3 Field extensions

Keywords: Primitive polynomial, Gauss' lemma, reduction mod p, Eisenstein, field extension, degree, primitive extension, algebraic element, transcendental element, minimum polynomial, K-homomorphism, tower law.

3.1 Irreducibility criteria

In this section we shall learn a few methods for proving that a polynomial over a field is irreducible. Some irreducible polynomials can be shown to be irreducible by one or more of our criteria, some cannot.

Definition 40. Let A be a UFD. For example $A = \mathbb{Z}$. A polynomial in $A[X]$ is called **primitive** if the ideal generated by its coefficients is A.

Lemma 41: Gauss' lemma. Let A be a UFD and $K = \operatorname{Frac} A$.

(a) If $g, h \in A[X]$ are primitive then gh is primitive.

(b) Let $f \in A[X]$ be non-constant. If f is irreducible in $A[X]$ then it is irreducible in $K[X]$.

Proof. Proof of (a). Let $p \in A$ be an irreducible element and write $g = \sum_i g_i X^i$, $h = \sum_i h_i X^i$. Since g, h are primitive, there are $r, s \geq 0$ such that

$$\begin{aligned} p \mid g_0, g_1, \ldots, g_{r-1}, \qquad & p \nmid g_r, \\ p \mid h_0, h_1, \ldots, h_{s-1}, \qquad & p \nmid h_s. \end{aligned}$$

The coefficient of X^{r+s} in gh is

$$\sum_{k=0}^{r+s} g_k h_{r+s-k} = \Big(\sum_{k=0}^{r-1} g_k h_{r+s-k} \Big) + g_r h_s + \Big(\sum_{k=r+1}^{r+s} g_k h_{r+s-k} \Big). \tag{42}$$

Now all factors h_{r+s-k} in the last sum are in (p), and so are all factors g_k in the last sum but one. Also, (p) is a prime ideal not containing either of g_r, h_s, hence not containing the middle term $g_r h_s$. Therefore, the coefficient (42) is not in (p).

Thus no irreducible element of A divides all the coefficients of gh, so that gh is primitive.

Proof of (b). Let $g, h \in K[X]$ be such that $f = gh$. Then there are coprime elements $a, b \in A$ and primitive $g_1, h_1 \in A[X]$ such that g/g_1 and h/h_1 are constants in K, and $af = bg_1h_1$. Now g_1h_1 is primitive by (a) and clearly so is f. It immediately follows that both a, b are units in A; we may as well assume they are 1. Then $f = g_1h_1$. As f is irreducible in $A[X]$, one among g_1, h_1 is a unit in $A[X]$, say g_1 is. Then g_1 is constant and therefore so is g. This proves that f is irreducible in $K[X]$. □

Example 43. Prove that $f = X^3 + 2X + 7 \in \mathbb{Q}[X]$ is irreducible.

Solution. By proposition 41b (with $A = \mathbb{Z}$ and $K = \mathbb{Q}$) it is enough to prove that f is irreducible in $\mathbb{Z}[X]$. Suppose $f = gh$ with $g, h \in \mathbb{Z}[X]$ both

nonconstant. We may suppose that $\deg g = 1$, $\deg h = 2$, say, $g = aX - b$, $h = cX^2 + dX + e$. Then $ac = 1$, say, $a = c = 1$. Then b is a root of g whence of f. Also, $be = 7$, so $b \in \{-1, 1, -7, 7\}$. None of these four values is a root of f. This contradiction finishes the proof. □

Example 44. Prove that $f = X^5 - 3X^4 + 2X^2 - X + 5$ has no roots in $\mathbb{Q}$.

Solution. Clearly, a factorisation $f = g_1 \cdots g_k$ exists with $g_i \in \mathbb{Z}[X]$ irreducible. Suppose that f has a root in $\mathbb{Q}$. Then some g_i has. By Gauss' lemma, g_i is irreducible in $\mathbb{Q}$ so it must be of degree 1, say, $g_i = aX - b$. Then

$$X^5 - 3X^3 + 2X^2 - X + 5 = f = (aX - b)(c_0X^4 + \cdots + c_4)$$

for some $c_i \in \mathbb{Z}$. By looking at the first and last coefficients we find $ac_0 = 1$ (say $a = 1$) and $5 = -bc_4$. So the root b of $g_i = X - b$ is an integer, and a divisor of 5. So b is in $\{-1, 1, -5, 5\}$. Try them all and find that none is a root of f. □

Theorem 45. Let $f \in \mathbb{Z}[X]$. Let $\mathbb{F}_p = \mathbb{Z}/(p)$ and let $\phi\colon \mathbb{Z} \to \mathbb{F}_p$ be the natural map. Denote the extension $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ by ϕ too. Suppose that $\phi(f)$ is irreducible in $\mathbb{F}_p[X]$ and has the same degree as f. Then $f \in \mathbb{Q}[X]$ is irreducible.

Proof. Note that f is not constant (otherwise $\phi(f)$ isn't irreducible). We may also suppose that f is primitive; for otherwise, divide it by the gcd of its coefficients, which is coprime to p by (1). By proposition 41b (with $A = \mathbb{Z}$ and $K = \mathbb{Q}$) it is enough to prove that f is irreducible in $\mathbb{Z}[X]$.

Suppose $f = gh$ with $g, h \in \mathbb{Z}[X]$. Then $\phi(f) = \phi(g)\,\phi(h)$. As $\phi(f)$ is assumed to be irreducible in $\mathbb{F}_p[X]$ one among $\phi(g)$, $\phi(h)$ has the same degree as $\phi(f)$, say $\phi(g)$ has. Then $\deg g \geq \deg \phi(g) = \deg \phi(f) = \deg f$. It follows that f is irreducible in $\mathbb{Z}[X]$ as required. □

Example 46: Irreducible polynomials over $\mathbb{F}_2$. We will compute all irreducible polynomials in $\mathbb{F}_2[X]$ of degree $d \leq 4$.

***d* = 1.** Such polynomials are always irreducible and they are X, $X + 1$.

***d* = 2.** Irreducible polynomials of degree ≥ 2 are not divisible by X nor $X + 1$, that is, the constant coefficient is not 0 and the sum of the coefficients is not 0. For $d = 2$ only

$$X^2 + X + 1$$

remains which is indeed irreducible.

***d* = 3.** From now on we write, for example, 1101 instead of $X^3 + X^2 + 1$. A polynomial of degree 3 is irreducible if and only if it has no linear factor. So

$$1101 \quad \text{and} \quad 1011$$

is a complete list of irreducible polynomials of degree 3.

***d* = 4.** The polynomials of degree 4 without linear factor are 11001, 10101, 10011, 11111. The only reducible polynomial among them is $(X^2 + X + 1)^2 = (111)^2 = 10101$. So

$$11001, \quad 10011 \quad \text{and} \quad 11111$$

is a complete list of irreducible polynomials of degree 4.

Applying theorem 45 we find lots of irreducible polynomials over $\mathbb{Q}$. For example, $3X^4 + 5X^3 - 2X^2 + 5$ is irreducible in $\mathbb{Q}[X]$ because mod 2 it is 11001 which is irreducible.

Theorem 47: Eisenstein. Let A be a UFD, $K = \operatorname{Frac} A$. Let $p \in A$ be an irreducible element. Let $f = \sum_{i=0}^{m} a_i X^i \in A[X]$ be a nonconstant primitive polynomial satisfying

(1) $a_m \notin (p)$,

(2) $a_i \in (p)$ for $0 \leq i \leq m-1$,

(3) $a_0 \notin (p^2)$.

(We call f **Eisenstein** at p). Then f is irreducible in $A[X]$ and $K[X]$.

Proof. By Gauss' lemma, it is enough to prove that f is irreducible in $A[X]$. Suppose $g, h \in A[X]$ are such that $f = gh$. Write $g = \sum b_i X^i$, $h = \sum c_i X^i$. We have $a_0 = b_0 c_0$. By assumptions (2) and (3) precisely one of b_0, c_0 is in (p). Say $b_0 \in (p)$ and $c_0 \notin (p)$.

By induction on k we shall prove that $b_k \in (p)$ if $k < m$. It is true for $k = 0$. Let $0 < k < m$. Then

$$(p) \ni a_k = \sum_{i=0}^{k} b_i c_{k-i} = \Big(\sum_{i=0}^{k-1} b_i c_{k-i} \Big) + b_k c_0.$$

The factors b_i in the last sum are all in (p). It follows that $b_k c_0 \in (p)$. As (p) is a prime ideal not containing c_0 it must contain b_k. This proves that $b_k \in (p)$ whenever $k < m$. We have $g \notin pA[X]$, for otherwise $f \in pA[X]$, contradicting (1). Thus g has the same degree as f. As f is assumed to be primitive and nonconstant, it is irreducible in $A[X]$ as promised. □

Example 48. Let p be a prime number. We shall prove that the cyclotomic polynomial

$$\phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1 = \frac{X^p - 1}{X - 1}$$

is irreducible. We have

$$\phi_p(Y+1) = \frac{(Y+1)^p - 1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}.$$

This is an Eisenstein polynomial at p hence is irreducible.

Example 49. We shall prove that $f = X^5 + Y^4 + Y^3$ is irreducible in $\mathbb{Q}[X, Y]$ and $\mathbb{Q}(Y)[X]$. In Eisenstein's criterion, put $A = \mathbb{Q}[Y]$, so that $K = \mathbb{Q}(Y)$. Then f is Eisenstein at the irreducible element $p = 1 + Y$ and the claim follows.

3.2 Field extensions

Notation 50. Let A be a ring. The notation $A[x_1, \ldots, x_n]$ has two possible meanings both of which we shall encounter. Firstly, it may denote the ring of

polynomials over A in n variables $x_1, \dots, x_n$. The second meaning is that a ring B containing A is understood, containing $x_1, \dots, x_n$; then $A[x_1, \dots, x_n]$ denotes the smallest subring of B containing $A \cup \{x_1, \dots, x_n\}$.

In order to make it clear which meaning applies, we agree that elements of rings are denoted by small or greek letters except if they are variables, in which case they are denoted by capital letters. Thus for $A[X]$ the first notion is meant, for $A[x]$ the second is.

The same story applies to fields instead of rings and round brackets $(\cdot)$ instead of square ones $[\cdot]$. For example, $K(X) := \operatorname{Frac} K[X]$ is the field of rational functions over a field K, but $K(x)$ indicates that a field $L \supset K$ and an element $x \in L$ have been specified earlier on, and $K(x)$ is the smallest subfield of L containing $K \cup \{x\}$.

We always have $A[x_1, \dots, x_n] = A(x_1, \dots, x_n)$ because every field is a ring.

A **field extension** is a pair (K, L) of a field L and a subfield K. Other notations are $K \subset L$ and L/K.

Example 51. Here is a baby example of a field extension, aiming to get us used to field extensions and the questions that interest us. Our methods can be shortened in many places once we know more of the theory to come, so don't take our solution as the last word.

(a) Prove that $\sqrt{2} \in \mathbb{R}$ is irrational.

(b) Prove that $1, \sqrt{2}$ are independent over $\mathbb{Q}$.

(c) Let $K = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Prove that K is a subfield of $\mathbb{R}$.

(d) Let L be a subfield of K. Prove that $L = \mathbb{Q}$ or $L = K$.

(e) Prove that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) = K$.

(f) Define $\sigma\colon K \to K$ by $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. Prove that σ is a field automorphism of K.

(g) Let ϕ be a field automorphism of K. Prove that $\phi(\sqrt{2})$ is either $\sqrt{2}$ or $-\sqrt{2}$.

(h) Prove that $\phi = 1$ or $\phi = \sigma$.

Solution. (a). Suppose not: $\sqrt{2} = p/q$ with $p, q \in \mathbb{Z}$ coprime. Then $2q^2 = p^2$. Then p^2 is even, so p is even. Then p^2 is divisible by 4, hence so is $2q^2$. So q is even, contradiction.

(b). This is immediate from (a).

(c). Let $x, y \in K$. We must show that $x - y$, xy and x^{-1} are in K (if $x \neq 0$). For $x - y$ this is easy. For xy, write $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ with $a, b, c, d \in \mathbb{Q}$. Then

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in K.$$

For x^{-1}, we have

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in K.$$

(d). By proposition 39 we know that $\mathbb{Q}$ is the smallest subfield of K. Suppose that $L \neq \mathbb{Q}$, say, $x = a + b\sqrt{2} \in L \setminus \mathbb{Q}$ with $a, b \in \mathbb{Q}$. Then $b \neq 0$ and $\sqrt{2} = (x - a)b^{-1} \in L$. So, for all $c, d \in \mathbb{Q}$ we have $c + d\sqrt{2} \in L$. So $L = K$.

(e). The inclusion $\mathbb{Q}[\sqrt{2}] \subset= \mathbb{Q}(\sqrt{2})$ is trivial. The inclusion $\mathbb{Q}(\sqrt{2}) = K$ holds because K is a field by (c). Finally $K \subset \mathbb{Q}[\sqrt{2}]$ is clear from the definition of K.

(f). In order to show that σ is a ring homomorphism $K \to K$, we must show $\sigma(1) = 1$, $\sigma(x + y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in K$. Writing $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ we have

$$\begin{aligned}\sigma(x)\,\sigma(y) &= (a - b\sqrt{2})(c - d\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} \\ &= \sigma\big((ac + 2bd) + (ad + bc)\sqrt{2}\big) \\ &= \sigma\big((a + b\sqrt{2})(c + d\sqrt{2})\big) = \sigma(xy).\end{aligned}$$

Do the other cases yourself. Finally, we observe that σ is bijective and is therefore a ring (hence field) automorphism of K.

(g). We have

$$\begin{aligned}(\phi(\sqrt{2}))^2 &= \phi(\sqrt{2}^2) && \text{because } \phi \text{ is a field automorphism} \\ &= \phi(2) \\ &= 2 && \text{because } \phi \text{ is a field automorphism.}\end{aligned}$$

So $\phi(\sqrt{2})$ is a square root of 2 in K. In other words, it is a zero of the polynomial $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ and must therefore be $\sqrt{2}$ or $-\sqrt{2}$.

(h). For all $a, b \in \mathbb{Q}$, we have $\phi(a + b\sqrt{2}) = a + b\,\phi(\sqrt{2})$. So if ϕ preserves $\sqrt{2}$ then $\phi = 1$. Also, if ϕ changes the sign of $\sqrt{2}$ then $\phi = \sigma$. □

Let L be a ring containing a field K. (Often L is a field too). On L we can then put a structure of a **vector space** over K as follows. Addition in the vector space L is addition in the ring L. Scalar multiplication $(a, x) \mapsto ax$ ($a \in K$, $x \in L$) is a particular case of multiplication in the ring L. Convince yourself that this makes L into a vector space over K.

If $K \subset L$ are fields, we define the **degree** $[L : K] := \dim_K(L)$, that is, the dimension of L as vector space over K. It is a positive integer or infinite.

Example 52. As we saw in example 51, $\{1, \sqrt{2}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2})$ and therefore $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Example 53. We have $[K : K] = 1$ for all fields. Conversely, if $[L : K] = 1$ then $L = K$.

3.3 Primitive extensions

A field extension L/K is said to be **primitive** if there exists $\alpha \in L$ such that $L = K(\alpha)$.

Definition 54. Let $K \subset L$ be fields and $\alpha \in L$. We say that α is **algebraic** over K if there exists a nonzero polynomial $f \in K[X]$ such that $f(\alpha) = 0$. Otherwise we call α **transcendental** over K.

Example 55. The complex numbers e and π are transcendental over $\mathbb{Q}$. For e this was proved by Hermite in 1873, and for π by von Lindemann in 1882. These results don't belong to Galois theory but rather a branch of number theory. Not much more is known; for example, it is unknown whether $e + \pi$ is transcendental.

Exercise (3.1) In this exercise, we will see that transcendental elements behave just as variables.

Let K be a field and α an element of a larger field. Suppose that α is transcendental over K. Then there exists a unique isomorphism of fields $h\colon K(X) \to K(\alpha)$ such that $h(X) = \alpha$ and $h(c) = c$ for all $c \in K$.

The case of algebraic α behaves as follows.

Proposition 56. Let K be a field and α be an element of a larger field. Suppose that α is algebraic over K. Let $f \in K[X]$ be a monic polynomial of minimal degree such that $f(\alpha) = 0$. Write $n = \deg f$. Then:

(a) f is unique.

(b) f is irreducible over K.

(c) A polynomial $g \in K[X]$ satisfies $g(\alpha) = 0$ if and only if g is a multiple of f.

(d) The elements $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are a K-basis of $K(\alpha)$.

(e) $[K(\alpha) : K] = n$.

(f) $K(\alpha) = K[\alpha]$.

Proof. Proof of (a). Let f_1, f_2 both satisfy the requirements, and suppose that $f_1 \neq f_2$. Then $\deg(f_1) = \deg(f_2)$. Let c be the leading coefficient of $f_1 - f_2$ and put $g = c^{-1}(f_1 - f_2)$. Then $\deg(g) < \deg(f_1) = \deg(f_2)$. By the assumption that $f_1(\alpha) = 0$ and $f_2(\alpha) = 0$ we have $g(\alpha) = 0$, which is a contradiction because $\deg(f_1)$ is minimal.

Proof of (b). Let $f = gh$ with $g, h \in K[X]$. We need to prove that g or h is invertible in $K[X]$. We may suppose that g and h are monic. We have $0 = f(\alpha) = g(\alpha) \cdot h(\alpha)$, so $g(\alpha) = 0$ or $h(\alpha) = 0$; say $g(\alpha) = 0$. Then $\deg(g) \geq \deg(f)$ because $\deg(f)$ is minimal among all monic polynomials in $K[X]$ vanishing at α. It follows that $g = f$ and $h = 1$ as required.

Proof of (c). Let $g \in K[X]$. If g is a multiple fh of f ($h \in K[X]$) then certainly $g(\alpha) = 0$. As to the converse, suppose that $g(\alpha) = 0$. By division with remainder (theorem 2) there are $q, r \in K[X]$ such that $g = q \cdot f + r$ and $\deg(r) < \deg(f)$. Now $r(\alpha) = 0$. But there are no nonzero polynomials in $K[X]$ vanishing at α of degree smaller than f, so $r = 0$. So $g = q \cdot f$ as required.

Proof of (d). We need to prove that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are spanning and independent.

Independent. Suppose $\sum_{k=0}^{n-1} c_k \alpha^k = 0$ with $c_k \in K$, not all zero. On defining $g \in K[X]$ by $g = \sum_{k=0}^{n-1} c_k X^k$ we have $g(\alpha) = 0$ and $\deg(g) < \deg(f)$. If c is the leading coefficient of g then $c^{-1}g$ is monic and we obtain a contradiction as $\deg(f)$ is minimal. This proves independent.

Spanning. Let A be the subspace of $K(\alpha)$ spanned by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. If we show that A is a field it will follow that $A = K(\alpha)$. First we prove $K[\alpha] \subset A$. Let $\beta \in K[\alpha]$, say, $\beta = \sum_k c_k \alpha^k$ with $c_k \in K$. Put $g = \sum_k c_k X^k$. By division with remainder (theorem 2) there are $q, r \in K[X]$ such that $g = q \cdot f + r$ and $\deg(r) < \deg(f)$. Then $\beta = g(\alpha) = r(\alpha) \in A$. This proves that $K[\alpha] \subset A$. In order to prove that A is a field, let $\beta \in A$ be nonzero. The map $L\colon A \to A$, $\gamma \mapsto \beta\gamma$ is a K-linear map. Moreover, L is injective, because $L(\gamma) = 0$ implies $\beta\gamma = 0$ and therefore $\gamma = 0$. Thus, L is an injective linear map from a finite dimensional vector space A over K to itself, and therefore is surjective by things you learned in linear algebra. So there exists $\delta \in A$ such that $L(\delta) = 1$, that is, $\beta\delta = 1$, and therefore β has an inverse $\delta \in A$. This proves that A is a field and the proof of spanning is complete.

Parts (e) and (f) follow immediately from (d). □

Definition 57. Let K be a field and let α be an algebraic element of a field extension of K. The monic polynomial $f \in K[X]$ of minimal degree such that $f(\alpha) = 0$ (which is unique by proposition 56a) is called the **minimum polynomial** over K of α, and is written $f = \mathrm{mp}_K(\alpha)$. The degree of $\mathrm{mp}_K(\alpha)$ is written $\deg_K(\alpha)$ and called the **degree** over K of α.

Example 58. Let $f = X^3 + X + 1$ and let α be an element in a field containing $\mathbb{Q}$ such that $f(\alpha) = 0$. It can be shown that $f \in \mathbb{Q}[X]$ is irreducible. Therefore, $\{1, \alpha, \alpha^2\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha)$ by proposition 56d. Thus α^{-2} is of the form $c_0 + c_1\alpha + c_1\alpha^2$ for unique c_0, c_1, c_2. Here is how to find the c_i.

The polynomials f and $g := X^2$ are coprime so there are unique polynomials $p, q \in \mathbb{Q}[X]$ such that $pf + qg = 1$ and $\deg q < \deg f$. We find p, q by Euclid's algorithm for polynomials. The result is $(1 - X) \cdot f + (X^2 - X + 1) \cdot g = 1$. Substituting α for X gives $(1 - \alpha) \cdot f(\alpha) + (\alpha^2 - \alpha + 1) \cdot \alpha^2 = 1$, whence $\alpha^{-2} = \alpha^2 - \alpha + 1$.

3.4 Existence and uniqueness of primitive extensions

Definition 59. Let L_1/K and L_2/K be two field extensions. By a ***K*-homomorphism** $f\colon L_1 \to L_2$ we mean a ring homomorphism f such that $f(c) = c$ for all $c \in K$. The set of K-homomorphisms from L_1 to L_2 is written $\mathrm{Hom}_K(L_1, L_2)$.

Let K, L be fields and let $\sigma\colon K \to L$ be a ring homomorphism. We call (σ, K, L) a field extension (**in the wide sense**). This is indeed very similar to a field extension (in the usual or narrow sense) because $L/\sigma(K)$ is a field extension, and it is easy to prove that σ is injective, whence K and $\sigma(K)$ are isomorphic. Conversely, every field extension L/K gives rise to a field extension (i, K, L) in the wide sense by putting $i\colon K \to L$ to be the inclusion.

Most notions and results about field extensions in the narrow sense ex-

tend to extensions in the wide sense. We won't always make the generalisations explicit and you should be able to produce and use the generalisations yourself when necessary.

For example, the generalisation of definition 59 is as follows. If (σ_1, K, L_1) and (σ_2, K, L_2) are field extensions of K in the wide sense then a K-homomorphism $f\colon L_1 \to L_2$ is by definition a ring homomorphism such that $\sigma_2 \circ f = \sigma_1$.

Note that every minimum polynomial is irreducible by proposition 56b. We have the following converse:

Proposition 60. Let K be a field and let $f \in K[X]$ be an irreducible monic polynomial. Then the following hold.

(a) There exists an element α in a larger field whose minimum polynomial is f.

(b) Consider two primitive field extensions $K(\alpha)/K$ and $K(\beta)/K$ such that α and β have equal minimum polynomials over K. Then there exists a unique K-isomorphism $h\colon K(\alpha) \to K(\beta)$ such that $h(\alpha) = \beta$.

(c) Consider two field extensions $K(\alpha)/K$ and L/K. Then there exists a bijection

$$\phi\colon \mathrm{Hom}_K\big(K(\alpha), L\big) \to \big\{\text{roots in } L \text{ of } \mathrm{mp}_K(\alpha)\big\}$$

defined by $\phi(g) = g(\alpha)$.

Proof. Proof of (a). By proposition 56b, f is irreducible in $K[X]$. By propositions 32 and 33, the ideal $(f) \subset K[X]$ generated by f is therefore maximal. By proposition 30 this implies that $L := K[X]/(f)$ is a field. Let $p\colon K[X] \to L$ be the natural map: $p(g) = g + (f)$. Put $\alpha = p(X)$. Then $f(\alpha) = 0$ because $f(\alpha) = f(X + (f)) = f(X) + (f) = (f) = 0$.

Proof of (b). Existence. Define the ring homomorphism $\theta\colon K[X] \to K(\alpha)$ by $\theta(g) = g(\alpha)$ and $\theta(c) = c$ for all $c \in K$.

Let $I = \ker\theta$ and let $\theta(K[X])$ denote the image of θ. By proposition 36 (first isomorphism theorem) there is a ring homomorphism $\theta'\colon K[X]/I \to \theta(K[X])$ defined by $\theta'(g + I) = \theta(g)$; it satisfies $\theta'(X + I) = \alpha$.

By proposition 56c we have $I = (f)$. Also, $\theta(K[X]) = K[\alpha] = K(\alpha)$ by proposition 56f. Thus, we have a K-isomorphism $\theta'\colon K[X]/I \to K(\alpha)$ taking $X + I$ to α. Likewise, there exists a K-isomorphism $\theta''\colon K[X]/I \to K(\alpha)$ taking $X + I$ to β. The quotient of θ' and θ'' is a K-isomorphism $K(\alpha) \to K(\beta)$ taking α to β. This proves existence.

Uniqueness. Let g and h be K-isomorphisms $K(\alpha) \to K(\beta)$ taking α to β, Then g, h agree on $K \cup \{\alpha\}$ hence on $K(\alpha)$, that is, $g = h$. This proves uniqueness and thereby (b).

Proof of (c). Write $f = \mathrm{mp}_K(\alpha)$. First we should prove that $\phi(g)$ is always a root of f. Let $g \in \mathrm{Hom}_K(K(\alpha), L)$. Write $f = \sum c_i X^i$, $c_i \in K$. Then

$$\begin{aligned} f(g(\alpha)) &= \sum_i c_i\, g(\alpha)^i \\ &= \sum_i g(c_i)\, g(\alpha)^i \quad \text{because } g \text{ is a } K\text{-homomorphism} \end{aligned}$$

$$
\begin{aligned}
&= g \sum_i c_i \alpha^i && \text{because } g \text{ is a ring homomorphism} \\
&= g(f(\alpha)) \\
&= g(0) \\
&= 0 && \text{because } g \text{ is a ring homomorphism}
\end{aligned}
$$

as required.

That ϕ is injective is proved as unicity in (b).

Finally, we prove that ϕ is surjective. Let $\beta \in L$ be a root of f. By (b), there exists a K-isomorphism $g\colon K(\alpha) \to K(\beta)$ taking α to β. Then g is certainly a K-homomorphism $K(\alpha) \to L$, and $\phi(g) = g(\alpha) = \beta$. □

3.5 The tower law

Next we consider a **tower** of three fields $K \subset L \subset M$. Then M is a vector space over both L and K. In order to distinguish the two we extend the usual terminology of basis, spanning, independent, vector space and say ***K*-basis, spanning over *L*** and so on.

Theorem 61: Tower law. Let $K \subset L \subset M$ be fields. Then $[M : K]$ is finite if and only if $[M : L]$ and $[L : K]$ are both finite. If they are then

$$[M : K] = [M : L][L : K].$$

Proof. Suppose that $[M : K]$ is finite. Let $z_1, \ldots, z_n$ be a K-basis of M. Then the z_i span M as an L-vector space, so $[M : L] < \infty$. Suppose that $[L : K] = \infty$. Then there are infinitely many K-linearly independent elements in L; they are also in M and show that $[M : K] = \infty$, a contradiction. So $[L : K] < \infty$.

In the remaining part of the proof, we assume that $[M : L]$ and $[L : K]$ are finite. Let $x_1, \ldots, x_m$ be an L-basis of M and $y_1 \ldots, y_\ell$ a K-basis of L. To finish the proof, we shall prove that $B = \{x_i\, y_j \mid 1 \le i \le m,\ 1 \le j \le \ell\}$ is a K-basis of M. We must show that they span and that they are independent.

Spanning. Let $z \in M$. We may write $z = \sum_i a_i\, x_i$ ($a_i \in L$) because the x_i span M over L. We may write $a_i = \sum_j b_{ij}\, y_j$ ($b_{ij} \in K$) because the y_j span L over K. We get $z = \sum_i a_i\, x_i = \sum_i (\sum_j b_{ij}\, y_j)\, x_i = \sum_{ij} b_{ij}\, x_i\, y_j$. This proves that B spans M over K.

Independent. Let $\sum_{ij} b_{ij}\, x_i\, y_j = 0$ and $b_{ij} \in K$. We need to prove that $b_{ij} = 0$ for all i, j. We have $0 = \sum_i (\sum_j b_{ij}\, y_j)\, x_i$, which is a linear combination of the x_i whose coefficients $a_i := \sum_j b_{ij}\, y_j$ are in L. As the x_i are L-independent, we find $a_i = 0$ for all i. Now fix i, and consider the equation $0 = \sum_j b_{ij}\, y_j$. The right hand side is a K-linear combination of the y_j. As the y_j are K-independent, we find $b_{ij} = 0$ for all j as promised. □

Example 62. Recall that we proved in example 51d that there are no fields properly between $\mathbb{Q}$ and $K := \mathbb{Q}(\sqrt{2})$. Prove this again using the tower law.

Solution. We know already that $[K : \mathbb{Q}] = 2$. Suppose that $\mathbb{Q} \subset L \subset K$ are fields. The tower law gives $2 = [K : \mathbb{Q}] = [K : L][L : \mathbb{Q}]$. But 2 is prime so

either $[K : L] = 1$ or $[L : \mathbb{Q}] = 1$. The first case implies that $L = K$ and the second that $L = \mathbb{Q}$. □

Example 63. Put $\alpha = \sqrt{2} + \sqrt{5}$.

(a) Find a monic $f \in \mathbb{Q}[X]$ of degree 4 such that $f(\alpha) = 0$.

(b) Prove $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\alpha)$.

(c) Prove $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$.

(d) Prove that f is irreducible.

Solution. (a). We have

$$\begin{aligned} 2 = (\sqrt{2})^2 = (\alpha - \sqrt{5})^2 = \alpha^2 - 2\sqrt{5}\,\alpha + 5, \\ 2\sqrt{5}\,\alpha = \alpha^2 + 5 - 2, \\ 20\alpha^2 = (\alpha^2 + 3)^2 \end{aligned} \tag{64}$$

so $f = (X^2 + 3)^2 - 20X^2$ does it.

(b). The inclusion $\supset$ is obvious. By (64) we have

$$\sqrt{5} = \frac{\alpha^2 + 3}{2\alpha} \in \mathbb{Q}(\alpha).$$

It follows that $\sqrt{2} = \alpha - \sqrt{5} \in \mathbb{Q}(\alpha)$. This proves the reverse inclusion $\subset$.

(c). Suppose that $\sqrt{5} \in \mathbb{Q}(\sqrt{2})$, say $\sqrt{5} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. Then

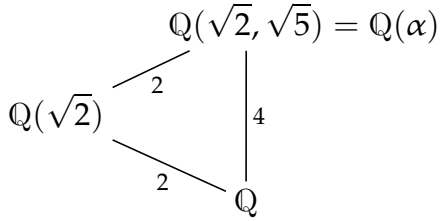
$$5 = (a + b\sqrt{2})^2 = (a^2 + 2b^2) + (2ab)\sqrt{2}.$$

We know that $1, \sqrt{2}$ are linearly independent over $\mathbb{Q}$ so $2ab = 0$ so

$$5 = a^2 \quad \text{or} \quad 5 = 2b^2$$

both of which are absurd.

(d). We know that $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] = 2$ by (c) and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.



By the tower law we find $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. By proposition 56 the degree of the minimum polynomial g of α over $\mathbb{Q}$ has degree 4. It is also a divisor of f by (a) so $f = g$. So f is irreducible. (It is harder to prove f to be irreducible by the methods of section 3.1). □

3.6 Exercises

(3.2) In example 46 we computed the irreducible polynomials in $\mathbb{F}_2[X]$ of degree ≤ 4. Compute those of degree 5.

(3.3)

(a) Prove that $h := X^3 + 6X - 11 \in \mathbb{Z}[X]$ is irreducible.

(b) Prove that $s := X^{13} + X^{10} + X^7 + X^4 + 1$ has no roots in $\mathbb{Q}$. Hint: Use Gauss' lemma.

(c) Prove that $r := X^5 + X^2 + 1 \in \mathbb{F}_2[X]$ is irreducible. (Hint: if reducible, it must have a linear or quadratic factor. Try them all.) Deduce that the lift $X^5 + X^2 + 3 \in \mathbb{Q}[X]$ is irreducible.

(d) Prove that $f := X^7 + 6X^3 + 12 \in \mathbb{Z}[X]$ is Eisenstein. Deduce that it is irreducible in $\mathbb{Z}[X]$ and in $\mathbb{Q}[X]$.

(e) Prove that $g := 2X^{10} + 4X^5 + 3 \in \mathbb{Q}[X]$ is irreducible. Hint: which related polynomial is Eisenstein? Use the result of exercise (4) below.

(f) Prove that $X^8 + (Y^4 - 1)X^3 + (Y^4 - Y)$ is irreducible in $\mathbb{Q}(Y)[X]$.

(3.4) Let K be a field. Let $a, b, c, d \in K$ be such that $ad - bc \neq 0$. Let $f \in K[X]$ be a polynomial of degree $n > 1$.

(a) Prove that the expression

$$g(X) := (cX + d)^n f\Big(\frac{aX + b}{cX + d}\Big)$$

is in $K[X]$ and of degree $\leq n$.

(b) Prove that f is irreducible if and only if g is irreducible of degree n.

(3.5) Let K be a field, A a nonzero ring, $f\colon K \to A$ a ring homomorphism.

(a) Prove that f is injective. Note: by definition, we have $f(1_K) = 1_A$. One often writes $f(t)$ instead of t if $t \in K$, and calls A a K-algebra.

(b) Prove that A becomes a vector space over K on defining addition in (the vector space) A to be addition in (the ring) A, and scalar multiplication to be $(t, u) \mapsto (f(t))\,u$ ($t \in K$, $u \in A$).

(c) Let $a \in A$. Prove that the map $A \to A$, $u \mapsto au$ is K-linear.

(3.6) Let A be an integral domain containing a field K. Let $a \in A$ be nonzero. Recall from exercise (5) that A is a vector space over K and that the map

$$\begin{aligned} m_a\colon A &\longrightarrow A, \\ x &\longmapsto ax \end{aligned}$$

is K-linear. Assume that A has finite K-dimension.

(a) Prove that m_a is injective.

(b) Prove that m_a is surjective.

(c) Prove that A is a field.

(3.7) Consider fields $K \subset L \subset K(X)$ and suppose that $K \neq L$. Prove that $[K(X) : L] < \infty$.

(3.8) Let a be an element in an extension of $\mathbb{Q}$ such that $a^3 + 3a + 3 = 0$. Express each of $1/a$, $1/(1 + a)$ and $1/(1 + a^2)$ in the form $c_2a^2 + c_1a + c_0$ with $c_i \in \mathbb{Q}$.

(3.9) Consider the polynomials $f = X^5 + X^2 + 3$, $g = X^3 + 2$ over $\mathbb{Q}$. Using the Euclidean algorithm, find $p, q \in \mathbb{Q}[X]$ such that $pf + qg = 1$, with q of degree ≤ 4. Find $h \in \mathbb{Q}[X]$ such that if $f(\alpha) = 0$ (that is, α is a root of f in some field extension) then $h(\alpha) = g(\alpha)^{-1}$.

(3.10) Put $\alpha = 8^{1/4} \in \mathbb{R}$ and $\beta = \alpha + \alpha^2$.

(a) Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. [Hint: express $\beta(\beta - 2\alpha^2)$ in terms of α.]

(b) Compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and prove your result.

(3.11) Let L/K be an algebraic field extension. Let $\lambda \in L$ be nonzero and such that λ and λ^2 have the same minimum polynomial over K. Prove that λ is a root of unity.

(3.12) Let $L \supset K$ be a field extension such that $[L : K] = 2$.

(a) If K has characteristic 2, prove that there exists $\beta \in L \smallsetminus K$ such that $\beta^2 \in K$ or $\beta^2 + \beta \in K$.

(b) If K has characteristic $\neq 2$, prove that there exists $\beta \in L \smallsetminus K$ such that $\beta^2 \in K$.

(3.13) Let p be a prime number and $\alpha = \cos(2\pi/p)$. Prove $[\mathbb{Q}(\alpha) : \mathbb{Q}] = (p-1)/2$.

(3.14) Let K be a field. Let α be an element in a larger field whose minimum polynomial over K has odd degree. Prove that $K(\alpha) = K(\alpha^2)$. Is the converse true?

(3.15) (a) Let $\alpha = \sqrt[5]{2} \in \mathbb{R}$. Prove $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$.

(b) Let $\beta = \alpha + \alpha^3$. Use the tower law to prove $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

(3.16) Suppose that $K \subset L$ is a field extension. Let $\alpha \in L$ be algebraic over K of degree m and $\beta \in L$ be algebraic over K of degree n.

(a) Prove that $\alpha + \beta$ is algebraic over K of degree $\leq mn$.

(b) If m, n are coprime, prove $[K(\alpha, \beta) : K] = mn$.

(c) Let $\alpha := 2^{1/2} \in \mathbb{R}$, $\beta := 5^{1/3} \in \mathbb{R}$, $\gamma := \alpha + \beta$. Prove $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$.

(d) Prove that γ is of degree 6 over $\mathbb{Q}$.

(e) Compute the minimal polynomial of γ over $\mathbb{Q}$.

(3.17) Let $\epsilon = \exp(2\pi i/7)$, $\alpha = \varepsilon + \varepsilon^2 + \varepsilon^4$, $\beta = \varepsilon^3 + \varepsilon^5 + \varepsilon^6$.

(a) Compute the elementary symmetric polynomials in α, β and prove that they are in $\mathbb{Q}$.

(b) Find $d \in \mathbb{Q}$ such that $\alpha \in \mathbb{Q}(\sqrt{d})$.

(c) Compute the elementary symmetric polynomials in $\varepsilon, \varepsilon^2, \varepsilon^4$ and prove that they are in $\mathbb{Q}(\alpha)$. (So the 7-gon can be constructed by solving quadratics and a single cubic).

(3.18) Prove that the 13th roots of unity can be obtained by solving a single cubic equation and some quadrics.

(3.19) Let p be a prime number. Prove that for any field K and any $a \in K$, the polynomial $f(X) = X^p - a$ is either irreducible, or has a root.

[Hint: If $f = gh$, factorise g, h into linear factors over a bigger field, and consider their constant terms.]

(3.20) Let p be a prime number and K a field over which $X^p - 1$ splits into linear factors. Suppose that L/K is a field extension, and that $\alpha \in L$ has minimal polynomial $f \in K[X]$ of degree n coprime to p. Prove that $K(\alpha) = K(\alpha^p)$; find a counterexample if K does not contain all the pth roots of 1. [Hint: argue on the degree $[K(\alpha) : K(\alpha^p)]$ and use the result of exercise (19).]

(3.21) Let $K \subset L$ be an extension having degree $[L : K] = n$ coprime to a prime number p. Let $a \in K$. Prove that a is a pth power in K if and only if it is in L.