field of f over K, then L is the splitting field of the same polynomial f over K.

Indeed, L contains the roots $\alpha_1, \ldots, \alpha_n$ of f, and $L = F(\alpha_1, \ldots \alpha_n)$. Moreover $f = c(x - \alpha_1) \cdots (x - \alpha_n), c \in F$.

$F \subset K \subset L$ and $\alpha_1, \ldots, \alpha_n \in L$, thus $K(\alpha_1, \ldots, \alpha_n) \subset L = F(\alpha_1, \ldots, \alpha_n) \subset K(\alpha_1, \ldots, \alpha_n)$. Consequently, $L = K(\alpha_1, \ldots, \alpha_n)$, and f splits completely over the extension $K \subset L$ since $c \in F \subset K$. The conditions (a), (b) of definition 5.1.1 are filled: L is the splitting field of f over K.

Note: therefore, if $F \subset K \subset L$, and if $F \subset L$ is a normal extension, so is $K \subset L$. $\square$

Ex. 5.1.11 *Suppose that $f \in F[x]$ is irreducible of degree $n > 0$, and let L be the splitting field of f over F.*

(a) Prove that $n \mid [L : F]$.

(b) Give an example to show that $n = [L : F]$ can occur in part (a).

Proof. (a) Let $\alpha \in L$ a root of f. Then $F \subset F(\alpha) \subset L$, thus

$$[L : F] = [L : F(\alpha)]\ [F(\alpha) : F].$$

As f is the minimal polynomial of α, $[F(\alpha) : F] = \deg(f) = n$, thus $n \mid [L : F]$.

(b) In Exercise 6, we have seen that $f = x^4 - 4x^2 + 2$, of degree $n = 4$, has for splitting field $L = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, of degree 4 over $\mathbb{Q}$. Here $[L : \mathbb{Q}] = 4 = \deg(f)$, the equality in relation (a) is so a possibility.

□

Ex. 5.1.12 *In the situation of Theorem 5.1.6, explain why $[L_1 : F_1] = [L_2 : F_2]$.*

Proof. $\overline{\varphi} : L_1 \to L_2$ is a field isomorphism, whose restriction to F_1 (and co-restriction to F_2) is the field isomorphism $\varphi : F_1 \mapsto F_2$.

$[L_1 : F_1] < \infty$. Let $(f_1, \dots, f_d)$ a basis of L_1 over F_1. We show that $(\overline{\varphi}(f_1), \dots, \overline{\varphi}(f_d))$ is a basis of L_2 over F_2.

• If $\sum_{i=1}^d b_i \overline{\varphi}(f_i) = 0$, where $b_i \in F_2$, then, since $\varphi : F_1 \to F_2$ is surjective, $b_i = \varphi(a_i),\ a_i \in F_1,\ i = 1, \dots d$.

As the restriction of $\overline{\varphi}$ to F_1 is φ, $b_i = \varphi(a_i) = \overline{\varphi}(a_i)$. $\overline{\varphi}$ being a ring homomorphism,

$$0 = \sum_{i=1}^d b_i \overline{\varphi}(f_i) = \sum_{i=1}^d \overline{\varphi}(a_i)\overline{\varphi}(f_i) = \overline{\varphi}\left(\sum_{i=0}^d a_i f_i\right).$$

As the kernel of $\overline{\varphi}$ is 0, $\sum_{i=0}^d a_i f_i = 0$, where the family $(f_i)_{0 \le i \le d}$ is free, thus $a_1 = \cdots = a_d = 0$, and since $b_i = \varphi(a_i)$, $b_1 = \cdots = b_d = 0$. So the family $(\overline{\varphi}(f_i))_{1 \le i \le d}$ is free.

• Let y be any element in L_2. As $\overline{\varphi}$ is surjective, there exists $x \in L_1$ such that $y = \overline{\varphi}(x)$. $(f_1, \cdots, f_d)$ being a basis, there exists $(a_0, \cdots, a_d) \in F_1^d$ such that $x = \sum_{i=0}^d a_i f_i$.

Then

$$y = \overline{\varphi}(x) = \sum_{i=0}^d \overline{\varphi}(a_i)\overline{\varphi}(f_i) = \sum_{i=0}^d \varphi(a_i)\overline{\varphi}(f_i) = \sum_{i=0}^d b_i \overline{\varphi}(f_i),$$

where $b_i = \varphi(a_i) \in F_2$. Consequently $(\overline{\varphi}(f_i))_{1 \le i \le d}$ is a basis of L_2/F_2, and so

$$[L_2 : F_2] = d = [L_1 : F_1].$$

□

Ex. 5.1.13 *Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Use Proposition 5.1.8 to prove that there is an isomorphism $\sigma : L \simeq L$ such that $\sigma(\sqrt{2}) = \sqrt{2}$ and $\sigma(\sqrt{3}) = -\sqrt{3}$.*

Proof. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$f = x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Indeed, $\deg(f) = 2$, and f has no root in $\mathbb{Q}(\sqrt{2})$, otherwise $\sqrt{3} = a + b\sqrt{2},\ a, b \in \mathbb{Q}$. But then $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. If $ab \neq 0$, then $\sqrt{2} = (3 - a^2 - 2b^2)/(2ab) \in \mathbb{Q}$, which is false, thus $ab = 0$. If $b = 0$, then $\sqrt{3} \in \mathbb{Q}$, and if $a = 0$, $\sqrt{3/2} \in \mathbb{Q}$: the two cases are impossible. Consequently $f = x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$.

(This gives an alternative proof of $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.)

As $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $x^2 - 3$ over $\mathbb{Q}(\sqrt{2})$, by Proposition 5.1.8 there exists a field isomorphism $\sigma : L \to L$ which is the identity on $\mathbb{Q}(\sqrt{2})$ and which takes $\sqrt{3}$ to $-\sqrt{3}$. As σ is the identity on $\mathbb{Q}(\sqrt{2})$, we have also $\sigma(\sqrt{2}) = \sqrt{2}$. $\square$

5.2 NORMAL EXTENSIONS

Ex. 5.2.1 *Prove that $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$.*

Proof. This is equivalent to show that $\mathbb{Q}(\sqrt[4]{2})$ is not a normal extension of $\mathbb{Q}$.

$x^4 - 2$ is an irreducible polynomial over $\mathbb{Q}$ by Schönemann-Eisenstein Criterion with $p = 2$.

The roots of the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ are $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$.

As the root $i\sqrt[4]{2}$ is a non real complex, it is not in $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. So $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ is not a normal extension, thus $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$. $\square$

Ex. 5.2.2 *Prove that an algebraic extension $F \subset L$ is normal if and only if for every $\alpha \in L$, the minimal polynomial of α over F splits completely over L.*

Proof. Let $F \subset L$ a normal extension. Let $\alpha \in L$. Its minimal polynomial $f \in F[x]$ is irreducible, thus this polynomial splits completely over F by definition of a normal extension.

Conversely, suppose that every $\alpha \in L$ is such that its minimal polynomial splits completely over F.

Let $g \in F[x]$ any irreducible polynomial, and α a root of g in L. Then g is the minimal polynomial of α over L. So g splits completely over L by hypothesis. Hence every irreducible polynomial g which has a root in L splits completely over L. So the extension $F \subset L$ is normal. $\square$

Ex. 5.2.3 *Determine wether the following extensions are normal. Justify your answers.*

(a) $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$, *where* $\zeta_n = e^{2\pi i/n}$.

(b) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

(c) $F = \mathbb{F}_3(t) \subset F(\alpha)$, *where t is a variable and α is a root of $x^3 - t$ in a splitting field.*

Proof. (a) As $\mathbb{Q}(\zeta_n)$ contient ζ_n^k pour tout $k \in \mathbb{Z}$,

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}).$$

$\mathbb{Q}(1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}) = \mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$.

Conclusion: $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ is a normal extension.

(b) The minimal polynomial of $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = L$ over $\mathbb{Q}$ is $f = x^3 - 2$. The roots of f are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$. But $\omega\sqrt[3]{2} \notin \mathbb{R}$, and $L \subset \mathbb{R}$, thus $\omega\sqrt[3]{2} \notin L$. So $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ is not a normal extension.

(c) By Exercise 4.2.9, the polynomial $f = x^3 - t$ is irreducible over $\mathbb{F}_3(t)$. Let α a root of f in the spitting field L of $x^3 - t$ over F.

As the characteristic of F is 3, $f = x^3 - t = (x - \alpha)^3$, where $\alpha \in L$. The splitting field of f over F is so $F(\alpha)$, thus $F \subset F(\alpha)$ is a normal extension.

□

Ex. 5.2.4 *Give an example of a normal extension of $\mathbb{Q}$ that is not finite.*

Proof. $\overline{\mathbb{Q}}$ is by definition the set of all complex algebraic numbers over $\mathbb{Q}$. Theorem 4.4.10 shows that $\overline{\mathbb{Q}}$ is an algebraically closed field. If $f \in \mathbb{Q}[x]$ is an irreducible polynomial over $\mathbb{Q}$, a fortiori $f \in \overline{\mathbb{Q}}[x]$, and by definition of an algebraically closed field, f splits completely over $\overline{\mathbb{Q}}$. Thus $\mathbb{Q} \subset \overline{\mathbb{Q}}$ is a normal extension. In Exercise 4.4.1, we showed that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. This extension is so an example of a normal extension of $\mathbb{Q}$ that is not finite. □

5.3 SEPARABLE EXTENSION

Ex. 5.3.1 *Prove (5.6) :*

$$\begin{aligned}(ag + bh)' &= ag' + bh'\\ (gh)' &= g'h + gh'\end{aligned}$$

where $f, g \in F[x]$, $a, b \in F$.

Proof. Write

$$g = \sum_{i=0}^{n} a_i x^i, \qquad h = \sum_{j=0}^{m} b_j x^j \in F[x]. \tag{4}$$

(We suppose $a_i = 0$ if $i > m$ or $i < 0$, $b_j = 0$ if $j > m$ or $j < 0$.)

(a) Write $N = \max(n, m)$: then

$$g = \sum_{i=0}^{N} a_i x^i, \qquad h = \sum_{i=0}^{N} b_i x^i.$$

$$g' = \sum_{i=1}^{N} i a_i x^{i-1}, \qquad h' = \sum_{i=1}^{N} i b_i x^{i-1}.$$

If $a, b \in F$, then

$$ag' + bh' = \sum_{i=1}^{N} i(a a_i + b b_i) x^{i-1}.$$

Moreover

$$\begin{aligned} ag + bh &= \sum_{i=0}^{N} (aa_i + bb_i)x^i, \\ (ag + bh)' &= \sum_{i=1}^{N} i(aa_i + bb_i)x^{i-1}, \end{aligned}$$

thus

$$(ag + bh)' = ag' + bh'.$$

(b) By (4), lthe definition of the product of two polynomials gives

$$gh = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k.$$

Thus

$$(gh)' = \sum_{k=1}^{m+n} k \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^{k-1} = \sum_{k=0}^{m+n-1} (k+1) \left(\sum_{i=0}^{k+1} a_i b_{k+1-i} \right) x^k.$$

As

$$\begin{aligned} g' &= \sum_{i=1}^{n} i a_i x^{i-1} = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i, \\ h' &= \sum_{j=1}^{m} j b_j x^{j-1} = \sum_{j=0}^{m-1} (j+1) b_{j+1} x^j, \end{aligned}$$

we obtain

$$\begin{aligned} g'h &= \sum_{k=0}^{m+n-1} \left(\sum_{i=0}^{k} (i+1) a_{i+1} b_{k-i} \right) x^k \\ &= \sum_{k=0}^{m+n-1} \left(\sum_{i=1}^{k+1} i a_i b_{k+1-i} \right) x^k \\ &= \sum_{k=0}^{m+n-1} \left(\sum_{i=0}^{k+1} i a_i b_{k+1-i} \right) x^k, \end{aligned}$$

and also

$$\begin{aligned} gh' &= \sum_{k=0}^{m+n-1} \left(\sum_{i=0}^{k} (k+1-i) a_i b_{k+1-i} \right) x^k \\ &= \sum_{k=0}^{m+n-1} \left(\sum_{i=0}^{k+1} (k+1-i) a_i b_{k+1-i} \right) x^k. \end{aligned}$$

Thus

$$\begin{aligned}
g'h + gh' &= \sum_{k=0}^{m+n-1} \left(\sum_{i=0}^{k+1} i a_i b_{k+1-i} + \sum_{i=0}^{k+1} (k+1-i) a_i b_{k+1-i} \right) x^k \\
&= \sum_{k=0}^{m+n-1} \left(\sum_{i=0}^{k} (i + k + 1 - i) a_i b_{k+1-i} \right) x^k \\
&= \sum_{k=0}^{m+n-1} (k+1) \left(\sum_{i=0}^{k+1} a_i b_{k+1-i} \right) x^k \\
&= (gh)'.
\end{aligned}$$

We have proved the equations 5.6 :

$$\begin{aligned}
(ag + bh)' &= ag' + bh', \\
(gh)' &= g'h + gh'.
\end{aligned}$$

□

Ex. 5.3.2 *Let F have characteristic p, and suppose that $\alpha, \beta \in F$. Lemma 5.3.10 shows that $(\alpha + \beta)^p = \alpha^p + \beta^p$.*

(a) Prove that $(\alpha - \beta)^p = \alpha^p - \beta^p$ if $\alpha, \beta \in F$.

(b) Prove that $(\alpha + \beta)^{p^e} = \alpha^{p^e} + \beta^{p^e}$ for all $e \geq 0$.

Proof. (a) Let F have characteristic p, $p \neq 0$. Then p is prime. Let $\alpha, \beta \in F$.

If p is an odd prime,

$$(\alpha - \beta)^p = \alpha + (-\beta)^p = \alpha^p + (-1)^p \beta^p = \alpha^p - \beta^p.$$

In the remaining case $p = 2$, then $1 = -1$, thus

$$(\alpha - \beta)^p = (\alpha + \beta)^p = \alpha^p + \beta^p = \alpha^p - \beta^p.$$

(b) Let $H : F \to F, x \mapsto x^p$ the Frobenius homomorphism of F. By induction, we show that $H^n(x) = x^{p^n}$ for all $x \in F$:

$H^0(x) = x = x^{p^0}$, et

$H^n(x) = x^{p^n} \Rightarrow H^{n+1}(x) = H(H^n(x)) = (x^{p^n})^p = x^{p \cdot p^n} = x^{p^{n+1}}$.

If $e \in \mathbb{N}$, as H^e, power of a homomorphism, is a homomorphism, so

$$H^e(\alpha + \beta) = H^e(\alpha) + H^e(\beta),$$

namely

$$(\alpha + \beta)^{p^e} = \alpha^{p^e} + \beta^{p^e}.$$

□

Ex. 5.3.3 *Let F be a field of characteristic p. The nth roots of unity are defined to be the roots of $x^n - 1$ in the splitting field $F \subset L$ of $x^n - 1$.*

(a) If $p \nmid n$, show that there are n distinct nth roots of unity in L.

(b) Show that there is only one pth root of unity, namely $1 \in F$.

Proof. (a) Here $n \geq 1$.

As $f = x^n - 1$, then $f' = nx^{n-1}$.

If $p \nmid n$, then $n \neq 0$ in the field F of characteristic p, thus n is a unit in $F[x]$.

$x(nx^{n-1}) - n(x^n - 1) = n = xf' - nf$ is a Bézout's relation between f and f', which proves that $f \wedge f' = 1$. So f is a separable polynomial, and the n roots of f in its splitting field, which are the nth roots of unity, are distinct.

(b) If the characteristic of F is p, by Exercise 2,

$$x^p - 1 = (x - 1)^p.$$

The only pth root of unity is thus 1.

□

Ex. 5.3.4 *Let $f \in \mathbb{Z}[x]$ be monic and nonconstant and have discriminant $\Delta(f)$. Then let $f_p \in \mathbb{F}_p[x]$ be obtained from f by reducing modulo p. Prove that $\Delta(f_p) \in \mathbb{F}_p$ is the congurence class of $\Delta(f)$.*

Proof. Write $\Delta = \Delta(\sigma_1, \cdots, \sigma_n) \in F(\sigma_1, \cdots, \sigma_n) \subset F(x_1, \cdots, x_n)$ the discriminant.

Let $f = x^n + a_1 x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be a monic nonconstant polynomial.

In the section 2.4, $\Delta(f)$ is defined by

$$\Delta(f) = \Delta(-a_1, \cdots, (-1)^i a_i, \cdots, (-1)^n a_n).$$

obtained by applying to $\Delta(\sigma_1, \cdots, \sigma_n)$ the evaluation homomorphism defined by $\sigma_i \mapsto (-1)^i a_i$, which sends $\tilde{f} = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n$ on f, and Δ sur $\Delta(f)$.

Write f_p the reduction of f modulo p :

$f_p = x^n + \overline{a}_1 x^{n-1} + \cdots + \overline{a}_0$, where we write $\overline{k} = [k]_p$ the class of $k \in \mathbb{Z}$ modulo p.

By definition,

$$\Delta(f_p) = \Delta(-\overline{a}_1, \cdots, (-1)^i \overline{a}_i, \cdots, (-1)^n \overline{a}_n).$$

Δ is a polynomial with coefficients in $\mathbb{Z}$ of $\sigma_1, \cdots, \sigma_n$, thus $\Delta(-\overline{a}_1, \cdots, (-1)^i \overline{a}_i, \cdots, (-1)^n \overline{a}_n)$ is the reduction modulo p of $\Delta(-a_1, \cdots, (-1)^i a_i, \cdots, (-1)^n a_n)$, so $\Delta(f_p)$ is the reduction modulo p of $\Delta(f)$:

$$\Delta(f_p) = [\Delta(f)]_p.$$

□

Ex. 5.3.5 *For $f = x^7 + x + 1$, find all primes for which f_p is not separable, and compute $\gcd(f_p, f_p')$ as in (5.14).*

Proof. The following Sage instructions give the wanted factorisation of the discriminant of f:

```
P.<x> = PolynomialRing(QQ)
f = x^7+x+1
g = diff(f(x),x)
d = f.resultant(g);d
```

$$870199$$

```
f.discriminant()
```

$$-870199$$

```
d.factor()
```

$$11 \cdot 239 \cdot 331$$

```
P.<x> = PolynomialRing(GF(11))
f = x^7 + x + 1; df = diff(f(x),x)
gcd(f,df)
```

$$x + 3$$

```
factor(f)
```

$$(x+3)^2 \cdot (x^5 + 5x^4 + 5x^3 + 2x^2 + 9x + 5)$$

```
P.<x> = PolynomialRing(GF(239))
f = x^7 + x + 1; df = diff(f(x),x)
gcd(f,df)
```

$$x + 41$$

```
factor(f)
```

$$(x+41)^2 \cdot (x^5 + 157x^4 + 24x^3 + 122x^2 + 81x + 30)$$

```
P.<x> = PolynomialRing(GF(331))
f = x^7 + x + 1; df = diff(f(x),x)
gcd(f,df)
```

$$x + 277$$

```
factor(f)
```

$$(x+277)^2 \cdot (x^2 + 188x + 203) \cdot (x^3 + 251x^2 + 84x + 80).$$

So

$$\gcd(f_p, f_p') = \begin{cases} x+3, & p = 11, \\ x+41, & p = 239, \\ x+277, & p = 331, \\ 1 & \text{otherwise.} \end{cases}$$

□

Ex. 5.3.6 *Use part (a) of Theorem 5.3.15 to show that the splitting field of a separable polynomial gives a separable extension.*

Proof. Let $F \subset L$ the splitting field of a separable polynomial $f \in F[x] : L = F(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f, and

$$f = c(x - \alpha_1) \cdots (x - \alpha_n).$$

Let f_i be the minimal polynomial of α_i over F. Then f_i divides f, thus $f_i \in F[x]$ is a separable polynomial, since the unicity of the decomposition in irreducible factors in $L[x]$ shows that the only irreducible factors of f_i in $L[x]$ are associate to $x - \alpha_j$. Consequently the α_i are separable for all $i,\ 1 \leq i \leq n$. Part (a) of Theorem 5.3.15 shows then that $F \subset L$ is a separable extension. □

Ex. 5.3.7 *Suppose that F is a field of characteristic p. The goal of this exercise is to prove Proposition 5.3.16. To begin the proof, let $f \in F[x]$ be irreducible.*

- *(a) Assume that f' is not identically zero. Then use the argument of Lemma 5.3.5 to show that f is separable.*
- *(b) Now assume that f' is identically zero. Show that there is a polynomial $g_1 \in F[x]$ such that $f(x) = g_1(x^p)$.*
- *(c) Show that the polynomial of part (b) is irreducible.*
- *(d) Now apply parts (a)-(c) to g_1 repeatedly until you get a separable polynomial g, and conclude that $f(x) = g(x^{p^e})$ where $e \geq 0$ and $g \in F[x]$ is irreducible and separable.*

Proof. Soit F un corps de caractéristique p, et $f \in F[x]$ irréductible sur F, de degré $n \geq 1$.

(a) We suppose first that $f' \neq 0$.

Let $d = f \wedge f'$. Then d divides f (and d is monic), and f is irreducible over F, thus $d = 1$ or $d = \lambda f, \lambda \in F^*$. If $d = \lambda f$, then $f = \lambda^{-1} d$ divides f'. As $f' \neq 0$, $f' = qf$ implies that $\deg(f) = n \leq \deg(f') \leq n - 1$: this is a contradiction.

Thus $d = f \wedge f' = 1$, and then Proposition 5.3.2 shows that f is separable.

(b) Suppose now that $f' = 0$, where $f = \sum\limits_{i=0}^{n} a_i x^i$. Then $0 = f' = \sum\limits_{i=1}^{n} i a_i x^{i-1}$, and consequently $i a_i = 0,\ i = 1, \cdots, n$. If $p \nmid i, a_i = 0$, thus

$$f = \sum_{0 \leq i \leq n,\ p \mid i} a_i x^i = \sum_{k=0}^{\lfloor n/p \rfloor} a_{kp} x^{kp}.$$

If we write $g_1 = \sum\limits_{k=0}^{\lfloor n/p \rfloor} a_{kp} x^k$, then $f = g_1(x^p)$.

(c) If g_1 was reducible,

$$g_1 = uv,\ g_1, g_2 \in F[x], 1 \leq \deg(u), 1 \leq deg(v).$$

But then $f = g_1(x^p) = u(x^p) v(x^p)$, where $\deg(u(x^p)) = p \deg(u) \geq 1, \deg(v(x^p)) \geq 1$, and so f would be reducible, which contradicts the hypothesis on f.

(d) If $g_1' \neq 0$, part (a) shows that g_1 is separable, and then the wanted conclusion is obtained with $e = 1$. Otherwise the arguments of parts (b) and (c) shows that there exits an irreducible polynomial $g_2 \in F[x]$ such that $g_1 = g_2(x^p)$, so $f = g_2(x^{p^2})$, and so on. While $g_i' \neq 0$, we can build a sequence $g_1, \cdots, g_k$ such that $g_i = g_{i+1}(x^p)$, where g_i irreducible over F.

    This sequence is necessarily finite, since $\deg(g_{i+1}) = \deg(g_i)/p < \deg(g_i)$.

    Thus there exists an integer $e \geq 1$ such that $f = g_1(x^p), g_1 = g_2(x^p), \cdots, g_{e-1} = g_e(x^p)$, and $g_e' \neq 0$, and so $g = g_e$ is separable.

    If we take the induction hypothesis $f = g_k(x^{p^k})$, for $k < e$, (verified for $k = 1$) then $f = g_{k+1}((x^{p^k})^p) = g_{k+1}(x^{p \cdot p^k}) = g_{k+1}(x^{p^{k+1}})$.

    Hence $f = g_e(x^{p^e}) = g(x^{p^e})$.

    Conclusion: if F is a field of characteristic p, and if $f \in F[x]$ is irreducible over F, then there exists an integer $e \geq 1$ and an irreducible separable polynomial $g \in k[x]$ such that $f = g(x^{p^e})$.

□

Ex. 5.3.8 *Let $F = k(t, u)$ and $f = (x^2 - t)(x^3 - u)$ be as in Example 5.3.17. Then the splitting field of f contains elements α, β such that $\alpha^2 = t$ and $\beta^3 = u$.*

(a) Prove that $x^2 - t$ is the minimal polynomial of α over F. Also show that $x^2 - t$ is separable.

(b) Similarly, prove that $x^3 - u$ is the minimal polynomial of β over F, and show that $x^3 - u$ is not separable.

Proof. Here k is a field of characteristic 3.

Let $F = k(t, u)$, where t, u are two variables, $f = (x^2 - t)(x^3 - u)$, and α, β in a splitting field L of f such that $\alpha^2 = t, \beta^3 = u$.

(a) The Exercice 4.2.9, applied to the field $k(u)$, shows that $x^2 - t$ has no root in $F = k(t, u) = k(u)(t)$, so it is irreducible over F. So $x^2 - t$ is the minimal polynomial of α over F.

    In L, $x^2 - u = (x - \alpha)(x + \alpha)$, and $\alpha \neq -\alpha$, otherwise $2\alpha = 0$, with $2 = -1 \neq 0$ in k, and $\alpha \neq 0$ since $\alpha^2 = t \neq 0$.

    Thus the minimal polynomial $x^2 - u \in F[x]$ of α over F is separable, so α is separable.

(b) Similarly, $x^3 - u$ has no root in $F = k(t, u) = k(t)(u)$, and its degree is 3, thus it is irreducible over F: $x^3 - u$ is the minimal polynomial of β over F.

    As the characteristic is 3, $x^3 - u = (x - \beta)^3$, so this polynomial is not separable : β is not separable.

So $F \subset L$ is not a separable extension, and is not a purely inseparable extension. □

Ex. 5.3.9 *Let F be a field of characteristic p, and consider $f = x^p - a \in F[x]$. We will assume that f has no roots in F, so that f is irreducible by Proposition 4.2.6. Let α be a root of f in some extension of F.*

(a) Argue as in Example 5.3.11 that $F(\alpha)$ is the splitting field of f and that $[F(\alpha) : F] = p$.

(b) Let $\beta \in F(\alpha) \setminus F$. Use Lemma 5.3.10 to show that $\beta^p \in F$.

(c) Use parts (a) and (b) to show that the minimal polynomial of β over F is $x^p - \beta^p$.

(d) Conclude that $F \subset F(\alpha)$ is purely inseparable.

Proof. (a) As the characteristic is p, $f = x^p - a = (x - \alpha)^p$ has only one root α. The splitting field of f over F is so $F(\alpha)$, and f being the minimal polynomial of α over F, $[F(\alpha) : F] = \deg(f) = p$.

(b) Let $\beta \in F(\alpha) \setminus F$. As α is algebraic over F, $F(\alpha) = F[\alpha]$: there exists so a polynomial $p = \sum_{i=0}^{d} a_i x^i \in F[x]$ such that

$$\beta = p(\alpha) = \sum_{i=0}^{d} a_i \alpha^i.$$

Then (by Lemma 5.3.10),

$$\beta^p = \sum_{i=0}^{d} a_i^p \alpha^{ip} = \sum_{i=0}^{d} a_i^p a^i \in F.$$

(c) Write $b = \beta^p \in F$. Then β is a root of $x^p - b \in F[x]$.

As $x^p - b = (x - \beta)^p$, with $\beta \notin F$, $x^p - b$ has no root in F : by Proposition 4.2.6 $x^p - b$ is irreducible over F. Thus $x^p - b = x^p - \beta^p$ is so the minimal polynomial of β over F.

(d) Every element $\beta \in F(\alpha) \setminus F$ has so a inseparable minimal polynomial, thus every $\beta \in F(\alpha) \setminus F$ is inseparable. By definition, the extension $F \subset F(\alpha)$ is purely inseparable.

□

Ex. 5.3.10 *Suppose that F has characteristic p and $F \subset L$ is a finite extension.*

(a) Use Proposition 5.3.16 to prove that $F \subset L$ is purely inseparable if and only if the minimal polynomial of every $\alpha \in L$ is of the form $x^{p^e} - a$ for some $e \geq 0$ and $a \in F$.

(b) Now suppose that $F \subset L$ is purely inseparable. Prove that $[L : F]$ is a power of p.

Proof. Suppose that F has characteristic p and $F \subset L$ is a finite extension.

(a) • Suppose that the extension $F \subset L$ is purely inseparable. Let α any element in L. α is algebraic over F since $[L : F] < \infty$.

If $\alpha \in F$, the minimal polynomial of α over F is $x - \alpha = x^{p^0} - a$, where $a = \alpha \in F$.

Suppose now that $\alpha \notin F$. By definition of a purely inseparable extension, the minimal polynomial f of α over F is not separable.

By Proposition 5.3.16 (see Ex. 7),

$$f = g(x^{p^e}), \; g \in F[x], e \geq 1,$$

where g is a separable irreducible polynomial.

If $\deg(g) > 1$, then g has the root $\beta = \alpha^{p^e} \in L$, and $\beta \notin F$, otherwise g would be divisible by $x - \beta$ and would so be reducible over F. As g is irreducible, the minimal polynomial of β over F is g, which is separable. Thus β is separable, and $\beta \notin F$, in contradiction with the hypothesis "$F \subset L$ is purely inseparable". Hence $\deg(g) = 1$. As f is monic, g is also monic, thus $g = x - a, a \in F$, and $f = x^{p^e} - a$.

So the minimal polynomial over F of every $\alpha \in L$ is of the form $x^{p^e} - a, \; a \in F, e \geq 0$.

• Conversely, suppose that the minimal polynomial over F of every $\alpha \in L$ is of the form $f = x^{p^e} - a, a \in F, e \geq 0$.

If $\alpha \in L \setminus F$, then $e \geq 1$, otherwise $\alpha = a \in F$.

Consequently, $f' = p^e x^{p^e - 1} = 0$, since $p \mid p^e, e \geq 1$. So $f \wedge f' = f \neq 1$, thus f is not separable. No element of $L \setminus F$ is separable, so the extension $F \subset L$ is purely inseparable.

Conclusion : $F \subset L$ is purely inseparable if and only if the minimal polynomial of every $\alpha \in L$ is of the form $x^{p^e} - a$ for some $e \geq 0$ and $a \in F$.

(b) **Lemma.** *If $F \subset L$ is a finite purely inseparable extension, and if $F \subset K \subset L$, then $K \subset L$ is purely inseparable.*

Proof (of Lemma). Let $\beta \in L \setminus K$, and $f \in F[x]$ the minimal polynomial of β over F, and $f_K \in K[x]$ the minimal polynomial of β over K. As $f \in F[x] \subset K[x]$ and $f(\beta) = 0$, f_K divides f.

By part (a), f is of the form $f = x^{p^e} - a, a \in F, e \geq 1$. As $f = x^{p^e} - a = x^{p^e} - \beta^{p^e} = (x - \beta)^{p^e}$, $x - \beta$ is the only monic irreducible factor of f. Since $f_K \mid f$, $f_K = (x - \beta)^k, \; k \geq 1$. As $\beta \notin K$, $k \geq 2$, thus β is not separable over K, and this is true for every $\beta \in L \setminus K$, so $K \subset L$ is a purely inseparable extension. $\square$.

Suppose now that $F \subset L$ is a purely inseparable extension. As $F \subset L$ is finite, there exists $\alpha_1, \ldots, \alpha_n \in L$ such that $L = F(\alpha_1, \ldots, \alpha_n)$. Let $F_0 = F$ and $F_i = F(\alpha_1, \ldots, \alpha_i), \; 1 \leq i \leq n$

Reasoning by induction, suppose that $[F_i : F]$ is a power of p. This is true for $i = 0$ since $[F_0 : F] = [F : F] = 1 = p^0$.

By the preceding Lemma, L is purely inseparable over F_i. By part (a) applied to F_i, we know that the minimal polynomial f_{i+1} of α_{i+1} over F_i is of the form $f = x^{p^e} - a, a \in F_i, e \geq 0$. Thus $[F_{i+1} : F_i] = [F_i(\alpha_{i+1}) : F_i] = \deg(f_{i+1}) = p^e$. Consequently, $[F_{i+1} : F] = [F_{i+1} : F_i][F_i : F]$ is a power of p, which conclude the induction.

Finally, $[L : F] = [F(\alpha_1, \ldots, \alpha_n) : F]$ is a power of p.

$\square$

Ex. 5.3.11 *Let $f \in F[x]$ be nonconstant. We say that f is* **squarefree** *if f is not divisible by the square of a non constant polynomial in $F[x]$.*

(a) Prove that f is squarefree if and only if f is a product of irreducible polynomials, no two of which are multiples of each other.

(b) Assume that F has characteristic 0. Prove that f is separable if and only if f is squarefree.

Proof. (a) Suppose that f is squarefree.

Let $f = f_1 \cdots f_r$ a decomposition of f in irreducible factors in $k[x]$.

If two irreducible factors $f_i, f_j, i \neq j$ in this decomposition are associate (i.e. $f_i \mid f_j, f_j \mid f_i$), then $f_j = \lambda f_i, \lambda \in F^*$. Then f_i^2 divides $f_i f_j$ which divides f, and f is not squarefree.

Conversely, suppose that f is not squarefree. Then f is divisible by a square factor g^2, where g is a nonconstant polynomial. Let f_1 an irreducible factor of g. The unicity of the decomposition in irreducible factors shows that any decomposition in irreducible factors contains two factors g_1, g_2 associate to f_1, so $g_1 \mid g_2, g_2 \mid g_1$.

Conclusion: f is squarefree if and only if f is product of irreducible factors, no two of which are associate.

(b) Assume that F has characteristic 0.

Proposition 5.3.7(c) shows that f is separable if and only if f is product of irreducible factors, no two of which are associate.

By part (a), this is equivalent to f is squarefree.

Note: this equivalence remains true in a finite field.

Counterexample in $F = \mathbb{F}_3(t)$: the polynomial $f = x^3 - t \in \mathbb{F}_3(t)[x]$ is irreducible over F, so is squarefree, but if α is a root of f in a splitting field L, $x^3 - t = x - \alpha^3 = (x - \alpha)^3$ is not separable. This is due to the fact that "squarefree" is a notion which depends of the field: f is squarefree over F, not over L. ☐

Ex. 5.3.12 *Prove that $f \in F[x]$ is separable if and only if f is nonconstant and f and f' have no common roots in any extension of F.*

Proof. By Proposition 5.3.2(c), $f \in F[x]$ is separable if and only if f is nonconstant and $f \wedge f' = 1$.

If f, f' have a common root α in an extension L of F, then $x - \alpha$ divides f dans $L[x]$, and also f', so divides their gcd in $L[x]$, and so $\gcd(f, f') \neq 1$ (we know that the gcd is the same in $F[x]$ and in $L[x]$).

We have proved that if $f \wedge f' = 1$, then f, f' have no common root in any extension of F.

Conversely, if $f \wedge f' \neq 1$, then f, f' have a common nonconstant factor $g \in F[x]$. Let L an extension of F such that g has a root $\alpha \in F$. Then $\alpha \in L$ is a root of f and f'.

Conclusion: $f \in F[x]$ is separable if and only if f is nonconstant and f and f' have no common roots in any extension of F. ☐

Ex. 5.3.13 *Let F have characteristic p, and let $F \subset L$ be a finite extension with $p \nmid [L:F]$. Prove that $F \subset L$ is separable.*

Proof. Let $\alpha \in L$, and f its minimal polynomial over F. Then $F \subset F(\alpha) \subset L$, thus $[F(\alpha) : F] = \deg(f)$ divides $[L : F]$. Consequently $p \nmid \deg(f)$. By Lemma 5.3.6, this implies that f is separable. Hence every $\alpha \in L$ is separable over F. The extension $F \subset L$ is so separable. $\square$

Ex. 5.3.14 *Let $F \subset K \subset L$ be field extensions, and assume that L is separable over F. Prove that $F \subset K$ and $K \subset L$ are separable extensions.*

Proof. By hypothesis, $F \subset K \subset L$, and L is separable over F.

- Every element of L is separable over F. A fortiori every element of K is separable over F, thus $F \subset K$ is separable.
- Let α any element of L. As α is separable over F, the minimal polynomial $f \in F[x]$ of α over F is separable, thus f has only simple roots in a splitting field R of f over L. The minimal polynomial f_K of α over K divides f (since $f(\alpha) = 0$ and $f \in F[x] \subset K[x]$). As $f_K \mid f$, the order of multiplicity of a root of f_K is at most the order of multiplicity of this root in f, thus all the roots of f_K in the splitting field R are simple, thus α is separable over K. Therefore the extension $K \subset L$ is separable. $\square$

Ex. 5.3.15 *Let f be the polynomial considered in Example 5.3.9. Use Maple or Mathematica to factor f and to verify that the product of the distinct irreducible factors of f is the polynomial given in (5.10).*

Proof. Sage instructions:

```
f = x^11-x^10+2*x^8-4*x^7+3*x^5-3*x^4+x^3+3*x^2-x-1; f
```

$$x^{11} - x^{10} + 2\,x^{8} - 4\,x^{7} + 3\,x^{5} - 3\,x^{4} + x^{3} + 3\,x^{2} - x - 1$$

```
f1 = f.derivative(); f1
```

$$11\,x^{10} - 10\,x^{9} + 16\,x^{7} - 28\,x^{6} + 15\,x^{4} - 12\,x^{3} + 3\,x^{2} + 6\,x - 1$$

```
d = gcd(f,f1); d
```

$$x^{6} - x^{5} + x^{3} - 2\,x^{2} + 1$$

```
p = (f/d).simplify_rational(); p
```

$$x^{5} + x^{2} - x - 1$$

```
v = p.factor(); v
```

$$\left(x^{3} + x + 1\right)(x + 1)(x - 1)$$

```
w = d.factor(); w
```

$$\left(x^{3} + x + 1\right)(x + 1)(x - 1)^{2}$$

```
s = f.factor(); s
```

$$\left(x^{3} + x + 1\right)^{2}(x + 1)^{2}(x - 1)^{3}$$

```
s.expand()
```

$$x^{11} - x^{10} + 2\,x^8 - 4\,x^7 + 3\,x^5 - 3\,x^4 + x^3 + 3\,x^2 - x - 1$$

□

Ex. 5.3.16 *Let F have characteristic p and consider $f = x^p - x + a \in F[x]$.*

(a) Show that f is separable.

(b) Let α be a root of f in some extension of F. Show that $\alpha + 1$ is also a root.

(c) Use part (b) to show that f splits completely over $F(\alpha)$.

(d) Use part (a) of Theorem 5.3.15 to show that $F \subset F(\alpha)$ is separable and normal.

Proof. Let F have characteristic p and consider $f = x^p - x + a \in F[x]$.

(a) $f' = -1$, thus $f \wedge f' = 1$, so f is separable.

(b) Let α be a root of f in some extension L of F. Then $f(\alpha) = \alpha^p - \alpha + a = 0$, thus

$$\begin{aligned} f(\alpha+1) &= (\alpha+1)^p - (\alpha+1) + a \\ &= \alpha^p + 1 - \alpha - 1 + a \\ &= 0, \end{aligned}$$

$\alpha + 1 \in L$ is also a root of f.

(c) So $\alpha, \alpha+1, \ldots, \alpha+p-1$ are roots of f. These roots are distinct since $0, 1, \ldots, p-1$ are the p distinct elements of the prime subfield of F, isomorphic to $\mathbb{F}_p$, and identified with $\mathbb{F}_p$.

Thus f is divisible by $(x-\alpha)\cdots(x-\alpha-p+1)$, of degree $p = \deg(f)$. As both polynomials are monic,

$$f = (x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1). \tag{5}$$

(d) • $F(\alpha)$ contains F and thus contains also $\mathbb{F}_p$. So $F(\alpha)$ contains $\alpha, \alpha+1, \ldots, \alpha+p-1$, thus $F(\alpha) = F(\alpha, \alpha+1, \ldots, \alpha+p-1)$.

$F(\alpha)$ is so the splitting field of f by (5). $F \subset F(\alpha)$ is a normal extension.

• The minimal polynomial g of α over F divides f, which has only simple roots, thus g has only simple roots. So α is separable over F. By Theorem 5.3.15(a), $F \subset F(\alpha)$ is a separable extension.

□

Ex. 5.3.17 *Let β be a root of a polynomial f.*

(a) Assume that $f(x) = (x-\beta)^m h(x)$ for some polynomial $h(x)$, and let $f^{(m)}$ denote the mth derivative of f. Prove that $f^{(m)}(\beta) = m!h(\beta)$.

(b) Assume that we are in characteristic 0. Prove that β has multiplicity m as a root of f if and only if $f(\beta) = f'(\beta) = \cdots = f^{(m-1)}(\beta) = 0$ and $f^{(m)}(\beta) \neq 0$.

(c) *Assume that we are in characteristic p. How big does p need to be relative to m in order for the equivalence of part (b) to be still valid?*

(a)

$$\begin{aligned} f(x) &= (x-\beta)^m h(x) \\ f'(x) &= m(x-\beta)^{m-1}h(x) + (x-\beta)^m H'(x) \\ &= (x-\beta)^{m-1}[mh(x) + (x-\beta)h'(x)] \end{aligned}$$

Thus $f'(x) = (x-\beta)^{m-1}h_1(x)$, where $h_1(x) = mh(x)+(x-\beta)h'(x)$, $h_1(\beta) = mh(\beta)$. By induction, suppose that there exists $h_k \in F[x]$, for $k < m$, such that

$$f^{(k)}(x) = (x-\beta)^{m-k}h_k(x) \text{ and } h_k(\beta) = \frac{m!}{(m-k)!}h(\beta).$$

Then

$$\begin{aligned} f^{(k+1)}(x) &= (m-k)(x-\beta)^{m-k-1}h_k(x) + (x-\beta)^{m-k}h_k'(x) \\ &= (x-\beta)^{m-k-1}[(m-k)h_k(x) + (x-\beta)h_k'(x)] \\ &= (x-\beta)^{m-k-1}h_{k+1}(x) \end{aligned}$$

where $h_{k+1}(x) = (m-k)h_k(x) + (x-\beta)h_k'(x)$, thus

$$h_{k+1}(\beta) = (m-k)h_k(\beta) = (m-k)\frac{m!}{(m-k)!}h(\beta) = \frac{m!}{(m-k-1)!}h(\beta),$$

and the induction is done.The property is so true up to rank $k = m$, so

$$f^{(m)}(x) = h_m(x), \qquad f^{(m)}(\beta) = h_m(\beta) = m!h(\beta).$$

Conclusion : if $f(x) = (x-\beta)^m h(x)$, then $f^{(m)}(\beta) = m!h(\beta)$.

(b) Let $f \in F[x]$, where the characteristic of F is 0. The multiplicity of β in f, written $\mathrm{ord}_f(\beta)$, is defined by

$$\mathrm{ord}_f(\beta) = m \iff (x-\beta)^m \mid f,\ (x-\beta)^{m+1} \nmid f.$$

• Suppose that $\mathrm{ord}_f(\beta) = m$. Then $f(x) = (x-\beta)^m h(x), h \in F[x]$, and $h(\beta) \neq 0$, otherwise $(x-\beta) \mid h$, and so $(x-\beta)^{m+1} \mid f$.

By part (a), for all integer $k, 0 \le k \le m-1$, $f^{(k)}(x) = (x-\beta)^{m-k}h_k(x), h_k \in F[x]$, thus $f(\beta) = f'(\beta) = \cdots = f^{(m-1)}(\beta) = 0$.

Moreover, $f^{(m)}(\beta) = m!h(\beta) \neq 0$, since $h(\beta) \neq 0$, and since the characteristic is 0, so $m! \neq 0$ in F.

We have proved $f(\beta) = f'(\beta) = \cdots = f^{(m-1)}(\beta) = 0, f^{(m)}(\beta) \neq 0$.

• Conversely, suppose that

$$f(\beta) = f'(\beta) = \cdots = f^{(m-1)}(\beta) = 0, f^{(m)}(\beta) \neq 0.$$

As $f(\beta) = 0$, $x - \beta$ divides f. We take as induction hypothesis, for $k < m$, that $(x-\beta)^k \mid f(x)$.

Then $f(x) = (x-\beta)^k h_k(x)$, and part (a) shows that $f^{(k)}(\beta) = k! h_k(\beta) = 0$, since $k < m$. As the characteristic of F is 0, $k! \neq 0$, thus $h_k(\beta) = 0$, therefore $(x-\beta) \mid h_k(x)$, so $(x-\beta)^{k+1} \mid f$.

This induction proves that $(x-\beta)^m \mid f(x)$.

Using again part (a), $f(x) = (x-\beta)^m h(x)$, gives $h(\beta) = \frac{f^{(m)}}{m!} \neq 0$, thus $(x-\beta) \nmid h_k(x)$, so $(x-\beta)^{m+1} \nmid f(x)$. Consequently $\mathrm{ord}_f(\beta) = m$.

Conclusion: if the characteristic of f is 0,

$$\mathrm{ord}_f(\beta) = m \iff f(\beta) = f'(\beta) = \cdots = f^{(m-1)}(\beta) = 0, f^{(m)}(\beta) \neq 0.$$

(c) If the characteristic of F is p, the preceding argumentation remains valid if $m! \neq 0$ in F. In this case, $k! \neq 0$ for all $k = 0, 1, \ldots, m$.

Moreover $m! \neq 0$ is equivalent to $p > m$.

So we can state:

if the characteristic of F is p, and if $m < p$,

$$\mathrm{ord}_f(\beta) = m \iff f(\beta) = f'(\beta) = \cdots = f^{(m-1)}(\beta) = 0, f^{(m)}(\beta) \neq 0.$$

5.4 THEOREM OF THE PRIMITIVE ELEMENT

Ex. 5.4.1 *Use the hints given in the text to prove that (5.18) has coefficients in F.*

Proof. $s(x)$ is defined in (5.18) by

$$s(x) = \prod_{j=1}^{m} f(x - \lambda\gamma_j).$$

Let $g = \prod_{j=1}^{m} f(x - \lambda x_j) \in F[x_1, \ldots, x_m][x]$.

If $u = u(x_1, \ldots, x_m) \in F[x_1, \ldots, x_m]$, and $\sigma \in S_m$, we define $\sigma\cdot u = u(x_{\sigma(1)}, \ldots, x_{\sigma(m)})$. If $v = u(x_1, \ldots, x_m, x) \in F[x_1, \ldots, x_m][x]$, where $v = \sum_{i=0}^{d} p_i x^i, p_i \in F[x_1, \ldots, x_m]$, we write $\sigma \cdot v = \sum (\sigma \cdot p_i) x^i$.

Then $\sigma \cdot (\tau \cdot v) = (\sigma\tau) \cdot v$, and $\sigma \cdot (vw) = (\sigma \cdot v)(\sigma \cdot w)$, for all $\sigma, \tau \in S_n, v, w \in F[x_1, \ldots, x_m][x]$.

For every permutation $\sigma \in S_n$,

$$\begin{aligned}
\sigma \cdot g &= \sigma \cdot \prod_{j=1}^{m} f(x - \lambda x_j) \\
&= \prod_{j=1}^{m} \sigma \cdot f(x - \lambda x_j) \\
&= \prod_{j=1}^{m} f(x - \lambda x_{\sigma(j)}) \\
&= \prod_{j=1}^{m} f(x - \lambda x_j) \\
&= g.
\end{aligned}$$

As $g = \sum_{i=0}^{d} p_i(x_1, \ldots, x_m)x^i$ $(d = lm)$, and $g = \sigma \cdot g = \sum_{i=0}^{d} \sigma \cdot p_i(x_1, \cdots, x_m)x^i$, every coefficient $p_i(x_1, \ldots, x_m) \in F[x_1, \ldots, x_m]$ is a symmetric polynomial.

The evaluation homomorphism φ defined by $x_1 \mapsto \gamma_1, \ldots, x_m \mapsto \gamma_m$, where $\gamma_1, \ldots, \gamma_m$ are the roots of $g \in F[x]$ sends the coefficients of g on the coefficients of s. Corollary 2.2.5 show that $p_i(\gamma_1, \ldots, \gamma_m) \in F$, $i = 0, \ldots d$, thus

$$s(x) = \sum_{i=0}^{d} p_i(\gamma_1, \ldots, \gamma_m)x^i \in F[x].$$

□

Ex. 5.4.2 *Let F be a finite field, and let $F \subset L$ be a finite extension. We claim that there is $\alpha \in L$ such that $L = F(\alpha)$ and α is separable over F.*

(a) Show that L is a finite field.

(b) The set $L^* = L \setminus \{0\}$ is a finite group under multiplication and hence is cyclic by Proposition A.5.3. Let $\alpha \in L^*$ be a generator. Prove that $L = F(\alpha)$.

(c) Let $m = |L| - 1$. Show that α^i is a root of $x^m - 1$ for all $0 \le i \le m-1$, and conclude that

$$x^m - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{m-1}).$$

(d) Use part (c) to show that α is separable over F.

Proof. Let F a finite field, and $F \subset L$ a finite extension.

(a) As $n = [L : F] < \infty$, there exists a basis $(l_1, \cdots, l_n)$ of L over F, thus every element $\alpha \in L$ is of the form $\alpha = \gamma_1 l_1 + \cdots + \gamma_n l_n$, with a unique $(\gamma_1, \ldots, \gamma_n) \in F^n$. Therefore L is isomorphic to F^n as vector space, thus $|L| = |F|^n < \infty$. L is so a finite field.

(b) L^* being the finite multiplicative group of a field is cyclic (Proposition A.5.3), with a generator $\alpha \in L$:

$$L^* = \{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}.$$

Every γ in L^* is so of the form $\gamma = \alpha^k, k \in \mathbb{N}$, thus $L^* \subset F(\alpha)$, and $0 \in F[\alpha]$, so $L \subset F(\alpha)$. Moreover $F \subset L$, and $\alpha \in L$, thus $F(\alpha) \subset L$.

$$L = F(\alpha).$$

(c) As $(L^*, \times)$ is a group of cardinality $m = |L| - 1$, Lagrange's Theorem shows that every $\gamma \in L^* = \{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ satisfies $\gamma^m = 1$, and so is a root of $x^m - 1$.

Since the order of α is m, $\alpha^i \ne \alpha^j$ if $0 \le i < j \le m-1$, thus the polynomial $p = (x-1)(x-\alpha)\cdots(x-\alpha^{m-1})$ divides $x^m - 1$. The degree of the quotient is 0, so this quotient is a constant $c \in F^*$. Since p and $x^m - 1$ are monic, $c = 1$.

$$x^m - 1 = (x-1)(x-\alpha)\cdots(x-\alpha^{m-1}).$$

(d) The minimal polynomial f of α over F divides $x^m - 1$, which is separable by part (c). Thus f is also separable. Therefore α is separable, and $L = F(\alpha)$: the Theorem of the Primitive Element is proved in the case of a finite extension of a finite field.

□

Ex. 5.4.3 *In the equation $\alpha = t_1\alpha_1 + \cdots + t_n\alpha_n$ in part (b) of Corollary 5.4.2, show that we can assume that $t_1, \cdots, t_n \in \mathbb{Z}$.*

Proof. Here we suppose that F has characteristic 0. So F has $\mathbb{Q}$ as subfield, and $\mathbb{Z}$ as subring.

As $\mathbb{Z}$ is infinite, we can find in $\mathbb{Z}$ an integer λ which satisfies (5.16):

$$\beta_r + \lambda\gamma_s \neq \beta_i + \lambda\gamma_j \text{ pour } (r,s) \neq (i,j).$$

The remainder of of the proof is unchanged, and at each step of the induction, we choose such a $\lambda \in \mathbb{Z}$, so the primitive element $\alpha = t_1\alpha_1 + \cdots + t_n\alpha_n$ satisfies $t_i \in \mathbb{Z}$. $\square$

Ex. 5.4.4 *In the extension $F \subset L$ of example 5.4.4, we have $F = k(t,u)$, where k has characteristic p and L is the splitting field of $(x^p - t)(x^p - u) \in F[x]$. We also have $\alpha, \beta \in L$ satisfying $\alpha^p = y, \beta^p = u$. Prove the following properties of $F \subset L$:*

(a) $L = F(\alpha, \beta)$ and $[L : F] = p^2$.

(b) $[F(\gamma) : F] = p$ for all $\gamma \in L \setminus F$.

(c) $F \subset L$ is purely inseparable.

Proof. (a) As $\alpha, \beta \in L$, and as $F \subset L$, $F(\alpha, \beta) \subset L$.

Since F has characteristic p, $f = (x^p - t)(x^p - u) = (x - \alpha)^p(x - \beta)^p$ has only the roots α, β. The splitting field of f over F is so $F(\alpha, \beta)$.

$$L = F(\alpha, \beta).$$

The polynomial $x^p - u$ has no root in $k(t, u, \alpha) = F(\alpha)$ by Exercise 4.2.9. applied to the field $k(t, \alpha)$. Moreover, p is prime, so Proposition 4.2.6 shows that $h = x^p - u$ is irreducible over $F(\alpha)$. Therefore h is the minimal polynomial of β sur $F(\alpha)$. Consequently,

$$[L : F(\alpha)] = [F(\alpha, \beta) : F(\alpha)] = \deg(x^p - u) = p.$$

With the same argument, $x^p - t$ has no root in $F(t)$ and is irreducible. $x^p - t$ is the minimal polynomial of α over F, thus $[F(\alpha) : F] = p$.

Finally

$$[L : F] = [L : F(\alpha)]\,[F(\alpha) : F] = p^2.$$

(b) Let $\gamma \in L \setminus F$.

We have proved in Example 5.3.4 that the extension $F \subset L$ has no primitive element, thus $F(\gamma) \neq L$:

$$F \subsetneq F(\gamma) \subsetneq L.$$

So $d = [F(\gamma) : F]$ divides $p^2 = [L : F]$. Moreover $d \neq 1$, otherwise $F(\gamma) = F, \gamma \in F$, and $d \neq p^2$, otherwise $F(\gamma) = L$, thus

$$[F(\gamma) : F] = p$$

.

(c) By part (b), the minimal polynomial g of γ over F has degree p. Moreover $b = \gamma^p \in F$ by Example 5.4.4, so γ is a root of $x^p - b \in F[x]$. Thus $g \mid x^p - b$. As $\deg(g) = \deg(x^p - b)$, and as g and $x^p - b$ are monic, $x^p - b = g$ is the minimal polynomial of γ over F. Since $g = (x - \gamma)^p$, this polynomial is not separable. Consequently every $\gamma \in L \setminus F$ is inseparable, so the extension $F \subset L$ is purely inseparable.

$\square$

Ex. 5.4.5 *Let $F \subset L = F(\alpha, \beta)$ be as in Exercise 4, and consider the intermediate fields $F \subset F(\alpha + \lambda\beta) \subset L$ as λ varies over all elements of F. Suppose that $\lambda \neq \mu$ are two elements of F such that $F(\alpha + \lambda\beta) = F(\alpha + \mu\beta)$.*

(a) Show that $\alpha, \beta \in F(\alpha + \lambda\beta)$.

(b) Conclude that $F(\alpha + \lambda\beta) = F(\alpha, \beta)$, and explain why this contradicts Example 5.4.4.

It follow that the fields $F(\alpha + \lambda\beta)$, $\lambda \in F$, are all distinct. Since F is infinite, we see that there are infinitely many fields between F and L.

Proof. As in Exercise 4, $F \subset L = F(\alpha, \beta)$.

Suppose that $F(\alpha + \lambda\beta) = F(\alpha + \mu\beta)$, $\lambda \neq \mu$.

(a) Then

$$\alpha + \mu\beta \in F(\alpha + \lambda\beta),$$
$$\alpha + \lambda\beta \in F(\alpha + \lambda\beta).$$

Consequently their difference is also in the subfield $F(\alpha + \lambda\beta)$:

$$(\mu - \lambda)\beta \in F(\alpha + \lambda\beta).$$

As $\mu - \lambda \in F, \mu - \lambda \neq 0$,

$$\beta \in F(\alpha + \lambda\beta).$$

Since $\alpha = (\alpha + \lambda\beta) - \lambda\beta$, with $\alpha + \lambda\beta, \beta \in F(\alpha + \lambda\beta)$, and $\lambda \in F$, then

$$\alpha \in F(\alpha + \lambda\beta).$$

(b) $\alpha + \lambda\beta \in F(\alpha, \beta)$, thus $F(\alpha + \lambda\beta) \subset F(\alpha, \beta)$. Moreover, by part (a), $\alpha, \beta \in F(\alpha + \lambda\beta)$, thus $F(\alpha, \beta) \subset F(\alpha + \lambda\beta)$.

$$F(\alpha, \beta) = F(\alpha + \lambda\beta).$$

But Example 5.4.4 shows that $F(\alpha, \beta)$ has no primitive element : this is a contradiction.

This reductio ad absurdum shows that all the fields $F(\alpha + \lambda\beta)$, where λ varies over all elements of F, are distinct. F being infinite, there exists infinitely many intermediate fields between F and L.

$\square$

Ex. 5.4.6 *Explain why the proof of Theorem 5.4.1 implies that $F(\beta+\lambda\gamma) = F(\beta,\gamma)$ when γ is separable over F, β is algebraic over F, and λ satisfies (5.17).*

Proof. The proof of $F(\alpha,\beta) = F(\alpha+\lambda\beta)$ uses only 5.17 (5.16 is used only to prove the separability of $\alpha+\lambda\beta$). The separability of γ (thus of g) is used only to prove that another root of h, which is also a root of g, is one of the $\gamma_j, j \geq 2$. The separability of β is not used, only the algebraic nature of β,γ, to define their minimal polynomials. $\square$

Ex. 5.4.7 *Let $F \subset L = F(\alpha_1,\ldots,\alpha_n)$ be a finite extension, and suppose that $\alpha_1,\ldots,\alpha_{n-1}$ are separable over F. Prove that $F \subset L$ has a primitive element.*

Proof. Let a finite extension $F \subset L = F(\alpha_1,\cdots,\alpha_n)$, where $\alpha_1,\cdots,\alpha_{n-1}$ are separable over F (but not α_n). The Primitive Element Theorem (5.4.1) shows that $F(\alpha_1,\cdots,\alpha_{n-1})$ has a primitive element β separable over F.

The extension $F \subset L = F(\beta,\alpha_n)$ is such that β is algebraic separable over F, and α_n algebraic over F.

If F is infinite, by Exercise 6 this is sufficient to prove the existence of a primitive element of $F \subset L$ (but perhaps not separable).

If F is a finite field, then L also, and it has a primitive element by Exercise 2(b). $\square$

Ex. 5.4.8 *Use Exercise 7 to find an explicit primitive element for $F = k(t,u) \subset L$, where k has characteristic 3 and L is the splitting field of $(x^2-t)(x^3-u)$. Note that this extension is not separable, by Exercise 8 of Section 5.3.*

Proof. Here $F = k(t,u) \subset L$, where the characteristic of k is 3, L is the splitting field of $(x^2-t)(x^3-u)$, and $\alpha,\beta \in L$ are such that $\alpha^2 = t, \beta^3 = u$.

α is separable, but not β (cf Exercise 5.3.8).

We know (by Exercice 5.3.8) that

$$f(x) = x^3 - u,$$
$$g(x) = x^2 - t,$$

are the respective minimal polynomials of β and α over F.

The two polynomials

$$g(x) = x^2 - t \in F[x] \subset F(\alpha+\beta)[x]$$
$$f(\alpha+\beta-x) = -x^3 + (\alpha+\beta)^3 - u \in F(\alpha+\beta)[x]$$

vanish at α, since $g(\alpha) = 0, f(\beta) = 0$, and they are both in $F(\alpha+\beta)[x]$.

Thus $x - \alpha \mid h(x) = \gcd(g(x), f(\alpha+\beta-x))$.

$1 \leq \deg(h) \leq 2$. If $\deg(h) = 2$, as $h \mid g$, we would have $h = g = (x-\alpha)(x+\alpha)$, and then $x + \alpha \mid h \mid f(\alpha+\beta-x)$.

As $f(x) = (x-\beta)^3$, then $f(\alpha+\beta-x) = -(x-\alpha)^3$, which is not divisible by $x+\alpha$, since $-\alpha \neq \alpha$.

Therefore $\deg(h) = 1$, and $h(x) = \mathrm{pgcd}(g(x), f(\alpha+\beta-x)) = x - \alpha$.

Thus there exists a Bézout's relation

$$A(x)g(x) + B(x)f(\alpha+\beta-x) = x - \alpha,\ A,B \in F(\alpha+\beta)[x].$$

This proves that $\alpha \in F(\alpha+\beta)$, thus also $\beta = (\alpha+\beta) - \alpha \in F(\alpha+\beta)$, which implies that $L = F(\alpha,\beta) = F(\alpha+\beta) : \alpha+\beta$ is a primitive element of L/F.

We compute explicitly the gcd of the polynomials $f(\alpha+\beta-x), g(x)$:
The first Euclidean division of $f(\alpha+\beta-x)$ by $g(x)$ gives

$$
\begin{aligned}
-x^3+(\alpha+\beta)^3-u+x(x^2-t) &= -tx+(\alpha+\beta)^3-u \\
&= -t\left(x-\frac{(\alpha+\beta)^3-u}{t}\right).
\end{aligned}
$$

We must then have

$$\alpha=\frac{(\alpha+\beta)^3-u}{t}\in F(\alpha+\beta).$$

We compute a direct proof of this equality :

$$\frac{(\alpha+\beta)^3-u}{t}=\frac{\alpha^3+\beta^3-u}{t}=\frac{\alpha^3}{t}=\frac{\alpha^3}{\alpha^2}=\alpha.$$

This equality proves also that $\alpha+\beta$ is a primitive element of $F\subset L$ $\square$