

## EXERCISES GALOIS THEORY AND SOME SOLUTIONS

CARSTEN DIETZEL, SILVIA PROPERZI

### 1. WEEK 1

**Exercise 1.1.** Let  $\sigma : K \rightarrow L$  be a field homomorphism, prove that  $\sigma$  is injective.

*Solution.* [using ring theory] We know that  $\ker \sigma$  is an ideal of  $K$ . But  $K$  is a field so the only possibilities are that  $\ker \sigma = \{0\}$  or  $\ker \sigma = K$ . As  $\sigma(1) = 1 \neq 0$ , we know that  $1 \notin \ker \sigma$ , hence  $\ker \sigma = \{0\}$  which means that  $\sigma$  is injective. ■

*Solution.* [by hands] Let  $a, b \in K$  such that  $\sigma(a) = \sigma(b)$ . Then

$$\sigma(a - b) = \sigma(a) - \sigma(b) = 0.$$

If we assume that  $a \neq b$ , then  $a - b$  is a non-zero element in a field, hence it is invertible. Then

$$1 = \sigma(1) = \sigma((a - b)(a - b)^{-1}) = \sigma(a - b)\sigma((a - b)^{-1}) = 0,$$

which is a contradiction. Therefore  $a = b$  and so  $\sigma$  is injective. ■

**Exercise 1.2.** Let  $K$  be a field,  $K_0$  be its prime field and  $\sigma : K \rightarrow K$  be a field homomorphism. Prove that  $\sigma \in \text{Hom}(K/K_0, K/K_0)$ .

**Exercise 1.3.** Let  $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ ,  $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$  and  $\mathbb{Q}(i) = \{\frac{a+ib}{c+di} \mid a, b, c, d \in \mathbb{Q}\}$ ,  $\mathbb{Q}(\sqrt{2}) = \{\frac{a+\sqrt{2}b}{c+\sqrt{2}d} \mid a, b, c, d \in \mathbb{Q}\}$ .

- (i) Prove that  $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$  and  $\mathbb{Q}(i) = \mathbb{Q}[i]$ .
- (ii) Prove that  $\mathbb{Q}(i)$  and  $\mathbb{Q}(\sqrt{2})$  are not isomorphic.

**Exercise 1.4.**

- (i) Let  $a = \sqrt{2}$  and  $b = \sqrt[3]{3}$ . Prove that  $ab$  is algebraic over  $\mathbb{Q}$ .
- (ii) Show that  $\sqrt{2} + i$  is algebraic over  $\mathbb{Q}$  by finding a nonzero polynomial  $f \in \mathbb{Q}[X]$  with  $\deg(f) = 4$  such that  $f(\sqrt{2} + i) = 0$ . What are the other roots of  $f$ ?

*Solution.*

- (i) Observe that  $ab^6 = \sqrt{2} \sqrt[3]{3^6} = 8 \cdot 9 = 72$ . Therefore  $ab$  is a root of the polynomial  $X^6 - 72 \in \mathbb{Q}[X]$ .
- (ii) let  $\alpha = \sqrt{2} + i$ . Then  $\alpha^2 = 2 + 2\sqrt{2}i - 1 = 1 + 2\sqrt{2}i$  and  $\alpha^2 - 1 = 2\sqrt{2}i$ . Squaring both sides of the last equality we have that

$$\alpha^4 - 2\alpha^2 + 1 = (\alpha^2 - 1)^2 = (2\sqrt{2}i)^2 = -8.$$

Therefore the polynomial

$$f(X) = X^4 - 2X^2 + 1 + 8 = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$$

is such that  $f(\alpha) = 0$ .

Looking for other roots of  $f$  means to find all  $x \in C$  such that  $f(x) = 0$ , i.e.  $x^4 - 2x^2 + 9 = 0$ . Going back to how we construct  $f$ , this equation can also be written as  $(x^2 - 1)^2 = (2\sqrt{2}i)^2$ . Therefore  $x^2 - 1 = 2\sqrt{2}i$  or  $x^2 - 1 = -2\sqrt{2}i$ . So

$$x^2 = 2\sqrt{2}i + 1 = \alpha^2 \quad \text{or} \quad x^2 = -2\sqrt{2}i + 1 = \overline{\alpha^2} = \overline{\alpha}^2,$$

where  $\bar{\alpha}$  indicates the complex conjugate of  $\alpha$ . Thus  $x = \pm\alpha$  or  $x = \pm\bar{\alpha}$  and the 4 roots of  $f$  are

$$\begin{aligned}x_1 &= \alpha = \sqrt{2} + i, x_2 = -\alpha = -\sqrt{2} - i, \\x_3 &= \bar{\alpha} = \sqrt{2} - i, x_4 = -\bar{\alpha} = -\sqrt{2} + i.\end{aligned}$$

■

**Exercise 1.5.** Let  $p$  be a prime number. Denote by  $\binom{n}{k}$  the binomial coefficient “ $n$  over  $k$ ”.

- (i) Prove that  $p$  divides  $\binom{p}{k}$  for  $1 \leq k \leq p-1$ .
- (ii) Let  $K$  be a field of characteristic  $p$ . Show that the map  $\Phi : K \rightarrow K; x \mapsto x^p$  is a field endomorphism. This map is called the *Frobenius endomorphism* of  $K$ .

**Exercise 1.6.** Let  $L/K$  be a field extension and let  $M$  be a subring of  $L$  that contains  $K$ . Suppose that  $\dim_K M < \infty$ .

- (i) Prove that for any  $\alpha \in M$ , there is a nonzero  $f \in K[X]$  with  $f(\alpha) = 0$ .  
*Hint:* The elements  $\alpha^n$  ( $n \geq 0$ ) are linearly dependent.
- (ii) Prove that  $M$  is a field.  
*Hint:* For any  $0 \neq \alpha \in K$ , let  $f \in \mathbb{Q}[X]$  be a nonzero polynomial with  $f(\alpha) = 0$  whose degree is as small as possible. If  $f = \sum_{i=0}^{\infty} a_i X^i$ , prove that  $a_0 \neq 0$  and use this to construct an inverse of  $\alpha$  that lies in  $M$ .

**Exercise 1.7.** Let  $K$  be field.

- (i) Prove that  $K[X]$  is a PID.
- (ii) Let  $I \neq \{0\}$  be an ideal of  $K[X]$ , then there exists a unique monic polynomial that generates  $I$  as an ideal.

## 2. WEEK 2

**Exercise 2.1.** Let  $L/K$  be a field extension and let  $\alpha, \beta \in L$  such that

$$[K(\alpha) : K] = [K(\beta) : K] = 2.$$

Assume that the characteristic of  $K$  is not 2.

- (i) Prove that there is an  $\alpha' \in L$  such that  $K(\alpha') = K(\alpha)$  and  $\alpha'^2 \in K$ .
- (ii) Assume that  $\alpha, \beta \in L$  satisfy  $\alpha^2, \beta^2 \in K$ . Prove that  $K(\alpha) = K(\beta)$  if and only if  $\frac{\alpha^2}{\beta^2}$  is a square in  $K$ .
- (iii) Prove that there is a bijective map

$$K^\times / (K^\times)^2 \longrightarrow \{L \mid L/K \text{ is a field extension with } [L : K] \leq 2\}.$$

*Solution.*

- (i) Since  $[K(\alpha) : K] = 2$ ,  $\alpha \notin K$  and the 3 elements  $1, \alpha, \alpha^2$  are linearly dependent over  $K$ . Thus there exist  $a_0, a_1, a_2 \in K$  not all zero such that

$$a_0 + a_1\alpha + a_2\alpha^2 = 0.$$

If  $a_2 = 0$ , then  $a_0 + a_1\alpha = 0$ , hence either  $a_1 = 0$  or  $\alpha = -a_0/a_1$ . If  $a_1 = 0$ , then also  $a_0 = 0$ . But this is not possible because  $(a_0, a_1, a_2) \neq (0, 0, 0)$ . On the other hand, if  $\alpha = -a_0/a_1$ , then  $\alpha \in K$ , a contradiction.

So we have that  $a_2 \neq 0$  and we can divide by  $a_2$ , obtaining

$$b + a\alpha + \alpha^2 = 0, \text{ i.e. } \alpha^2 + a\alpha = -b,$$

where  $a = a_2^{-1}a_1 \in K$  and  $b = a_2^{-1}a_0 \in K$ . Since we assumed that  $K$  has not characteristic two, we can also complete the square:

$$(\alpha + a/2)^2 = \alpha^2 + a\alpha + a^2/4 = -b + a^2/4 \in K.$$

Therefore  $\alpha' = \alpha + a/2$  is such that  $\alpha'^2 = -b + a^2/4 \in K$ . Moreover  $\alpha' = \alpha + a/2 \in K(\alpha)$ , so  $K(\alpha') \subseteq K(\alpha)$  and  $\alpha = \alpha' - a/2 \in K(\alpha')$  so  $K(\alpha) \subseteq K(\alpha')$ . Therefore  $K(\alpha) = K(\alpha')$  and  $\alpha'^2 \in K$ .

- (ii) Assume that  $\frac{\alpha^2}{\beta^2}$  is a square in  $K$ , i.e. there is a  $k \in K$  such that  $\frac{\alpha^2}{\beta^2} = k^2$ . (Note that  $k \neq 0$  otherwise  $\alpha = 0 \in K$  and  $[K(\alpha) : K] = [K : K] = 1$ .)

Then  $\alpha = k^2\beta^2$ , hence  $\alpha = \pm k\beta \in K(\beta)$ . So  $K(\alpha) \subseteq K(\beta)$ . On the other hand,  $\beta^2 = \frac{\alpha^2}{k^2}$ , hence  $\beta = \pm \frac{\alpha}{k} \in K(\alpha)$ . So  $K(\beta) \subseteq K(\alpha)$ . Having proved both inclusions we deduce that  $K(\alpha) = K(\beta)$ .

Vice versa, assume that  $K(\alpha) = K(\beta)$ . Knowing that  $[K(\alpha) : K] = 2$ , we have that  $\{1, \alpha\}$  is a generating set of the  $K$ -vector space  $K(\alpha) = K(\beta)$ . Therefore there exist  $a, b \in K$  such that  $\beta = a + b\alpha$ . Squaring both sides of the equality, we get  $\beta^2 = a^2 + 2ab\alpha + \alpha^2$ . So  $2ab\alpha = \beta^2 - a^2 - \alpha^2$  is a sum of elements in  $K$ . Hence  $2ab\alpha \in K$ , but  $\alpha \notin K$ . Therefore the only possibility is that  $2ab = 0$ , i.e. (since we are not in characteristic 2)  $ab = 0$ . But  $b \neq 0$ , otherwise  $\beta = a \in K$ , which is not possible (otherwise and  $[K(\beta) : K] = [K : K] = 1$ ). Thus  $a = 0$ , i.e.  $\beta = b\alpha$  and so  $\frac{\beta^2}{\alpha^2} = a^2$  is a square in  $K$ .

- (iii) Let  $L/K$  be a field extension with  $[L : K] = 2$ . Take  $\alpha \in L \setminus K$ , then

$$1 < [K(\alpha) : K] \leq [L : K] = 2.$$

Hence  $L = K(\alpha)$ . Moreover, the first part of this exercise allows us to choose  $\alpha$  such that  $\alpha^2 \in K$ . Now we can define the following map

$$\psi : \{L \mid L/K \text{ is a field extension with } [L : K] \leq 2\} \rightarrow K^\times / (K^\times)^2$$

as  $\psi(K) = [1]$  and for  $[L : K] = 2$  as  $\psi(L) = [\alpha^2] \in K^\times / (K^\times)^2$ , for  $\alpha \in L \setminus K$  (so  $L = K(\alpha)$ ) such that  $\alpha^2 \in K$ .

This map is well-defined: take  $L/K$  of degree 2 and  $\alpha, \beta \in L \setminus K$  such that  $\alpha^2 \in K$ . Then, by the remark made at the beginning,  $L = K(\alpha) = K(\beta)$ . As shown in the second part of this exercise, this is equivalent to  $\frac{\alpha^2}{\beta^2} \in (K^\times)^2$ , so  $[\alpha^2] = [\beta^2] \in K^\times / (K^\times)^2$ . (Note also that  $[\alpha^2] = [1]$  if and only if  $\alpha^2 = k^2 \in K^2$ , so  $\alpha = \pm k \in K$  and  $K(\alpha) = L$ .)

Let now prove that  $\psi$  is injective. Assume that we have two extensions  $L/K$  and  $L'/K$  of degree  $\leq 2$ , such that  $[\alpha^2] = \psi(L) = \psi(L') = [\beta^2]$ .

If  $[\beta^2] = [\alpha^2] = [1]$ , then  $L = K(\alpha) = K = K(\beta) = L'$ .

Otherwise,  $\beta^2/\alpha^2 \in (K^\times)^2$ , so, by the previous part of this exercise,  $L = K(\alpha) = K(\beta) = L'$ .

Finally, for the surjectivity, let  $x \in K^\times$ . If  $x \in (K^\times)^2$ , then  $x = \alpha^2$  for some  $\alpha \in K^\times$  and so  $L = K(\alpha)$  is an extension of  $K$  of degree  $\leq 2$  and  $\psi(L) = [x]$ .

If  $x \notin (K^\times)^2$ , then we can find an extension  $L = K(\alpha)$  such that  $\alpha^2 = x \in K^\times$  and so  $\psi(L) = [x] \in K^\times / (K^\times)^2$ . To construct this extension consider the polynomial  $f(X) = X^2 - x \in K[X]$ . It has to be irreducible, otherwise  $X^2 - x = (aX + b)(cX + d) = acX^2 + (ad + bc)X + bd$ , for some  $a, c \in K^\times$  and  $b, d \in K$ . So  $1 = ac$ ,  $0 = ad + bc$  and  $-x = bd$ , i.e.  $c = a^{-1}$ ,  $d = -a^{-1}bc = bc^2$  and  $-x = bd = b^2c^2 \in (K^\times)^2$ , a contradiction to the assumption  $x \notin (K^\times)^2$ . Then we can consider the field  $L = K[X]/(X^2 - x)$  that contains  $K$  (it is a field because the ideal  $(X^2 - x)$  is maximal, since it is generated by an irreducible polynomial). Defining  $\alpha$  as the class of  $X$  in  $L$  we get that  $L = K(\alpha)$  and  $\alpha^2 = x \in K$ . ■

**Exercise 2.2.** Let  $E/K$  be a field extension and  $a$  and  $b$  be algebraic over  $K$ .

- (1) Assume that  $[K(a) : K] = m$ ,  $[K(b) : K] = n$ . Prove that  $K[a, b] \subseteq E$  is generated, as a vector space over  $K$ , by the elements  $a^i b^j$  ( $1 \leq i \leq m$ ,  $1 \leq j \leq n$ ).
- (2) Prove that  $a + b$  and  $ab$  are algebraic over  $K$ . Can you estimate the quantities  $[K(a + b) : K]$  and  $[K(ab) : K]$ ?
- (3) Find a polynomial  $f \in \mathbb{Q}[X]$  such that  $\deg(f) \leq 6$  and  $f(\sqrt[3]{3} + \sqrt{5}) = 0$ .

The following lemma can be used, without proof, in the following exercise.

**Lemma** (Gauss' Lemma). *Let  $A$  be a unique factorization domain and  $K$  be its fraction field. A non-constant polynomial  $f \in A[X]$  is irreducible if and only if it is primitive and is irreducible in  $K[X]$ .*

**Exercise 2.3** (Eisenstein's irreducibility criterion). Let  $A$  be a unique factorization domain and  $K$  be its fraction field. Let  $f = \sum_{i=0}^n a_i X^i \in K[X]$  be a polynomial of degree  $n > 0$ . Assume that there exists a prime element  $p \in A$  such that  $p \mid a_i$  for all  $i \in \{0, 1, \dots, n-1\}$ ,  $p \nmid a_n$  and  $p^2 \nmid a_0$ . Then  $f$  is irreducible in  $K[X]$ .

**Exercise 2.4.** Let  $\zeta \in \mathbb{C}$  be a primitive cubic root of one. Set  $E = \mathbb{Q}[\sqrt[3]{2}]$ ,  $F = \mathbb{Q}(\zeta)$  and  $L = \mathbb{Q}[i]$ .

- (i) Prove that  $[E : \mathbb{Q}] = 3$  and  $[F : \mathbb{Q}] = 2$  and compute the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$  and over  $L$ .
- (ii) Prove that  $EF = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ .
- (iii) Compute  $[EF : \mathbb{Q}]$  and  $[E \cap F : \mathbb{Q}]$ .

**Exercise 2.5.** Let  $E/K$  be a field extension and let  $L/K$  and  $M/K$  be subextensions.

- (i) Prove that  $[LM : K] \cdot [L \cap M : K] \leq [L : K] \cdot [M : K]$ .

- (ii) Can you find examples where  $[LM : K] \cdot [L \cap M : K] < [L : K] \cdot [M : K]$ ?

*Hint:* Use two different roots of the polynomial  $X^3 - 2$ .

**Exercise 2.6.** Let  $E/K$  be a field extension and let  $f \in K[X]$  be a polynomial such that  $f$  factorizes in  $E[X]$  as  $f = \prod_{i=1}^n (x - \alpha_i)$ . Prove by induction that  $[K(\alpha_1, \alpha_2, \dots, \alpha_n) : K] \leq n!$ .

## 3. WEEK 3

**Exercise 3.1.** For every polynomial  $p(X) = \sum_{i=0}^n a_i X^i \in K[X]$  of degree  $n$ , define its *reciprocal polynomial* as

$$\widehat{p}(X) = \sum_{i=0}^n a_{n-i} X^i.$$

Let  $p(X), q(X) \in K[X]$  be polynomials of degree  $n$  and  $m$  respectively such that  $p(0) \neq 0$  and  $q(0) \neq 0$ . Prove that

- (i)  $\widehat{p}(X) = X^n p(1/X)$  in  $K(X)$ ,
- (ii)  $\widehat{\widehat{p}}(X) = p(X)$ ,
- (iii)  $\widehat{pq}(X) = \widehat{p}(X)\widehat{q}(X)$ ,
- (iv)  $\widehat{p}(X)$  is irreducible if and only if  $p(X)$  is irreducible.

*Solution.* Suppose that  $p(X) = \sum_{i=0}^n a_i X^i$  has degree  $n$  and  $q(X) = \sum_{i=0}^m b_i X^i$  has degree  $m$ .

- (i)  $X^n p(1/X) = X^n \sum_{i=0}^n a_i (1/X)^i = \sum_{i=0}^n a_i X^{n-i} = \sum_{j=0}^n a_{n-j} X^j = \widehat{p}(X)$
- (ii) Since  $p(0) \neq 0$ ,  $a_0 \neq 0$ , therefore  $\deg(\widehat{p}) = \deg(p) = n$ . Hence, using the previous part of this exercise,

$$\widehat{\widehat{p}}(X) = X^n \widehat{p}(1/X) = X^n (1/X)^n p(1/(1/X)) = p(X).$$

- (iii) Since  $p(0) \neq 0$  and  $q(0) \neq 0$  we deduce that also  $pq(0) \neq 0$ . Hence we can apply the previous results for  $p, q$  and  $pq$ . So, using also that  $pq(1/X) = p(1/X)q(1/X)$  and that  $\deg pq = n + m$ , we have that

$$\widehat{pq}(X) = X^{n+m} pq(1/X) = X^n p(1/X) X^m q(1/X) = \widehat{p}(X)\widehat{q}(X).$$

- (iv) Suppose  $\widehat{p}(X)$  is irreducible and let  $p = q_1 q_2$  for  $q_1(X), q_2(X) \in K[X]$ . Note that  $0 \neq p(0) = q_1(0)q_2(0)$  implies that both  $q_1(0) \neq 0$  and  $q_2(0) \neq 0$ . Considering now the reciprocal polynomials and using the previous properties,  $\widehat{p}(X) = \widehat{q_1}(X)\widehat{q_2}(X)$ . Since  $\widehat{p}(X)$  is irreducible, there is  $i \in \{1, 2\}$  such that  $\widehat{q_i}$  is a constant, i.e.  $\deg q_i = \deg \widehat{q_i} = 0$ . Thus,  $q_i$  is a constant too, and therefore  $p(X)$  is irreducible.

Vice versa, assume that  $p(X)$  is irreducible. Since we know that  $p(X) = \widehat{\widehat{p}}$ , by the property just proved, we obtain that  $\widehat{p}$  is also irreducible. ■

**Exercise 3.2.** Let  $E/K$  be a field extension and  $x \in E$  be an algebraic element and let  $f = f(x, K)$  is the minimal polynomial of  $x$  over  $K$  of degree  $\deg(f) = n$ .

- (i) Prove that  $[K(x) : K] = n$ .
- (ii) Prove that  $\frac{1}{f(0)}\widehat{f}$  is the minimal polynomial of  $1/x$  over  $K$ .
- (iii) Write  $f(X) = \sum_{i=0}^n a_i X^i = p(X^2) + Xd(X^2)$ , where

$$p(X) = \sum_{j=0}^{\lfloor n/2 \rfloor} a_{2j} X^j \text{ and } d(X) = \sum_{j=0}^{\lfloor n/2 \rfloor} a_{2j+1} X^j.$$

Let  $g(X) = p(X)^2 - Xd(X)^2$  and prove that

- if  $d(x^2) = 0$ , then the minimal polynomial of  $x^2$  over  $K$  is  $p(X)$ ,
- if  $d(x^2) \neq 0$ , then the minimal polynomial of  $x^2$  over  $K$  is  $(-1)^n g(X)$ .

*Solution.*

- (i) We will prove that  $B = \{1, x, \dots, x^{n-1}\}$  is a basis of  $K(x)$  as a  $K$  vector space which implies that  $[K(x) : K] = \dim_K(K(x)) = |B| = n$ .

- $B$  is a generating set for  $K(x)$  as a  $K$  vector space.

To prove this recall that  $K(x) = K[x]$ , since  $x$  is algebraic over  $K$ .

(Similar proof to 1)  $\Rightarrow$  2) of Theorem 2.7 of the lecture notes.)

Let  $z \in K(x) = K[x]$ , say  $z = h(x)$  for some  $h \in K[X]$ . Divide  $h$  by  $f$  to obtain polynomials  $q, r \in K[X]$  such that  $h = fq + r$ , where  $r = 0$  or  $\deg r < \deg f = n$ . This implies that

$$z = h(x) = f(x)q(x) + r(x) = r(x).$$

Moreover we can write  $r = \sum_{i=0}^{n-1} c_i X^i$  for some  $c_0, \dots, c_{n-1} \in K$ . Thus  $z = \sum_{i=0}^{n-1} c_i x^i \in \langle 1, x, \dots, x^{n-1} \rangle$  and hence  $K[x]$  is generated by  $\{1, x, \dots, x^{n-1}\}$  as a  $K$ -vector space.

- $B$  is linearly independent over  $K$ .

If  $B$  is linearly dependent over  $K$  then there exists a linear combination

$0 = \sum_{i=0}^{n-1} c_i x^i$  over  $K$ , with not all  $c_i$  equal to 0. Then the polynomial  $h(X) = \sum_{i=0}^{n-1} c_i X^i$  is in  $K[X] \setminus \{0\}$  and has  $x$  as a root. So

$$n - 1 = \deg(h) \leq \deg(f) = n,$$

a contradiction.

- (ii) First of all we note that  $f(0) \neq 0$ . Otherwise we can write  $f(X) = Xg(X)$  for some  $g(X) \in K[X]$ , but  $f$  is monic and irreducible in  $K[X]$ , hence  $g(X) = 1$  and  $f(X) = X$ . Evaluating  $f$  in  $x$  we obtain  $0 = f(x) = x$ , a contradiction with the hypothesis  $x \neq 0$ .

Since  $f(0) \neq 0$ , we can use the previous exercise and obtain that  $\hat{f}$  is also irreducible and  $\hat{f} = X^n f(1/X)$ . Hence

$$\frac{1}{f(0)} \hat{f}(1/x) = \frac{1}{f(0)} (1/x)^n f\left(\frac{1}{1/x}\right) = \frac{1}{f(0)x^n} f(x) = 0.$$

So we have that  $\frac{1}{f(0)} \hat{f}$  is an irreducible polynomial in  $K[x]$  with  $1/x$  as a root. To prove that  $\frac{1}{f(0)} \hat{f}$  is the minimal polynomial of  $1/x$  over  $K$  it remains to prove that it is monic. Looking at the definition of  $\hat{f}$  we see that its leading coefficient is the constant term of  $f$ , i.e.  $f(0)$ . Therefore the leading coefficient of  $\frac{1}{f(0)} \hat{f}$  is  $\frac{1}{f(0)} f(0) = 1$ , hence  $\frac{1}{f(0)} \hat{f}$  is monic.

- (iii) First of all note that

$$0 = f(x) = p(x^2) + xd(x^2), \quad (1)$$

therefore

$$g(x^2) = p(x^2)^2 - x^2 d(x^2)^2 = (p(x^2) + xd(x^2))(p(x^2) - xd(x^2)) = 0.$$

So  $x^2$  is a root of  $g$  and the degree of  $g$  is

$$\begin{cases} 2 \deg(p) & \text{if } n \text{ is even} \\ 1 + 2 \deg(d) & \text{if } n \text{ is odd} \end{cases} = \begin{cases} 2 \lfloor \frac{n}{2} \rfloor & \text{if } n \text{ is even} \\ 1 + 2 \lfloor \frac{n}{2} \rfloor & \text{if } n \text{ is odd} \end{cases} = n.$$

Moreover, by the first point of this exercise and the fact that the degree is multiplicative

$$n = \deg(f) = [K(x) : K] = [K(x) : K(x^2)][K(x^2) : K].$$

Hence, to compute  $[K(x^2) : K]$  (which is also the degree of  $f(x^2, K)$ , the minimal polynomial of  $x^2$  over  $K$ ), we need to know  $[K(x) : K(x^2)]$ . Observe that  $X^2 - x^2$  is a polynomial in  $K(x^2)[X]$  which has  $x$  as a root. Thus

$$[K(x^2) : K] = \deg(x, K(x^2)) \leq \deg(X^2 - x^2) = 2$$

Therefore

$$[K(x^2) : K] = \frac{[K(x) : K]}{[K(x) : K(x^2)]} \in \left\{n, \frac{n}{2}\right\}. \quad (2)$$

- If  $d(x^2) = 0$ , by Equation (1), also  $p(x^2) = 0$  and  $\deg(p) = \lfloor \frac{n}{2} \rfloor < n$ . So

$$[K(x^2) : K] = \deg(f(x^2, K)) \leq \deg(p) < n,$$

thus, by (2),  $[K(x^2) : K] = \frac{n}{2}$ , which implies that  $n$  has to be even,  $p(X)$  monic and

$$[K(x^2) : K] = \frac{n}{2} = \left\lfloor \frac{n}{2} \right\rfloor = \deg(p).$$

Therefore  $p(X)$  is a monic polynomial in  $K[X]$  which as  $x^2$  as a root and of degree  $[K(x^2) : K] = \deg(f(x^2, K))$ , hence it is  $\deg(f(x^2, K))$ , the minimal polynomial of  $x^2$  over  $K$ .

- If  $d(x^2) \neq 0$ , then, by Equation (1),

$$x = -\frac{p(x^2)}{d(x^2)} \in K(x^2).$$

Therefore  $K(x) \subseteq K(x^2) \subseteq K(x)$  and so  $K(x^2) = K(x)$ , which means  $[K(x) : K(x^2)] = 1$  and, by (2),

$$[K(x^2) : K] = \frac{[K(x) : K]}{[K(x) : K(x^2)]} = [K(x) : K] = n = \deg(g).$$

Moreover the leading coefficient of  $g(X)$  is

$$\begin{cases} a_n & \text{if } n \text{ is even} \\ -a_n & \text{if } n \text{ is odd} \end{cases} = (-1)^n a_n = (-1)^n.$$

Therefore we have the monic polynomial  $(-1)^n g(X) \in K[X]$  that vanishes in  $x^2$ , of degree  $n = [K(x^2) : K] = \deg(f(x^2, K))$ . Hence  $(-1)^n g(X) = f(x^2, K)$ . ■

The following lemma can be used, without proof, in the following exercise.

**Lemma** (Gauss' Lemma). *Let  $A$  be a unique factorization domain and  $K$  be its fraction field. A non-constant polynomial  $f \in A[X]$  is irreducible if and only if it is primitive and irreducible in  $K[X]$ .*

**Exercise 3.3** (Eisenstein's irreducibility criterion). Let  $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$  be a polynomial of degree  $n > 0$ . Assume that there exists a prime  $p$  such that  $p \mid a_i$  for all  $i \in \{0, 1, \dots, n-1\}$ ,  $p \nmid a_n$  and  $p^2 \nmid a_0$ . Then  $f$  is irreducible in  $\mathbb{Q}[X]$ .

*More general version*

Let  $A$  be a unique factorization domain and  $K$  be its fraction field. Let  $f = \sum_{i=0}^n a_i X^i \in A[X]$  be a polynomial of degree  $n > 0$ . Assume that there exists a prime element  $p \in A$  such that  $p \mid a_i$  for all  $i \in \{0, 1, \dots, n-1\}$ ,  $p \nmid a_n$  and  $p^2 \nmid a_0$ . Then  $f$  is irreducible in  $K[X]$ .

**Exercise 3.4.** Let  $\zeta \in \mathbb{C}$  be a primitive cubic root of one. Set  $E = \mathbb{Q}[\sqrt[3]{2}]$ ,  $F = \mathbb{Q}(\zeta)$  and  $L = \mathbb{Q}[i]$ .

- Prove that  $[E : \mathbb{Q}] = 3$  and  $[F : \mathbb{Q}] = 2$  and compute the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$  and over  $L$ .
- Prove that  $EF = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ .
- Compute  $[EF : \mathbb{Q}]$  and  $[E \cap F : \mathbb{Q}]$ .



**Exercise 3.5.** Let  $E/K$  be a field extension and let  $L/K$  and  $M/K$  be subextensions.

- (i) Prove that  $[LM : K] \cdot [L \cap M : K] \leq [L : K] \cdot [M : K]$ .
- (ii) Can you find examples where  $[LM : K] \cdot [L \cap M : K] < [L : K] \cdot [M : K]$ ?  
*Hint:* Use two different roots of the polynomial  $X^3 - 2$ .

**Exercise 3.6.** Let  $E/K$  be a field extension and let  $f \in K[X]$  be a polynomial such that  $f$  factorizes in  $E[X]$  as  $f = \prod_{i=1}^n (x - \alpha_i)$ . Prove by induction that  $[K(\alpha_1, \alpha_2, \dots, \alpha_n) : K] \leq n!$ .

## 4. WEEK 4

**Exercise 4.1.** Let  $K$  be a field. For a polynomial  $f = \sum_{k=0}^n a_k X^k \in K[X]$ , we define the *derivative* by

$$f' = \sum_{k=1}^n k a_k X^{k-1}.$$

- (i) Let  $\alpha \in K$  and  $f, g \in K[X]$ . Prove the following properties of the derivative
  - (a)  $(f + g)' = f' + g'$ ,
  - (b)  $(\alpha \cdot f)' = \alpha \cdot f'$ ,
  - (c)  $(f \cdot g)' = f' \cdot g + f \cdot g'$ .
- (ii) Let  $f \in K[X]$  be a polynomial that factorizes as  $f = \prod_{i=1}^n (X - \alpha_i)$ . Prove that the roots  $\alpha_1, \dots, \alpha_n$  are pairwise different if and only if  $\gcd(f, f') = 1$ .
- (iii) Let  $C$  be an algebraic closure of  $K$  and let  $f \in K[X]$  be a polynomial with  $\deg(f) \geq 1$  that is irreducible over  $K$ . Prove that  $f$  has repeated roots in  $C$  if and only if  $f' = 0$ . In particular, show that having such a polynomial  $f$  implies that  $\text{char}(K) = p > 0$  and  $f(X) = g(X^p)$  for some irreducible polynomial  $g \in K[X]$ .

*Solution.*

- (i) For sake of simplicity, write  $f = \sum_{k=0}^{\infty} a_k X^k$  and  $g = \sum_{k=0}^{\infty} b_k X^k$ . Then

$$\begin{aligned} (f + g)' &= \left( \sum_{k=0}^{\infty} (a_k + b_k) X^k \right)' = \sum_{k=1}^{\infty} k(a_k + b_k) X^{k-1} \\ &= \sum_{k=1}^{\infty} k a_k X^{k-1} + \sum_{k=1}^{\infty} k b_k X^{k-1} = f' + g'. \end{aligned}$$

Hence we have proved (a). We can now prove also (b) as:

$$(\alpha \cdot f)' = \left( \sum_{k=0}^{\infty} \alpha a_k X^k \right)' = \sum_{k=1}^{\infty} k \alpha a_k X^{k-1} = \alpha \cdot \sum_{k=1}^{\infty} k a_k X^{k-1} = \alpha \cdot f'.$$

To prove (c), we first check the equality for  $f = X^k$  and  $g = X^l$ :

$$(f \cdot g)' = (X^{k+l})' = (k+l)X^{k+l-1} = kX^{k-1}X^l + X^k lX^{l-1} = f' \cdot g + f \cdot g'.$$

Using the already-established  $K$ -linearity (i.e. (a) and (b) of this exercise), we can now calculate

$$\begin{aligned} (f \cdot g)' &= \left( \sum_{k,l \geq 0} a_k b_l X^{k+l} \right)' = \sum_{k,l \geq 0} a_k b_l (X^{k+l})' \\ &= \sum_{k,l \geq 0} a_k b_l ((X^k)' X^l + X^k (X^l)') \\ &= \sum_{k,l \geq 0} a_k b_l (X^k)' X^l + \sum_{k,l \geq 0} a_k b_l X^k (X^l)' \\ &= \left( \sum_{k=0}^{\infty} a_k X^k \right)' \cdot \left( \sum_{l=0}^{\infty} b_l X^l \right) + \left( \sum_{k=0}^{\infty} a_k (X^k)' \right) \cdot \left( \sum_{l=0}^{\infty} b_l X^l \right) \\ &= f' \cdot g + f \cdot g'. \end{aligned}$$

- (ii) Let  $\alpha_i$  be one of the roots of  $f$ . Write  $f = (X - \alpha_i) \cdot g$ . By the (i) of this exercise,

$$f' = (X - \alpha_i)' \cdot g + (X - \alpha_i) \cdot g' = g + (X - \alpha_i) \cdot g'.$$

Therefore,  $f'(\alpha_i) = g(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$ . This implies that  $f'(\alpha_i) = 0$  if and only if  $\alpha_i$  is a repeated root of  $f$  which is the case if and only if  $(X - \alpha_i)$  is a common divisor of  $f$  and  $f'$ .

As the linear factors  $(X - \alpha_i)$  are prime elements of  $K[X]$ , it follows that  $f$  and  $f'$  have common divisors if and only if  $f$  has repeated roots.

- (iii) Let  $f$  be irreducible in  $K[X]$  with repeated roots in  $C[X]$ . By the previous exercise,  $\gcd(f, f') \neq 1$ . As  $f$  is irreducible and  $\gcd(f, f') \in K[X]$ , this implies  $\gcd(f, f') = f$ . Therefore,  $f$  divides  $f'$ . As  $\deg(f') < \deg(f)$ , this implies  $f' = 0$ .

In case that  $f' = 0$ , we write  $f = \sum_{k=0}^{\infty} a_k X^k$  and consider that

$$f' = \sum_{k=1}^{\infty} k a_k X^{k-1} = 0.$$

Therefore, for all  $k \geq 0$ , we have  $k = 0$  or  $a_k = 0$ . As there is at least one  $k \geq 1$  with  $a_k \neq 0$  we conclude that  $k = 0$  holds in  $K$  for some nonzero  $k$ . This implies that  $\text{char}(K) = p > 0$  and that  $a_k = 0$  whenever  $p \nmid k$ . We can therefore write

$$f = \sum_{l=0}^{\infty} a_{pl} X^{pl} = g(X^p)$$

with  $g = \sum_{l=0}^{\infty} a_{pl} X^l$ . For a decomposition  $g = g_1 g_2$ , we also get a decomposition  $f(X) = g(X^p) = g_1(X^p) g_2(X^p)$  which implies that either  $g_1(X^p)$  or  $g_2(X^p)$  is in  $K$ , which amounts to saying that  $g_1$  or  $g_2$  is in  $K$ . Therefore,  $g$  has to be irreducible. ■

**Exercise 4.2.** Let  $L$  be a finite field.

- (i) Show that  $L$  is not algebraically closed.  
*Hint:* Consider the polynomial  $f(X) = 1 + \prod_{l \in L} (X - l) \in L[X]$ .
- (ii) Show that  $L$  contains a subfield  $K$  isomorphic to  $\mathbb{Z}/p$  (its ring of integers) and that  $|L| = p^m$ , where  $m = [L : K]$ .

Assume now that  $K = \mathbb{Z}/p$  and let  $f(X) = X^{p^m} - X \in K[X]$ . Let  $C$  be an algebraic closure of  $K$  and set  $L = \{\alpha \in C \mid f(\alpha) = 0\}$ . Prove that

- (iii)  $|L| = p^m$   
*Hint:* Use the previous exercise.
- (iv) Recall that, since  $K$  has characteristic  $p$ ,  $\Phi : K \rightarrow K; x \mapsto x^p$  is a field endomorphism (the Frobenius endomorphism). Prove that  $L$  is a field and  $K \subseteq L \subseteq C$ .

*Solution.*

- (i) The polynomial  $f(X) \in L[X]$  doesn't have roots in  $L$ . In fact consider any  $a \in L$ , then

$$f(a) = 1 + \prod_{l \in L} (a - l) = 1 + (a - a) \prod_{l \in L \setminus \{a\}} (X - l) = 1 + 0 = 1 \neq 0.$$

- (ii) Let  $K$  be the ring of integers of  $L$ . Since  $L$  is finite,  $K$  is finite too. Hence  $K$  is isomorphic to  $\mathbb{Z}/p$  for some prime  $p$ .  $L$  is a vector space of dimension  $m$  over  $K \cong \mathbb{Z}_p$ . Let  $\{x_1, x_2, \dots, x_m\}$  is a basis of  $L$  over  $K$ , then every element of  $L$  can be written in a unique way as a linear combination  $\sum_{i=1}^m a_i x_i$ , with  $a_i \in K$ . So the number of elements of  $L$  is equal to the number of tuples  $(a_1, \dots, a_m) \in K^m$ . Hence  $|L| = |K|^m = p^m$ .

- (iii) If  $f = X^{p^m} - X$ , then  $f' = p^m X^{p^m-1} - 1 = -1$ . So,  $\gcd(f, f') = 1$  and, by the previous exercise, we can conclude that  $f$  has  $p^m$  pairwise different roots in  $C$ , i.e.  $|L| = p^m$ .
- (iv) Using the Frobenius endomorphism  $\Phi$  of  $K$ , we can see that

$$L = \{\alpha \in C \mid \alpha^{p^m} = \alpha\} = \{\alpha \in C \mid \Phi^m(\alpha) = \alpha\}.$$

Since  $\Phi$  is an endomorphism,  $\Phi^m$  is also an endomorphism. Then for all  $\alpha, \beta \in L$ ,

$$\Phi^m(\alpha + \beta) = \Phi^m(\alpha) + \Phi^m(\beta) = \alpha + \beta$$

$$\Phi^m(-\alpha) = -\Phi(\alpha) = -\alpha$$

$$\Phi^m(\alpha\beta) = \Phi^m(\alpha)\Phi^m(\beta) = \alpha\beta.$$

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

So  $\alpha + \beta, \alpha, \alpha\beta, \alpha^{-1} \in L$ , i.e.  $L$  is a field. ■

**Exercise 4.3.** Let  $C/K$  be an algebraic field extension. Show that the following are equivalent:

- (i)  $C$  is an algebraic closure of  $K$ .
- (ii) For every algebraic extension  $L/K$  there is an extension homomorphism  $\varphi \in \text{Hom}(L/K, C/K)$ .

*Hint:* For (i) $\Rightarrow$ (ii) use Proposition 3.6 in the notes.

**Exercise 4.4.** Let  $f \in K[X]$  be a polynomial of degree  $n$ . Let  $C$  be an algebraic closure of  $K$  and  $A = \{\alpha_1, \dots, \alpha_k\} \subseteq C$  be the distinct roots of  $f$  in  $C$ . We know that  $E = K(\alpha_1, \dots, \alpha_k)$  is the decomposition field of  $f$  over  $K$ .

- (i) Prove that  $[E : K] \leq n!$ .
- (ii) Prove that there is an injective homomorphism  $\text{Gal}(E/K) \longrightarrow \mathbb{S}_A \cong \mathbb{S}_k$   
*Hint:* Prove that  $\sigma(A) = A$  for every  $\sigma \in \text{Gal}(E/K)$ .
- (iii) For  $K = \mathbb{Z}/3$  and  $f = X^3 - X - 1$ , compute  $[E : K]$  and  $\text{Gal}(E/K)$ .  
(Observe that in this case  $[E : K] < n!$ .)

**Exercise 4.5.** Let  $f = X^4 - 5X^2 + 5 \in \mathbb{Q}[X]$  and  $E$  be a decomposition field of  $f$  over  $\mathbb{Q}$ . Prove that  $[E : \mathbb{Q}] = 4$ .

*Hint:* Given  $\alpha, \beta \in \mathbb{C}$  two solutions of  $f$  such that  $\beta \neq -\alpha$ , compute  $\alpha\beta$ . Prove also that  $E = \mathbb{Q}(\alpha)$ .

(Carsten Dietzel) DEPARTMENT OF MATHEMATICS AND DATA SCIENCE, VRIJE UNIVERSITEIT BRUSSEL, PLEINLAAN 2, 1050 BRUSSEL, BELGIUM  
*Email address:* **Carsten.Dietzel@vub.be**

(Silvia Properzi) DEPARTMENT OF MATHEMATICS AND DATA SCIENCE, VRIJE UNIVERSITEIT BRUSSEL, PLEINLAAN 2, 1050 BRUSSEL, BELGIUM  
*Email address:* **Silvia.Properzi@vub.be**