Solutions to David A.Cox "Galois Theory"

Richard Ganaye

January 31, 2020

4 Chapter 4

4.1 FIELDS

Ex. 4.1.1 *Let $\alpha \in L \setminus \{0\}$ be algebraic over a subfield F. Prove that $1/\alpha$ is also algebraic over F.*

Proof. Suppose that $\alpha \in L \setminus \{0\}$ be algebraic over a subfield F of L. Then there exists a polynomial $p = \sum_{k=0}^{d} a_k x^k \in F[x]$, with $a_d \neq 0$, whose α is a root :

$$\sum_{k=0}^{d} a_k \alpha^k = 0.$$

Dividing by α^d, we obtain $\sum_{k=0}^{d} a_k \left(\frac{1}{\alpha}\right)^{d-k} = 0$, which we can write $\sum_{i=0}^{d} a_{d-i} \left(\frac{1}{\alpha}\right)^{i} = 0$.

So $1/\alpha$ is a root of the polynomial $q = \sum_{i=0}^{d} a_{d-i} x^i \in F[x]$ has $1/\alpha$, and $q \neq 0$ since $a_d \neq 0$, thus $1/\alpha$ is algebraic over F. □

Ex. 4.1.2 *Complete the proof of Lemma 4.1.3 by showing that if f and g are monic polynomials in $F[x]$ each of which divides the other, then $f = g$.*

Proof. Suppose that $f, g \in F[x]$ are monic, and $f \mid g, g \mid f$.

$f = gh, h \in F[x]$ and $g = fl, l \in F[x]$, so $f = fhl$, where $f \neq 0$ since f is monic, thus $hl = 1$, and so $\deg(h) + \deg(l) = 0$, $\deg(h) = \deg(l) = 0$.

Therefore $h = \lambda \in F^*$, $f = \lambda g$. In particular, f, g have the same degree d.

Write $f = \sum_{k=0}^{d} a_k x^k, g = \sum_{k=0}^{d} b_k x^k$.

As f, g are monic, $a_d = b_d = 1$, and $a_d = \lambda b_d$, so $\lambda = 1$, and $f = g$.

Conclusion : if f and g are monic polynomials in $F[x]$ each of which divides the other, then $f = g$ □

Ex. 4.1.3 *Suppose that $F \subset L$ is a field extension and that $\alpha_1, \ldots, \alpha_n \in L$. Show that $F[\alpha_1, \ldots, \alpha_n]$ is a subring of L and that $F(\alpha_1, \ldots, \alpha_n)$ is a subfield of L.*

Proof. • By hypothesis, $F \subset L$ and $\alpha_1, \ldots, \alpha_n \in L$.

$1 \in F[\alpha_1, \ldots, \alpha_n]$, so $F[\alpha_1, \ldots, \alpha_n] \neq \emptyset$.

Let $x, y \in F[\alpha_1, \ldots, \alpha_n]$. By definition, there exist polynomials $p, q \in F[x_1, \ldots, x_n]$ such that

$$x = p(\alpha_1, \ldots, \alpha_n), \quad y = q(\alpha_1, \ldots, \alpha_n).$$

As $p - q, pq \in F[x_1, \ldots, x_n]$, and as $x - y = (p - q)(\alpha_1, \ldots, \alpha_n), xy = pq(\alpha_1, \ldots, \alpha_n)$, so $x - y \in F[\alpha_1, \ldots, \alpha_n], xy \in F[\alpha_1, \ldots, \alpha_n]$.

Conclusion : $F[\alpha_1, \ldots, \alpha_n]$ is a subring of L.

• The same argument, where we take rational fractions p, q in place of polynomials show that $p, q \in F(x_1, \ldots, x_n) \Rightarrow p - q, pq \in F(x_1, \ldots, x_n)$, so $x - y = (p - q)(\alpha_1, \ldots, \alpha_n), xy = pq(\alpha_1, \ldots, \alpha_n) \in F(\alpha_1, \ldots, \alpha_n)$. Thus $F(\alpha_1, \ldots, \alpha_n)$ is a subring of L.

Moreover, if $x \in F(\alpha_1, \ldots, \alpha_n), x \neq 0$, then $x = \frac{p(\alpha_1, \ldots, \alpha_n)}{q(\alpha_1, \ldots, \alpha_n)}$, where $p, q \in F[x_1, \ldots, x_n]$, and $q(\alpha_1, \ldots, \alpha_n) \neq 0$. Since $x \neq 0$, we have also $p(\alpha_1, \ldots, \alpha_n) \neq 0$.

Hence $\frac{1}{x} = \frac{q(\alpha_1, \ldots, \alpha_n)}{p(\alpha_1, \ldots, \alpha_n)} \in F(\alpha_1, \ldots, \alpha_n)$.

Conclusion : $F(\alpha_1, \ldots, \alpha_n)$ is a subfield of L. □

Ex. 4.1.4 *Complete the proof of Corollary 4.1.11 by showing that*

$$F(\alpha_1, \ldots, \alpha_r)(\alpha_{r+1}, \ldots, \alpha_n) \subset F(\alpha_1, \ldots, \alpha_n).$$

Proof. $F(\alpha_1, \ldots, \alpha_r) \subset F(\alpha_1, \ldots, \alpha_n)$, $1 \leq r \leq n$, since $F(\alpha_1, \ldots, \alpha_n)$ contains F and $\alpha_1, \ldots, \alpha_r$, and since $F(\alpha_1, \ldots, \alpha_r)$ is the smallest subfield of L containing F and $\alpha_1, \ldots, \alpha_r$.

Moreover $F(\alpha_1, \ldots, \alpha_n)$ contains $\alpha_{r+1}, \ldots, \alpha_n$.

By Lemma 4.1.9, $F(\alpha_1, \ldots, \alpha_r)(\alpha_{r+1}, \ldots, \alpha_n)$ is the smallest subfield of L containing $F(\alpha_1, \ldots, \alpha_r)$ and $\alpha_{r+1}, \ldots, \alpha_n$, thus

$$F(\alpha_1, \ldots, \alpha_r)(\alpha_{r+1}, \ldots, \alpha_n) \subset F(\alpha_1, \ldots, \alpha_n).$$

We the reciprocal inclusion proved in section 4.1, we conclude that

$$F(\alpha_1, \ldots, \alpha_r)(\alpha_{r+1}, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n).$$

□

Ex. 4.1.5 *Prove carefully that* $F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] = F[\alpha_1, \ldots, \alpha_n]$.

Proof. • Let $\gamma \in F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n]$. Write $R = F[\alpha_1, \ldots, \alpha_{n-1}]$. By definition, there exists a polynomial $p = \sum_{k=0}^{d} a_k x_n^k \in R[x_n]$ such that $\gamma = p(\alpha_n)$, and for every $a_k \in K, 0 \leq k \leq d$, there exists $f_k \in F[x_1, \ldots, x_{n-1}]$ such that $a_k = f_k(\alpha_1, \ldots, \alpha_{n-1})$.

Thus

$$\gamma = \sum_{k=0}^{d} f_k(\alpha_1, \ldots, \alpha_{n-1}) \alpha_n^k.$$

Let $f = \sum\limits_{k=0}^{d} f_k(x_1, \ldots, x_{n-1}) x_n^k$. Then $f \in F[x_1, \ldots, x_n]$, and $\gamma = f(\alpha_1, \ldots, \alpha_n)$, so $\gamma \in F[\alpha_1, \ldots, \alpha_n]$. We have proved

$$F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] \subset F[\alpha_1, \ldots, \alpha_n].$$

• Reciprocally, let $\gamma \in F[\alpha_1, \dots, \alpha_n]$.

There exists $f \in F[x_1, \dots, x_n]$ such that $x = f(\alpha_1, \dots, \alpha_n)$.

As $F[x_1, \dots, x_n] = F[x_1, \dots, x_{n-1}][x_n]$, $f = \sum\limits_{k=0}^{d} f_k(x_1, \dots, x_{n-1})x_n^k$, where $f_k \in F[x_1, \dots, x_{n-1}]$.

So $\gamma = \sum\limits_{k=0}^{d} f_k(\alpha_1, \dots, \alpha_{n-1})\alpha_n^k = \sum\limits_{k=0}^{d} a_k x_n^k$, with $a_k = f_k(\alpha_1, \dots, \alpha_{n-1}) \in F[\alpha_1, \dots, \alpha_n] = R$.

Let $p = \sum_{k=0}^{d} a_k x_n^k$. Alors $p \in R[x_n]$ and $x = p(\alpha_n)$, thus $x \in R[\alpha_n] = F[\alpha_1, \dots, \alpha_{n-1}][\alpha_n]$.

The reciprocal inclusion

$$F[\alpha_1, \dots, \alpha_n] \subset F[\alpha_1, \dots, \alpha_{n-1}][\alpha_n]$$

is proven, and so

$$F[\alpha_1, \dots, \alpha_n] = F[\alpha_1, \dots, \alpha_{n-1}][\alpha_n].$$

Note : in an alternative way, we could write a lemma analogous to Lemma 4.1.9 and show that $F[\alpha_1, \dots, \alpha_n]$ is the smallest subring of L containing $\alpha_1, \dots, \alpha_n$ (where L is a ring containing F and $\alpha_1, \dots, \alpha_n$), and prove as in Exercise 4 that :

$$F[\alpha_1, \dots, \alpha_r][\alpha_{r+1}, \dots, \alpha_n] = F[\alpha_1, \dots, \alpha_n].$$

□

Ex. 4.1.6 *Suppose that $F \subset L$ and that $\alpha_1, \dots, \alpha_n \in L$ are algebraically independent over F (as defined in the Mathematical Notes to section 2.2). Prove that there is an isomorphism of fields*

$$F(\alpha_1, \dots, \alpha_n) \simeq F(x_1, \dots, x_n),$$

where $F(x_1, \dots, x_n)$ is the field of rational functions in variables $x_1, \dots, x_n$.

Proof. Let $f \in F(x_1, \dots, x_n)$, $f = p/q$, $p, q \in F[x_1, \dots, x_n], q \neq 0$. Since $\alpha_1, \dots, \alpha_n$ are algebraically independent over F, $q(\alpha_1, \dots, \alpha_n) \neq 0$. We can so define

$$\begin{aligned} \varphi : F(x_1, \dots, x_n) &\to F(\alpha_1, \dots, \alpha_n) \\ f = p/q &\mapsto f(\alpha_1, \dots, \alpha_n) = p(\alpha_1, \dots, \alpha_n)/q(\alpha_1, \dots, \alpha_n). \end{aligned}$$

(this quotient doesn't depend on the choice of the representent p/q of f).

φ is a ring homomorphism.

By definition of $F(\alpha_1, \dots, \alpha_n)$, φ is surjective.

Let $f = p/q \in F(x_1, \dots, x_n)$, with $p, q \in F[x_1, \dots, x_n], q \neq 0$. If $f \in \ker(\varphi)$, then $p(\alpha_1, \dots, \alpha_n)/q(\alpha_1, \dots, \alpha_n) = 0$, thus $p(\alpha_1, \dots, \alpha_n) = 0$. Since $\alpha_1, \dots, \alpha_n$ are algebraically independent, $p = 0$. Consequently $\ker(\varphi) = \{0\}$, and so φ is a ring isomorphism between two fields : it is a field isomorphism.

Conclusion : if $\alpha_1, \dots, \alpha_n \in L$ are algebraically independent over F,then

$$F(\alpha_1, \dots, \alpha_n) \simeq F(x_1, \dots, x_n).$$

□

Ex. 4.1.7 *In the proof of Proposition 4.1.14, we used the quotient ring $F[x]/\langle p\rangle$ to show that $F[\alpha]$ is a field when α is algebraic over F with minimal polynomial $p \in F[x]$.Here, you will prove that $F[\alpha]$ is a field without using quotient rings. Since we know that $F[\alpha]$ is a ring, it suffices to show that every nonzero element $\beta \in F[\alpha]$ has a multiplicative inverse in $F[\alpha]$. So pick $\beta \neq 0$ in $F[\alpha]$ Then $\beta = g(\alpha)$ for some $g \in F[x]$.*

(a) Show that g and p are relatively prime in $F[x]$.

(b) By part (a) and the Euclidean algorithm, we have $Ap + Bg = 1$ for some $A, B \in F[x]$. Prove that $B(\alpha) \in F[\alpha]$ is the multiplicative inverse of $g(\alpha)$.

Do you see how this exercice relates to Exercise 5 of section 3.1?

Proof. As in Proposition 4.1.14, we assume that $F \subset L$ is a field extension, and that $\alpha \in L$. Suppose that $\alpha \in L$ is algebraic over F, where $p \in F[x]$ is the minimal polynomial of α over F, and $\beta \in F[\alpha], \beta \neq 0$.

There exists $g \in F[x]$ such that $\beta = g(\alpha)$.

(a) The minimal polynomial p of α is irreducible over F (Prop. 4.1.5).

Let $u \in F[x]$ such that $u \mid p, u \mid g$. Then $p = uq,\ q \in F[x]$, and since p is irreducible over F, u or q is a constant of F^*.

If $q = \lambda \in F^*$, then $p = \lambda^{-1}u$ divides u, which divides g, thus p divides g. In this case, since $p(\alpha) = 0$, $\beta = g(\alpha) = 0$, in contradiction with the hypothesis $\beta \neq 0$.

So $u = \mu \in F^*$, $u \mid 1$. Consequently, for all $u \in F[x]$, $(u \mid p, u \mid g) \Rightarrow u \mid 1 : p, g$ are relatively prime.

(b) Then there exist a Bézout's relation between these two polynomials :

$$Ap + Bg = 1,\ A, B \in F[x].$$

The evaluation of these polynomials in α, since $p(\alpha) = 0$, gives

$$B(\alpha)g(\alpha) = 1, B(\alpha) \in F[\alpha]$$

So $B(\alpha)$ is the multiplicative inverse of $\beta = g(\alpha) \neq 0$ in $F[\alpha] : F[\alpha]$ is a field.

Note : we have proved in Exercice 3.5.1 that $F[x]/\langle f\rangle$, where f is irreducible over F, is a field with the same argumentation. Here $f = p$ is the minimal polynomial of α over F, so it is irreducible over f.

□

Ex. 4.1.8 *If a polynomial is irreducible over a field F, it may or may not remain irreducible over a large field. Here are examples of both types of behavior.*

(a) Prove that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$.

(b) In Example 4.1.7, we showed that $x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$ (it is the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$). Show that $x^4 - 10x^2 + 1$ is not irreducible over $\mathbb{Q}(\sqrt{3})$.

Proof. (a) x^2-3 is irreducible over $\mathbb{Q}$. We show that it remains irreducible over $\mathbb{Q}[\sqrt{2}]$. With a reductio ad absurdum, we suppose that f is reducible over F : $f = x^2 - 3 = uv,\ uv \in \mathbb{Q}[\sqrt{2}][x]$, where u, v are nonconstant polynomials. Then $\deg(u) \geq 1, \deg(v) \geq 1$, and as $\deg(u) + \deg(v) = \deg(f) = 2$, $\deg(u) = \deg(v) = 1$:

$$u = ax + b, a, b \in \mathbb{Q}[\sqrt{2}], a \neq 0.$$

Then $\alpha = -b/a \in \mathbb{Q}[\sqrt{2}]$ is a root of u, thus is a root of $f = x^2-3$. Since $\sqrt{2}^{2n} = 2^n$ et $\sqrt{2}^{2n+1} = 2^n\sqrt{2}$, every element of $\mathbb{Q}[\sqrt{2}]$ is of the form $c + d\sqrt{2},\ c, d \in \mathbb{Q}$.

We should have $\alpha = c + d\sqrt{2} = \pm\sqrt{3}$. Alors

$$\alpha^2 = c^2 + 2d^2 + 2cd\sqrt{2} = 3.$$

If $cd \neq 0$, $\sqrt{2} = (c^2 + 2d^2 - 3)/(2cd) \in \mathbb{Q}$, in contradiction with the irrationality of $\sqrt{2}$. Thus $c = 0$ ou $d = 0$.

$d = 0$ gives $\sqrt{3} = \pm c \in \mathbb{Q}$: this is in contradiction with the irrationality of $\sqrt{3}$.

$c = 0$ implies $\sqrt{\frac{3}{2}} = \pm d \in \mathbb{Q}$. But then $\sqrt{\frac{3}{2}} = \frac{p}{q}, (p, q) \in \mathbb{Z} \times \mathbb{N}^*, p \wedge q = 1$.

$3q^2 = 2p^2,\ q^2 \mid 2p^2$ and $q^2 \wedge p^2 = 1$. By Gauss Lemma, $q^2 \mid 2, q \in \mathbb{N}^*$, donc $q = 1, 3 = 2p^2$, thus 3 is even : this is absurd.

Conclusion : $x^2 - 3$ is irreducible $\mathbb{Q}[\sqrt{2}]$.

(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 equality $f = x^4 - 10x^2 + 1 = (x^2 - 2\sqrt{3}x + 1)(x^2 - 2\sqrt{3}x + 1)$ show that f is not irreducible over $\mathbb{Q}[\sqrt{3}]$.

Factorisation with Sage :

```
K = NumberField(x^2-3, 'a');L.<X> = PolynomialRing(K)
p = X^4-10*X^2+1
factor(p)
```

$$(X^2 - 2aX + 1).(X^2 + 2aX + 1)$$

□

4.2 IRREDUCIBLE POLYNOMIALS

Ex. 4.2.1 *This exercise will study the Lagrange interpolation formula. Suppose that F is a field and that $b_0, \ldots, b_d, c_0, \ldots, c_d \in F$, where $b_0, \ldots, b_d$ are distinct and $d \geq 1$. Then consider the polynomial*

$$g(x) = \sum_{i=0}^{d} c_i \prod_{j \neq i} \frac{x - b_j}{b_i - b_j} \in F[x].$$

(a) Explain why $\deg(g) \leq d$, *and give an example for $F = \mathbb{R}$ and $d = 2$ where* $\deg(g) < 2$.

(b) Show that $g(b_i) = c_i$ for $i = 0, \ldots, d$.

(c) Let h be a polynomial in $F[x]$ with $\deg(h) \leq d$ *such that $h(b_i) = c_i$ for $i = 0, \ldots, d$. Prove that $h = g$.*

Proof. Let $p_i(x) = \prod\limits_{j \neq i} \frac{x-b_j}{b_i-b_j}$ $, 0 \leq i \leq d$. Then $g(x) = \sum\limits_{i=0}^{d} c_i p_i(x)$.

(a) p_i is product of d linear polynomials, thus $\deg(p_i) = d$. Consequently $\deg(g) \leq \max(\deg(p_0), \ldots, \deg(p_d)) = d$:

$$\deg(g) \leq d.$$

This inequality can be a strict inequality : we show such an example for $d = 2$.
$(b_0, c_0) = (0, 0), (b_1, c_1) = (1, 1), (b_2, c_2) = (2, 2)$.
Then $p_0(x) = \frac{1}{2}(x-1)(x-2), p_1(x) = -x(x-2), p_2(x) = \frac{1}{2}x(x-1)$. So

$$\begin{aligned} g(x) &= 0.p_0(x) + 1.p_1(x) + 2.p_2(x) \\ &= -x(x-2) + x(x-1) \\ &= x \end{aligned}$$

Here $\deg(g) = 1 < d = 2$.

(b) $p_i(b_i) = 1$ and $p_i(b_j) = 0$ if $j \neq i$, so $p_i(b_j) = \delta_{i,j}$.

$$g(b_j) = \sum_{i=0}^{d} c_i \delta_{i,j} = c_j, \ j = 0, \ldots, d.$$

The graph of the polynomial g with degree at most d contains the $d + 1$ points $(b_0, c_0), \ldots, (b_d, c_d)$.

d) Suppose that the polynomial $h \in F[x]$ satisfies the same conditions as g :

$$h(b_i) = c_i, \ 0 \leq i \leq d, \text{ with } \deg(h) \leq d.$$

Let $p = g - h$. Then $\deg(p) \leq \max(\deg(g), \deg(h)) \leq d$, and $p(b_i) = g(b_i) - h(b_i) = c_i - c_i = 0, i = 0, \ldots, d$.

p is a polynomial with degree at most d and has $d + 1$ roots, hence $p = 0$, so

$$g = h.$$

Conclusion : there exists one and only one polynomial g with degree at most d such that $g(b_i) = c_i, \ i = 0, \ldots, d$ (where $b_0, \ldots, b_d$ are distinct, $d \geq 1$)

$\square$

Ex. 4.2.2 *This exercise deals with Schönemann's version of the irreducibility criterion.*

(a) Let $f(x) = (x-a)^n + pF(x)$, where $a \in \mathbb{Z}$ and $F(x) \in \mathbb{Z}[x]$ satisfy $\deg(F) \le n$, and $p \nmid F(a)$. Prove that f is irreducible over $\mathbb{Q}$.

(b) More generally, let $g(x) \in \mathbb{Z}[x]$ be irreducible modulo p (i.e., reducing its coefficients modulo p gives an irreducible polynomial in $\mathbb{F}_p[x]$). Then let $f(x) = g(x)^n + pF(x)$, where $F[x] \in \mathbb{Z}[x]$ and $g(x)$ and $F(x)$ are relatively prime modulo p. Also assume that $\deg(F) \le n \deg(g)$. Prove that f is irreducible over $\mathbb{Q}$.

Proof. (a) Let $f(x) = (x-a)^n + pF(x)$, where $a \in \mathbb{Z}$, p premieris prime. We show that f is irreducible by reductio ad absurdum. If we suppose that f is reducible over $\mathbb{Q}$, then by Corollary 4.2.1

$$f = gh, \ \ g,h \in \mathbb{Z}[x], k = \deg(g) \ge 1, l = \deg(h) \ge 1.$$

As $\deg(F) \le n$, $\deg(f) \le n$, and as the coefficient of x^n in f is congruent to 1 modulo p, it is nonzero, so $\deg(f) = n$, and $k + l = n$.

Write $\overline{f} \in \mathbb{F}_p[x]$ the reduction modulo p of f, and write $\overline{a} = [a]_p$ the class of $a \in \mathbb{Z}$ modulo p.

The application

$$\varphi : \mathbb{Z}[x] \to \mathbb{F}_p[x]$$
$$q = \sum_{i=0}^{d} a_i x^i \mapsto \overline{q} = \sum_{i=0}^{d} \overline{a_i} x^i$$

is a ring homomorphism, and so $\overline{f} = \overline{gh} = \overline{g}\,\overline{h}$.

Thus

$$\overline{f} = (x - \overline{a})^n = \overline{g}\overline{h}$$

As $\deg(\overline{g}) \le \deg(g), \deg(\overline{h}) \le \deg(h)$ and as $\deg(\overline{g}) + \deg(\overline{h}) = \deg((x-\overline{a})^n) = n = \deg(g) + \deg(h)$, we conclude that $\deg(\overline{g}) = \deg(g) = k, \deg(\overline{h}) = \deg(\overline{h}) = l$.

$x - \overline{a}$ is irreducible in $\mathbb{F}_p[x]$, as every polynomial of degree 1. $\mathbb{F}_p$ being a field, the unicity of the decomposition in irreducible factors in the principal ideal domain $\mathbb{F}_p[x]$ shows that the only irreducible factors of $\overline{g}, \overline{h}$ are associate to powers of $x - \overline{a}$:

$$\overline{g} = \overline{u}(x-\overline{a})^k, \overline{h} = \overline{v}(x-\overline{a})^l, \ \ \overline{u}, \overline{v} \in \mathbb{F}_p^*.$$

Hence there exist polynomials $G, H \in \mathbb{Z}[x]$ such that

$$g = u(x-a)^k + pG(x), h = v(x-a)^l + pH(x).$$

Consequently

$$f(x) = (x-a)^n + pF(x) = [u(x-a)^k + pG(x)][v(x-a)^l + pH(x)].$$

As $k \ge 1, l \ge 1$, $(x-a)^k$ et $(x-a)^l$ have the root a, thus

$$f(a) = pF(a) = p^2 G(a)H(a).$$

Then $F(a) = pG(a)H(a)$ is divisible by p, in contradiction with the hypothesis $p \nmid F(a)$.

Conclusion : $f \in \mathbb{Z}[x]$ is not product of nonconstant polynomials in $\mathbb{Z}[x]$. By Corollary 4.2.1, f is irreducible over $\mathbb{Q}$.

(b) More generally, suppose that $u \in \mathbb{Z}[x]$ is such that $\overline{u}$ is irreducible over $\mathbb{F}_p$, and that $f(x) = u(x)^n + pF(x)$, $F(x) \in \mathbb{Z}[x], \overline{u} \wedge \overline{F} = 1$ and $\deg(F) \le n \deg(u)$.

We must suppose also that the leading coefficient of u is not divisible by p, so $\deg(\overline{u}) = \deg(u)$.

Then $\deg(f) \le n \deg(u)$, and the coefficient of the monomial of degree $n \deg(u)$ being nonzero modulo p, $\deg(f) = n \deg(u) = n \deg(\overline{u}) = \deg(\overline{f})$.

If we suppose f reducible, then $f = gh, k = \deg(g) \ge 1, l = \deg(h) \ge 1$, which implies as in (a)

$$\overline{f} = \overline{u}^n = \overline{g}\overline{h}.$$

As $\overline{u}$ is irreducible,

$$\overline{g} = \overline{c}\,\overline{u}^i, \overline{h} = \overline{d}\,\overline{u}^j, \ i, j \in \mathbb{N}, \ \overline{c}, \overline{d} \in \mathbb{F}_p$$

As $\deg(\overline{g}) \le \deg(g), \deg(\overline{h}) \le \deg(g)$, and $\deg(\overline{g}) + \deg(\overline{h}) = \deg(\overline{f}) = \deg(f) = \deg(g) + \deg(h)$, we conclude $\deg(\overline{g}) = \deg(g) \ge 1, \deg(\overline{h}) = \deg(h) \ge 1$. Consequently $i \ge 1, j \ge 1$.

There exist polynomials $G, H \in \mathbb{Z}[x]$ such that

$$g = cu^i + pG, h = du^j + pH.$$

Thus

$$f = u^n + pF = (cu^i + pG)(du^j + pH).$$

As $i \ge 1, j \ge 1$, u divides $pF - p^2GH$ in $\mathbb{Z}[x]$: there exists $v \in \mathbb{Z}[x]$ such that

$$uv = p(F - pGH).$$

As $\overline{u}\,\overline{v} = 0$, and $\overline{u} \ne 0$ in the integral domain $\mathbb{F}_p[x]$, then $\overline{v} = 0$: tall the coefficients of v are divisible by p, thus $w = v/p \in \mathbb{Z}[x]$, and

$$uw = F - pGH, \qquad \overline{u}\,\overline{w} = \overline{F}.$$

Hencei $\overline{u} \mid \overline{F}$, in contradiction with the hypothesis $\overline{u} \wedge \overline{F} = 1$.

$f = u^n + pF$ is so irreducible.

□

Ex. 4.2.3 *Use part (a) of Exercise 2 with $a = 1$ to give another proof of Proposition 4.2.5.*

Proof. **Lemma** : *If p is prime, then for all $k, 0 \le k \le p - 1$,*

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

Proof by induction on k.
- If $k = 0$, $\binom{p-1}{0} = 1 = (-1)^0$.
- Suppose this property true for $k - 1$ $(1 \le k \le p - 1)$:

$$\binom{p-1}{k-1} \equiv (-1)^{k-1} \pmod{p}$$

Then, as $1 \leq k \leq p-1$, we know that $\binom{p}{k} \equiv 0$ $[p]$, thus from Pascal formula,

$$\binom{p-1}{k} = \binom{p}{k} - \binom{p-1}{k-1} \equiv 0 - (-1)^{k-1} \equiv (-1)^k \pmod{p},$$

which concludes the induction. $\square$

If $p = 2$, $\Phi_2 = 1 + x$ is irreducible. Suppose now that p is an odd prime.

Applying the lemma, we obtain

$$\begin{aligned}
\Phi_p(x) - (x-1)^{p-1} &= \sum_{k=0}^{p-1} x^k - \sum_{k=0}^{p-1} (-1)^{p-1-k} \binom{p-1}{k} x^k \\
&= \sum_{k=0}^{p-1} \left[1 - (-1)^{p-1-k} \binom{p-1}{k} \right] x^k \\
&= \sum_{k=0}^{p-1} \left[1 - (-1)^{k} \binom{p-1}{k} \right] x^k \\
&= p \sum_{k=0}^{p-1} a_k x^k \qquad (a_k \in \mathbb{Z})
\end{aligned}$$

since every coefficient $\left[1 - (-1)^k \binom{p-1}{k}\right]$ is divisible by p, of the form $pa_k, a_k \in \mathbb{Z}$.

Consequently

$$\Phi_p(x) = (x-1)^{p-1} + pF(x), F(x) = \sum_{k=0}^{p-1} a_k x^k \in \mathbb{Z}[x], \deg(F) \leq p-1.$$

Moreover

$$F(1) = \sum_{k=0}^{p-1} a_k = \sum_{k=0}^{p-1} \frac{1 - (-1)^k \binom{p-1}{k}}{p} = 1 - \frac{1}{p} \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} = 1 - \frac{1}{p}(1-1)^{p-1} = 1.$$

$F(1) \not\equiv 0[p]$. By Exercise 2, Φ_p is irreducible. $\square$

Ex. 4.2.4 *For each of the following polynomials, use a computer to determine wheter it is irreducible over the given field.*

Proof. (a) With Sage, the instructions

```
factor(x^4+x^3+x^2+x+2)
factor(3*x^6+6*x^5+9*x^4+2*x^3+3*x^2+1);
```

give the same polynomials.

So $x^4 + x^3 + x^2 + x + 2$ and $3x^6 + 6x^5 + 9x^4 + 2x^3 + 3x^2 + 1$ are irreducible over $\mathbb{Q}$.

(b) The instructions

```
K = NumberField(x^3-2, 'a'); L.<X> = PolynomialRing(K)
p =  3*x^6 + 6*x^5 + 9*x^4 + 2*x^3 + 3*x^2 + 1
u = factor(p)
```

give the following decomposition, where $a = \sqrt[3]{2}$:
$3x^6 + 6x^5 + 9x^4 + 2x^3 + 3x^2 + 1 =$
$\frac{1}{3}(3x^2 + (-a^2 + a + 2)x + a^2 - a + 1)\times$
$(3x^4 + (a^2 - a + 4)x^3 + (a + 4)x^2 + (-a^2 - a)x + a + 1)$
Thus $3x^6 + 6x^5 + 9x^4 + 2x^3 + 3x^2 + 1$ is not irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

□

Ex. 4.2.5 *Find the minimal polynomial of the 24th root of unity ζ_{24} as follows.*

(a) Factor $x^24 - 1$ over $\mathbb{Q}$. Determine which of the factors is the minimal polynomial of ζ_{24}.

Proof. (a) The instruction Sage 'factor' gives the decomposition
$x^{24} - 1 = (x^8 - x^4 + 1)(x^4 - x^2 + 1)(x^4 + 1)(x^2 + x + 1)(x^2 - x + 1)(x^2 + 1)(x + 1)(x - 1)$

(b) The Sage instructions

```
zeta = exp(2*i*pi/24)
(x^8 - x^4 + 1).subs(x=zeta).expand()
```

return the value 0.
Thus $\zeta_{24} = e^{2i\pi}/24$ is a root of $x^8 - x^4 + 1$, irreducible over $\mathbb{Q}$ by (a).
$x^8 - x^4 + 1$ is so the minimal polynomial over $\mathbb{Q}$ of ζ_{24}.
Verification : $\zeta_{24}^8 - \zeta_{24}^4 + 1 = e^{2i\pi/3} - e^{i\pi/3} + 1 = \omega + \omega^2 + 1 = 0$.
Note : if we know the cyclotomic polynomials, as is prime :

$$\begin{aligned}
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_6(x) &= \Phi_3(-x) = x^2 - x + 1 \\
\Phi_{24}(x) &= \Phi_{\mathrm{rad}(24)}(x^{\frac{24}{\mathrm{rad}(24)}}) = \Phi_6(x^4) = x^8 - x^4 + 1
\end{aligned}$$

$(24 = 3 \times 2^3, \mathrm{rad}(24) = 3 \times 2 = 6)$

Φ_{24} is the minimal polynomial of ζ_{24} sur $\mathbb{Q}$. The decomposition in (a) is the decomposition

$$x^{24} - 1 = \prod_{d|24} \Phi_d(x) = \Phi_{24}\,\Phi_{12}\,\Phi_8\,\Phi_3\,\Phi_6\,\Phi_4\,\Phi_2\,\Phi_1.$$

□

Ex. 4.2.6 *Let F be a finite field. Explain why there is an algorithm for deciding whether $f \in F[x]$ is irreducible.*

Proof. If f is reducible, of degree n, $f = gh, g, h \in F[x]$, where $1 \le \deg(g) \le \deg(h) \le n - 1$.

As $\deg(g) + \deg(h) = n$, $2\deg(g) \le n, \deg(g) \le n/2$. If we multiply g, h by appropriate constants, we can suppose that g is monic.

So f is reducible iff there exists a monic factor of f of degree d, $d, 1 \le d \le n/2$.

As F is finite, with cardinality q, we can list all monic polynomials of degree k, of the form $p = x^k + a_{k-1}x^{k-1} + \cdots + a_0$, by listing all q^k k-plets $(a_0, \cdots, a_{k-1})$, and test the divisibility of f by each such polynomial, for every value of $k, 1 \le k \le n/2$.

If f is irreducible, the number of polynomial division to prove the irreducibility is so

$$q + q^2 + \cdots q^r = q\,\frac{q^r - 1}{q - 1}, \qquad r = \lfloor n/2 \rfloor.$$

□

Ex. 4.2.7 *For each of the following polynomials, determine, without using a computer, whether it is irreducible over the given field.*

(a) $x^3 + x + 1$ *over* $\mathbb{F}_5$.

(b) $x^4 + x + 1$ *over* $\mathbb{F}_2$.

Proof. (a) $f = x^3 + x + 1$ being of degree 3, it is reducible iff it has a linear factor (see Ex. 6), iff it has a root in $\mathbb{F}_5$, which request 5 verifications :

$f(0) = 1, f(1) = 3, f(2) = 1, f(-2) = 1, f(-1) = -1$, all nonzero, so f is irreducible over $\mathbb{F}_5$..

(b) $f = x^4 + x + 1$ has no root in $\mathbb{F}_2$.

It is so sufficient to test the divisibility of f by quadratic polynomials, which are

$$x^2, x^2 + 1, x^2 + x, x^2 + x + 1.$$

x^2 et $x^2 + x$ are not irreducible, can be excluded of the list. It remains to test two divisons by

$$x^2 + 1, x^2 + x + 1$$

.

$$\begin{aligned} x^4 + x + 1 &= (x^2 + 1)(x^2 + 1) + x \\ &= (x^2 + x + 1)(x^2 + x) + 1 \end{aligned}$$

The remainders of these divisions being nonzero, $x^4 + x + 1$ is so irreducible over $\mathbb{F}_2$.

Note : the factorization of Φ_{15} over the field $\mathbb{F}_2$, gives the list of irreducible polynomials over $\mathbb{F}_2$.

```
S.<t> = GF(2)['t']
phi15 =( (x^15-1)*(x-1)*(x-1))/((x-1)*(x^3-1)*(x^5-1)); phi15
x^8 + x^7 + x^5 + x^4 + x^3 + x + 1
factor(phi15)
(x^4 + x + 1) * (x^4 + x^3 + 1)
```

□

Ex. 4.2.8 *Let $a \in \mathbb{Z}$ be a product of distinct prime numbers. Prove that $x^n - a$ is irreducible over $\mathbb{Q}$ for any $n \geq 1$. What does this imply about $\sqrt[n]{a}$ when $n \geq 2$.*

Proof. Let $a = p_1 \cdots p_r$ a product of distinct prime numbers.

With a reductio ad absurdum, suppose that f is reducible. By Gauss Lemma f has a monic factor $g \in \mathbb{Z}[x], 1 \leq \deg(g) < n$.

$$f = \prod_{\zeta \in \mathbb{U}_n} (x - \zeta \sqrt[n]{a}).$$

$\mathbb{C}[x]$ being a unique facoirization domain,

$$g = \prod_{\zeta \in A} (x - \zeta \sqrt[n]{a}), \emptyset \neq A \subsetneq \mathbb{U}_n$$

$|A| = s$ satisfies $1 \leq s < n$.

As $g \in \mathbb{Z}[x]$, the constant term is an integer N, given by

$$N = \xi \sqrt[n]{a}^s,$$

where $\xi = \prod_{\zeta \in A} \zeta \in \mathbb{U}_n$ is a n-th root of unity.

Moreover $\xi = N / \sqrt[n]{a}^s \in \mathbb{R}$, thus $\xi = \pm 1$, and $\sqrt[n]{a}^s = \pm N = M \in \mathbb{Z}$.

But then $p_1^s \cdots p_r^s = M^n$.

The unicity of the decomposition in prime factors shows that the p_i are the only prime divisors of M : $M = p_1^{k_1} \cdots p_r^{k_r}$, and $s = nk_i, i = 1, \ldots, r$.

Thus $n \mid s$, in contradiction with $1 \leq s < n$.

Conclusion : $x^n - a$ is irreducibal $\mathbb{Q}$, if $a = p_1 \cdots p_r$ is a product of distinct prime numbers.

The easy part of Proposition 4.2.6 shows that $x^n - a, n \geq 2$ has no root in $\mathbb{Q}$, in other words $\sqrt[n]{a}$ is irrational, for every a being a product of distinct prime numbers. $\square$

Ex. 4.2.9 *Let k be a field, and let $F = k(t)$ be the field of rational functions in t with coefficients in k. Then consider $f = x^p - t \in F[x]$, where p is prime. By Proposition 4.2.6, f is irreducible provided we can show that f has no roots in F. Prove this.*

Proof. If f has a root in $k(t)$, then there exist a rational function $u/v,\ u, v \in k[t], u \wedge v = 1$ such that

$$t = \left(\frac{u(t)}{v(t} \right)^p,$$

which is equivalent to the equality in $k[t]$:

$$u(t)^p = tv(t)^p.$$

As $u \wedge v = 1$, then $u \wedge v^p = 1$, and u divides tv^p, thus u divides t.

Since t is irreducible (as every polynomial of degree 1), $u(t) = \lambda$, or $u(t) = \lambda t$, $\lambda \in k^*$.

The case $u(t) = \lambda$ implies $t \mid 1$, which is false.

The case $u(t) = \lambda t$ gives $\lambda^p t^p = tv(t)^p$, thus $\lambda^p t^{p-1} = v(t)^p$, and as $p > 1$, t divides also v, which contradicts $u \wedge v = 1$.

Conclusion : if p is prime, $f = x^p - t$ is irreducible over $F = k(t)$. $\square$

4.3 THE DEGREE OF AN EXTENSION

Ex. 4.3.1 *In (4.9) we represented elements of $F(\alpha)$ uniquely using remainders on division by the minimal polynomial of α. In the exercise you will adapt the proof of Proposition 4.3.4 to the case of quatient rings. Suppose that $f \in F[x]$ has degree $n > 0$. Prove that every coset on $F[x]/\langle f \rangle$ can be written as*

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + \langle f \rangle,$$

where $a_0, a_1, \ldots, a_{n-1} \in F$ are unique.

Proof. Let $f \in F[x], \deg(f) = n > 0$, and $y \in F[x]/\langle f \rangle$. There exists $g \in F[x]$ such that $y = g + \langle f \rangle$.

The division of g by f gives

$$g = qf + r, \ \deg(r) < \deg(f) = n.$$

Thus $g - r = qf \in \langle f \rangle$, and consequently $y = g + \langle f \rangle = r + \langle f \rangle$.

As $\deg(r) < n$, $r = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, a_0, a_1, \ldots, a_{n-1} \in F$.

Every $y \in F[x]/\langle f \rangle$ can be written as

$$y = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + \langle f \rangle, \ a_0, a_1, \ldots, a_{n-1} \in F.$$

Unicité :

Suppose that $y \in g + \langle f \rangle$ is written as

$$\begin{aligned} y &= a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + \langle f \rangle \\ &= b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + \langle f \rangle \end{aligned}$$

$(a_i, b_i \in F, i = 0, \ldots, n-1)$.

Then there exist two polynomials $a, b \in \langle f \rangle$ tsuch that

$$p = \sum_{k=0}^{n-1} a_k x^k + a = \sum_{k=0}^{n-1} b_k x^k + b.$$

Let $r = \sum_{k=0}^{n-1} a_k x^k, s = \sum_{k=0}^{n-1} b_k x^k$. By definition of $\langle f \rangle$, there exists $q_1, q_2 \in F[x]$ such that

$$p = q_1 f + r = q_2 f + s, \qquad \deg(r) < n, \deg(s) < n.$$

The unicity of the remainder in the division of p by f shows that $r = s$, so $a_i = b_i, i = 0, \ldots, n-1$.

Conclusion : every element in $F[x]/\langle f \rangle$ is written as

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + \langle f \rangle, \qquad a_0, a_1, \ldots, a_{n-1} \in F.$$

where $a_0, a_1, \ldots, a_{n-1}$ are unique. ☐

Ex. 4.3.2 *Compute the degree of the following extensions:*

(a) $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt[4]{2})$.

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

(c) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2+\sqrt{2}})$

(d) $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{2+\sqrt{2}})$.

Proof. (a) $\sqrt[4]{2}$ is a root of $p = x^4 - 2 \in \mathbb{Q}[x]$, and p is irreducible over $\mathbb{Q}$ by Exercise 4.2.8 (or Schönemann-Eisenstein Criterion for the prime 2). Thus

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

i is a root of $x^2 + 1$, which has no root in $\mathbb{R}$, a fortiori in $\mathbb{Q}[\sqrt[4]{2}]$. As its degree is 2, it is irreducible over $\mathbb{Q}[\sqrt[4]{2}]$, thus

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2.$$

Moreover $\mathbb{Q}(i, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$. The tower theorem gives

$$[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \times [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8.$$

(b) $\sqrt[3]{2}$ is irrational, so well that $f = x^3 - 2$ has no root in $\mathbb{Q}$, and $\deg(f) = 3$, thus f is irreducible over $\mathbb{Q}$ and f is the minimal polynomial over $\mathbb{Q}$ of $\sqrt[3]{2}$, and so

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

The roots of $x^2 - 3$ are $\pm\sqrt{3}$ and are irrational. As $\deg(x^2 - 3) = 2$, and as $x^2 - 3$ has no root in $\mathbb{Q}$, $x^2 - 3$ is irreducible over $\mathbb{Q}$: it is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}$, thus

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2.$$

Moreover

$$\begin{aligned}[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] \times [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})] \\ &= [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})] \times [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}],\end{aligned}$$

thus, if we write $d = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}]$, then $2 \mid d, 3 \mid d$, with $2 \wedge 3 = 1$, thus $6 \mid d$, $6 \le d$.

$x^2 - 3$ has the root $\sqrt{3}$ and its degree is 2. Its coefficients are in $\mathbb{Q}$, a fortiori in $\mathbb{Q}(\sqrt[3]{2})$. Thus the minimal polynomial p of $\sqrt{3}$ over $\mathbb{Q}(\sqrt[3]{2})$ divides $x^2 - 3$: its degree $\delta = \deg(p) = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})]$ satisfies then $\delta \le 2$.

As $d = 3\delta \ge 6$, and $\delta \le 2$, $\delta = 2$, and so $d = 6$.

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] = 6.$$

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

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

α is a root of

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

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

Conclusion : $f = x^4 - 4x^2 + 2$ is irreducible over $\mathbb{Q}$. f is the minimal polynomial of $\alpha = \sqrt{2+\sqrt{2}}$, thus

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

(d) $x^2 + 1$ has no real root, a fortiori no root in $\mathbb{Q}(\sqrt{2+\sqrt{2}})$, and $\deg(x^2 + 1) = 2$. Thus x^2+1 is irreducible over $\mathbb{Q}(\sqrt{2+\sqrt{2}})$: it is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2+\sqrt{2}})$, thus

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

Consequently

$$\left[\mathbb{Q}\left(i, \sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(i, \sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)\right] \times \left[\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\right] = 8.$$

□

Ex. 4.3.3 *For each of the extensions in Exercise 2, find a basis over $\mathbb{Q}$ using the method of Example 4.3.9.*

Proof. (a) $(1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3)$ is a basis of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, and $(1, i)$ a basis of $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(\sqrt[4]{2})$, thus

$$(1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3, i, i\sqrt[4]{2}, i\sqrt[4]{2}^2, i\sqrt[4]{2}^3)$$

is a basis of $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$

(b) $(1, \sqrt[3]{2}, \sqrt[3]{2}^2)$ is a basis of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, and $(1, \sqrt{3})$ a basis of $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})$, thus

$$(1, \sqrt[3]{2}, \sqrt[3]{2}^2, \sqrt{3}, \sqrt{3}\sqrt[3]{2}, \sqrt{3}\sqrt[3]{2}^2)$$

is a basis of $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})/\mathbb{Q}$.

(c) The minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$ being of degree 4,

$$\left(1, \sqrt{2+\sqrt{2}}, \sqrt{2+\sqrt{2}}^2 = 2+\sqrt{2}, \sqrt{2+\sqrt{2}}^3 = (2+\sqrt{2})\sqrt{2+\sqrt{2}}, \sqrt{2+\sqrt{2}}^4 = (2+\sqrt{2})^2\right)$$

is a basis of $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)/\mathbb{Q}$.

(d) A basis of $\mathbb{Q}\left(i, \sqrt{2+\sqrt{2}}\right)/\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ being $(1, i)$,

$$(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3), \qquad \text{where } \alpha = \sqrt{2+\sqrt{2}},$$

is a basis of $\mathbb{Q}\left(i, \sqrt{2+\sqrt{2}}\right)/\mathbb{Q}$.

□

Ex. 4.3.4 *Suppose that $F \subset L$ is a finite extension with $[L : F]$ prime.*

(a) Show that that the only subfields of L containing F are F and L.

(b) Show that $L = F(\alpha)$ for any $\alpha \in L \setminus F$.

Proof. (a) If a subfield K of L satisfies $F \subset K \subset L$, then

$$[L : F] = [L : K][K : F],$$

so $[K : F]$ divides $p = [L : F]$, where p is a prime.

If $[K : F] = 1$, then $K = F$, and if $[K : F] = p$, then $[L : K] = 1$, thus $K = L$.

Conclusion : if $[L : F]$ is a prime number, the only intermediate subfields of the extension $F \subset L$ are L et F.

(b) If $\alpha \notin F$, then $F(\alpha) \neq F$, thus by (a), $F(\alpha) = L$.

$\square$

Ex. 4.3.5 *Consider the extension $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt[4]{2}, \sqrt[3]{3})$. We will compute $[L : \mathbb{Q}]$.*

(a) Show that $x^4 - 2$ and $x^3 - 3$ are irreducible over $\mathbb{Q}$.

(b) Use $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset L$ to show that $4 \mid [L : \mathbb{Q}]$ and $[L : \mathbb{Q}] \leq 12$.

(c) Use $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{3}) \subset L$ to show that $[L : \mathbb{Q}]$ is also divisible by 3.

(d) Explain why parts (b) and (c) imply that $[L : \mathbb{Q}] = 12$. This works because 3 and 4 are relatively prime. Do you see why ?

Proof. (a) The Scönemann-Eisenstein Criterion with $p = 2$ shows that $x^4 - 2$ is irreducible over $\mathbb{Q}$, and with $p = 3$ shows that $f = x^3 - 3$ is irreducible over $\mathbb{Q}$. (Alternatively, we can use Exercise 4.2.8).

(b) As $x^4 - 2$ is irreducible over $\mathbb{Q}$ by (a) d'après le (a),$x^4 - 2$ is the minimal polynomial over $\mathbb{Q}$ of $\sqrt[4]{2}$.

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})] \times [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}],$$

thus $4 = \deg(x^4 - 2) = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$ divides $[L : \mathbb{Q}]$.

As $x^3 - 3 \in \mathbb{Q}[x]$ is a fortiori in $\mathbb{Q}(\sqrt[4]{2})[x]$, the minimal polynomial P of $\sqrt[3]{3}$ over $\mathbb{Q}(\sqrt[4]{2})$ divides $x^3 - 3$: so its degree satisfies $\deg(P) \leq 3$. Consequently, $[L : \mathbb{Q}(\sqrt[4]{2})] = \deg(P) \leq 3$ (et $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$), thus

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})] \times [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \leq 12$$

(c) Similarly, $x^3 - 3$ is the minimal polynomial of $\sqrt[3]{3}$ over $\mathbb{Q}$.

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{3})] \times [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}],$$

thus $3 = \deg(x^3 - 3) = [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}]$ divides $[L : \mathbb{Q}]$.

(d) As $3 \mid [L : \mathbb{Q}]$, and as $4 \mid [L : \mathbb{Q}]$, where 3 et 4 are relatively prime,

$$12 = 3 \times 4 \mid [L : \mathbb{Q}].$$

In particular, $12 \leq [L : \mathbb{Q}]$. By (b), $12 \geq [L : \mathbb{Q}]$, thus

$$[L : \mathbb{Q}] = 12.$$

$\square$

Ex. 4.3.6 *Suppose that α and β are algebraic over F with minimal polynomials f and g respectively. Prove the* **Reciprocity theorem***: f is irreducible over $F(\beta)$ if and only if g is irreducible over $F(\alpha)$.*

Proof. Write $d_1 = [F(\alpha) : F], \delta_1 = [F(\alpha, \beta) : F(\alpha)], d_2 = [F(\beta) : F], \delta_2 = [F(\alpha, \beta) : F(\beta)]$.

The tower Theorem gives the two relations

$$[F(\alpha, \beta) : F] = \delta_1 d_1 = \delta_2 d_2. \tag{1}$$

Suppose that f is irreducible over $F(\beta)$ (this makes sense because $f \in F[x]$ has a fortiori its coefficients in $F(\beta)$).

Then f is the minimal polynomial of α over $F(\beta)$, thus

$$\delta_2 = [F(\alpha, \beta), F(\beta)] = \deg(f) = d_1.$$

$\delta_2 = d_1$, combined with the relation (**??**), gives $\delta_1 = d_2$.

Let G the minimal polynomial of β sur $F(\alpha)$.

As $g \in F[x] \subset F(\alpha)[x]$, and $g(\beta) = 0$, then $G \mid g$, and $\deg(g) = d_2 = \delta_1 = \deg(G)$, where g and G are monic, thus $g = G$.

As G is irreducible over $F(\alpha)$, g is also irreducible over $F(\alpha)$.

We have proved :

$$f \text{ is irreducible over } F(\beta) \Rightarrow g \text{ is irreducible over } F(\alpha).$$

The proof of the converse is similar, by exchange of α, β.

$$f \text{ is irreducible over } F(\beta) \iff g \text{ is irreducible over } F(\alpha).$$

□

Ex. 4.3.7 *Suppose we have extensions $L_0 \subset L_1 \subset \cdots \subset L_m$. Use induction to prove the following generalization of Theorem 4.3.8:*

(a) If $[L_i : L_{i-1}] = \infty$ for some $1 \le i \le m$, then $[L_m : L_0] = \infty$.

(b) If $[L_i : L_{i-1}] < \infty$ for all $1 \le i \le m$, then

$$[L_m : L_0] = [L_m : L_{m-1}][L_{m-1} : L_{m-2}] \cdots [L_2 : L_1][L_1 : L_0].$$

Proof. (a) The tower theorem shows that (a) et (b) are true for $m = 2$. Suppose that (a) et (b) are true for an integer $m \ge 2$. We prove that they remain true for the integer $m + 1$.

- Si $[L_i : l_{i-1}] = \infty$ pour un indice $i, 1 \le i \le m$, the induction hypothesis show that $[L_m : L_0] = \infty$, and as $L_0 \subset L_m \subset L_{m+1}$, the part (a) of Theorem 4.3.8 (tower theorem), shows that $[L_{m+1} : L_0] = \infty$.

Moreover, if $[L_{m+1} : l_m] = \infty$, this same part (a) gives also $[L_{m+1} : L_0] = \infty$.

For all $i, 1 \le i \le m + 1$,

$$[L_i : l_{i-1}] = \infty \Rightarrow [L_{m+1} : L_0] = \infty :$$

so the part (a) is proved for the integer $m + 1$.

- Suppose that $[L_i : L_{i-1}] < \infty$ pour tout $i, 1 \leq i \leq m+1$. The induction hypothesis gives then

$$[L_m : L_0] = \prod_{1 \leq i \leq m} [L_i : L_{i-1}]$$

The part (b) of theorem 4.3.8 imples that

$$\begin{aligned}[L_{m+1} : L_0] &= [L_{m+1} : L_m] \times [L_m : L_0] \\ &= [L_{m+1} : L_m] \times \prod_{1 \leq i \leq m} [L_i : L_{i-1}] \\ &= \prod_{1 \leq i \leq m+1} [L_i : L_{i-1}].\end{aligned}$$

So the induction is done.

□

4.4 ALGEBRAIC EXTENSIONS

Ex. 4.4.1 *Lemma 4.4.2 shows that a finite extension is algebraic. Here we will give an example to show that the converse is false. The field of algebraic numbers $\overline{Q}$ is by definition algebraic over $\mathbb{Q}$. You will show that $[\overline{Q} : \mathbb{Q}] = \infty$ as follows*

(a) Given $n \geq 2$ in $\mathbb{Z}$, use Example 4.2.4 from section 4.2 to show that $\overline{Q}$ has a subfield L such that $[L : \mathbb{Q}] = n$.

(b) Explain why part (a) implies that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Proof. (a) In Example 4.2.4, we have seen that the Schönemann-Eisenstein Criterion implies that, for all $n \geq 2$, and p prime,

$$f = x^n + px + p$$

is irreducible over $\mathbb{Q}$. Let α a root of f in $\mathbb{C}$. Since f is irreducible over $\mathbb{Q}$, lthe minimal polynomial of α over $\mathbb{Q}$ is f, and

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = n.$$

As $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$, every element of $\mathbb{Q}(\alpha)$ is algebraic, so

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \overline{\mathbb{Q}}.$$

$L = \mathbb{Q}(\alpha)$ is so an answer to the question.

(b) By reductio ad absurdum, suppose that $[\overline{\mathbb{Q}} : \mathbb{Q}] < \infty$. The tower theorem gives then

$$[\overline{\mathbb{Q}} : \mathbb{Q}] = [\overline{\mathbb{Q}} : \mathbb{Q}(\alpha)] \times [\mathbb{Q}(\alpha) : \mathbb{Q}] \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] \geq n.$$

Then for all integer $n \geq 2$, $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$, thus $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$, which is a contradiction.

Conclusion : $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

$\overline{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$, with infinite dimension.

□

Ex. 4.4.2 *Let $\alpha \in \mathbb{C}$ be a solution of (4.14). We will show that the minimal polynomial of α over $\mathbb{Q}$ has degree at most* 1760. *Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt[4]{12}, i, \sqrt[5]{17}, \alpha)$.*

(a) Show that $[L : \mathbb{Q}] \leq 1760$.

(b) Use Lemme 4.4.2 to show that the minimal polynomial polynomial of α has degree at most 1760.

Proof. (a) Let $\alpha \in \mathbb{C}$ a root of

$$f = x^{11} - (\sqrt{2} + \sqrt{5})x^5 + 3\sqrt[4]{12}x^3 + (1 + 3i)x + \sqrt[5]{17}.$$

Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt[4]{12}, i, \sqrt[5]{17}, \alpha)$, and $K = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt[4]{12}, i, \sqrt[5]{17})$.
$f \in K[x]$, and α is a root of f. The minimal polynomial p of α over K divides f, thus $[L : K] = [K(\alpha) : K] = \deg(p) \leq \deg(f) = 11$:

$$[L : K] \leq 11.$$

Moreover, if we write
$K_4 = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt[4]{12}, i), K_3 = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt[4]{12}), K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{5}), K_1 = \mathbb{Q}(\sqrt{2})$,
then

$$\begin{aligned}
[K : \mathbb{Q}] &= [K : K_4].[K_4 : K_3].[K_3 : K_2].[K_2 : K_1].[K_1 : \mathbb{Q}] \\
&= [K_4(\sqrt[5]{17}) : K_4].[K_3(i) : K_3].[K_2(\sqrt[4]{12}) : K_2].[K_1(\sqrt{5}) : K_1].[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]
\end{aligned}$$

The minimal polynomial P of $\sqrt[5]{17}$ over K_4 divides $x^5 - 17 \in \mathbb{Q}[x] \subset K_4[x]$, thus $[K_4(\sqrt[5]{17}) : K_4] = \deg(P) \leq 5$. With similar arguments,

$$[K_3(i) : K_3] \leq 2, [K_2(\sqrt[4]{12}) : K_2] \leq 4, [K_1(\sqrt{5}) : K_1] \leq 2, [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \leq 2,$$

Consequently

$$[K : \mathbb{Q}] \leq 5 \times 2 \times 4 \times 2 \times 2 = 160$$

and

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] \leq 11 \times 160 = 1760.$$

(b) By Lemma 4.4.2(b), as $\alpha \in L$, the degree of the minimal polynomial of α over $\mathbb{Q}$ divides $[L : \mathbb{Q}] = 1760$.

□

Ex. 4.4.3 *In the Mathematical Notes, we defined an algebraic integer to be a complex number $\alpha \in \mathbb{C}$ that is a root of a monic polynomial in $\mathbb{Z}[x]$.*

(a) Prove that $\alpha \in \mathbb{C}$ is an algebraic integer if and only if α is an algebraic number whose minimal polynomial over $\mathbb{Q}$ has integer coefficients.

(b) Show that $\omega/2$ is not an algebraic integer, where $\omega = (-1 + i\sqrt{3})/2$.

Proof. (a) • Following this definition, suppose that $p(\alpha) = 0$, where $p \in \mathbb{Z}[x]$ is monic.

Soit $P \in \mathbb{Q}[x]$ the minimal polynomial of α over $\mathbb{Q}$. Then P divides p in $\mathbb{Q}[x]$: there exists $q \in \mathbb{Q}[x]$ such that $p = Pq$.

By Gauss Lemma, Proposition A.3.2 of appendix A, there exists $\delta \in \mathbb{Q}^*$ such that $\tilde{P} = \delta P$ et $\tilde{q} = \delta^{-1} q$ have integer coefficients. So $p = \tilde{P}\tilde{q}, \tilde{P}, \tilde{q} \in \mathbb{Z}[x]$.

As p is monic, $\pm\tilde{P}, \pm\tilde{q}$ are also monic. Possibly by multiplying δ by -1, we can so suppose that $\tilde{P}, \tilde{q}$ are monic. Thus $P = \tilde{P}$, and so $P \in \mathbb{Z}[x]$.

• The converse is straightforward : if the minimal polynomial P of α over $\mathbb{Q}$ has integer coefficients, P is an example of monic polynomial such that $P(\alpha) = 0$, so α is an algebraic integer.

Conclusion : α is an algebraic integer iff the minimal polynomial of α over $\mathbb{Q}$ has integer coefficients.

(b) $\omega/2$ is a root of $x^2 + \frac{1}{2}x + \frac{1}{4}$, and $f = \omega/2 \notin \mathbb{Q}$, thus $x^2 + \frac{1}{2}x + \frac{1}{4}$ is the minimal polynomial of α over $\mathbb{Q}$. I$f \notin \mathbb{Z}[x]$: by part (a), $\omega/2$ is not an algebraic integer.

□

Ex. 4.4.4 *Use (4.10) and (4.11) to prove the following weak form of Lemma 4.4.2: if $n = [L : F] < \infty$, then every $\alpha \in L$ is a root of a nonzero polynomial of degree $\leq n$.*

Proof. If $n = [L : F] < \infty$, and $\alpha \in L$, then $(1, \alpha, \alpha^2, \cdots, \alpha^n)$ has $n+1$ elements in a space of dimension n. Thus there exists $(a_0, \cdots, a_n) \neq (0, \cdots, 0)$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. If we write $P = \sum_{i=0}^n a_i x^i$, then $P \neq 0$, and $P(\alpha) = 0, \deg(P) \leq n$.

Conclusion : if $n = [L : F] < \infty$, every $\alpha \in L$ is a root of a nonzero polynomial of degree at most n.

□

Ex. 4.4.5 *In 1873 Hermite proved that the number e is transcendental over $\mathbb{Q}$, and in 1882, Lindemann show that π is transcendental over $\mathbb{Q}$. It is unknown whether $\pi + e$ and $\pi - e$ are transcendental. Prove that* **at least** *one of these numbers is transcendental over $\mathbb{Q}$.*

Proof. If $\pi + e$ and $\pi - e$ were both algebraic, then $\pi + e, \pi - e \in \overline{\mathbb{Q}}$. As $\overline{\mathbb{Q}}$ is a field containing $\mathbb{Q}$, we should have

$$\pi = \frac{1}{2}\left((\pi + e) + (\pi - e)\right)$$

element of $\overline{\mathbb{Q}}$, which is false.

At least one of the numbers $\pi + e, \pi - e$ is transcendental over $\mathbb{Q}$.

□

Ex. 4.4.6 *Let F be a field. Show that other than the elements of F itself, no elements of $F(x)$ are algebraic over F.*

Proof. Let $f \in F(x), f \neq 0$. Then $f = p/q,\ p, q \in F[x],\ p \wedge q = 1,\ p \neq 0, q \neq 0$.

If f is algebraic over F, let $P = \sum_{k=0}^{d} a_i x^k \in F[x]$ the minimal polynomial f over F, of degree n. Then $a_n = 1 \neq 0$, and $a_0 \neq 0$ (if $a_0 = 0$, P/x has the root f and so P should not be the minimal polynomial). Then

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_0 = 0,$$

thus

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n = 0.$$

This equality, with $a_0 \neq 0, a_n \neq 0$, shows that $p \mid q^n$, with $p \wedge q = 1$, so $p \wedge q^n = 1$ shows that $p \mid 1$. Similarly $q \mid 1$. Thus $\deg(p) = \deg(q) = 0$, and so $f = p/q \in F$.

The only elements of $F(x)$ which are algebraic over F are the elements of F. □

Ex. 4.4.7 *Suppose that F is an algebraically closed field, and let $F \subset L$ be an algebraic extension. Prove that $F = L$.*

Proof. Let $\alpha \in L$. As L is algebraic over F, α is algebraic over F. Let $f \in F[x]$ the minimal polynomial of α over F.

As F is an algebraically closed field, f is a product of linear factors in $F[x]$, thus all the roots of f are in F. In particular, $\alpha \in F$ (and so f has degree 1). This proves the inclusion $L \subset F$, and as $F \subset L$, $F = L$.

An algebraically closed field has no proper algebraic extension. □

Ex. 4.4.8 *In this exercise you will show that every algebraic extension of $\mathbb{R}$ is finite of degree at most 2. To prove this, consider an extension $\mathbb{R} \subset L$.*

(a) Explain why we can find an extension $L \subset K$ such that $x^2 + 1$ has a root $\alpha \in K$.

(b) Prove that $L(\alpha)$ is algebraic over $\mathbb{R}(\alpha)$ and that $\mathbb{R}(\alpha) \simeq \mathbb{C}$.

(c) Now use the previous exercise to conclude that $[L : \mathbb{R}] \leq 2$ and that equality occurs if and only if $L \simeq \mathbb{C}$

Proof. (a) Soit $\mathbb{R} \subset L$ an algebraic extension.

If $x^2 + 1$ has a root α in L, we can take $K = L$. Otherwise $x^2 + 1$, being of degree 2, is irreducible over L, thus $K = L[x]/\langle x^2 + 1\rangle$ if an extension of L containing $\alpha = \overline{x} = x + \langle x^2 + 1\rangle$, root of $x^2 + 1$ in K.

In the two cases, there exists an extension $L \subset K$ such that $x^2 + 1$ has a root α in K (and $[L[\alpha] : L] \leq \deg(x^2 + 1) = 2$).

(b) Let $\beta \in L(\alpha)$. As $L[\alpha]$ is algebraic over L (since $[L(\alpha) : L] \leq 2$), and as L is algebraic over $\mathbb{R}$, the Theorem 4.4.7 shows that β is algebraic over $\mathbb{R}$. As the coefficients of the minimal polynomial of β over $\mathbb{R}$ are real, these coefficients are a fortiori in $\mathbb{R}(\alpha)$, thus $L(\alpha)$ is algebraic over $\mathbb{R}(\alpha)$.

As α is a root of $x^2 + 1$, irreducible over $\mathbb{R}$, $\mathbb{R}(\alpha) = \mathbb{R}[\alpha] \simeq \mathbb{R}[x]/\langle x^2 + 1\rangle \simeq \mathbb{C}$.

(c) As $\mathbb{R}(\alpha)$ is isomorphic to $\mathbb{C}$, $\mathbb{R}(\alpha)$ is an algebraically closed field. Moreover $L(\alpha)$ is algebraic over $\mathbb{R}(\alpha)$. By Exercice 4.4.7, $L(\alpha) = \mathbb{R}(\alpha)$.

Comme

$$2 = [\mathbb{R}(\alpha) : \mathbb{R}] = [L(\alpha) : \mathbb{R}] = [L(\alpha) : L] \times [L : \mathbb{R}], \tag{2}$$

$[L : \mathbb{R}]$ divides 2, thus $[L : \mathbb{R}] = 1$ or 2.

Conclusion : Every algebraic extension of $\mathbb{R}$ is finite of degree at most 2.

By (**??**),

$$\begin{aligned}[L : \mathbb{R}] = 2 &\iff [L(\alpha) : L] = 1 \\ &\iff L(\alpha) = L \\ &\Rightarrow \mathbb{C} \simeq L\end{aligned}$$

Reciprocally, if $\mathbb{C} \simeq L$, then $L(\alpha) \simeq L$. Let $\varphi : L(\alpha) \to L$ an isomorphism. Then $\beta = \varphi(\alpha) \in L$ satisfies $\beta^2 + 1 = 0$, thus $\beta \notin \mathbb{R}$. Consequently $\mathbb{R} \subsetneq L$, $1 < [L : \mathbb{R}] \le 2$, thus $[L : \mathbb{R}] = 2$.

$$[L : \mathbb{R}] = 2 \iff L \simeq \mathbb{C}.$$

□

Ex. 4.4.9 *Prove that $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}$.*

Proof. • If $\alpha \in \mathbb{Z}$, α is a root of the monic polynomial $x - \alpha \in \mathbb{Z}[x]$, thus α is an algebraic integer.

• Reciprocally, let $\alpha \in \mathbb{Q}$ an algebraic integer.

$$\alpha = p/q, \qquad (p, q) \in \mathbb{Z} \times \mathbb{N}^*,\ p \wedge q = 1.$$

α is a root of $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the coefficients a_i are integers. Thus

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_0 = 0,$$

that is

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_0q^n = 0.$$

This implies $q \mid p^n$, where $q \wedge p = 1$, thus $q \wedge p^n = 1$. Hence $q \mid 1$, where $q > 0$, thus $q = 1$, and $\alpha = p/q = p \in \mathbb{Z}$.

Conclusion : if $\alpha \in \mathbb{Q}$, α is an algebraic integer iff $\alpha \in \mathbb{Z}$.

$$\overline{\mathbb{Q}} \cap \mathbb{Q} = \mathbb{Z}.$$

□