

## §51 Kronecker's Theorem

In this paragraph, we prove an important theorem due to L. Kronecker which states that any polynomial over a field has a root in some extension field. It can be regarded as the fundamental theorem of field extensions. As might be expected from Kronecker's philosophical outlook, the proof is constructive: we do not merely prove the existence of such an extension in an unseen world; we actually describe what its elements are and how to add, multiply and invert them.

In our discussions concerning the roots of polynomials, we assumed, up to this point, that we are given: (1) a field  $K$ ; (2) a polynomial  $f(x)$  in  $K[x]$ ; (3) an extension field  $E$  of  $K$ ; (4) an element  $a$  of  $E$  which is a root of  $f(x)$ . But in many cases, we are given only a field  $K$  and a polynomial  $f(x)$  in  $K[x]$ , and the problem is to find a root of  $f(x)$ . In more detail, the problem is to find a field  $E$ , an extension of  $K$ , and an element  $a$  in  $E$  such that  $f(a) = 0$ . Not only are we to find  $a$ , but we are also to find  $E$ , which is not given in advance. Kronecker's theorem tells us how to do this.

Let us consider a historical example, viz. the introduction of complex numbers into mathematics in the 18th and 19th centuries. Mathematicians had the field  $\mathbb{R}$  of real numbers, and the polynomial  $x^2 + 1 \in \mathbb{R}[x]$ . This polynomial has no root in  $\mathbb{R}$ , because there is no real number whose square is  $-1$ . However, there were strong indications (for instance Cardan's formula for the roots of a cubic polynomial) that a root of this polynomial would be very welcome. What did mathematicians do, then? They invented a symbol  $\sqrt{-1}$ , which they perfectly knew not to be a real number, and considered the expressions  $a + b\sqrt{-1}$ , where  $a, b \in \mathbb{R}$ . These expressions were coined "complex numbers" (not a fortunate name, by the way). Two complex numbers  $a + b\sqrt{-1}$  and  $a' + b'\sqrt{-1}$  are regarded as equal if and only if  $a = a'$  and  $b = b'$ . The sum of two complex numbers is defined in the obvious way. The product of two complex numbers  $a + b\sqrt{-1}$ ,  $c + d\sqrt{-1}$  is found from the naïve calculation

$$(a + b\sqrt{-1})(c + d\sqrt{-1}) = ac + ad\sqrt{-1} + b\sqrt{-1}c + b\sqrt{-1}d\sqrt{-1}$$

$$\begin{aligned}
&= ac + bd(\sqrt{-1})^2 + (ad + bc)\sqrt{-1} \\
&= (ac - bd) + (ad + bc)\sqrt{-1},
\end{aligned}$$

where we interpret  $(\sqrt{-1})^2$  as the real number  $-1$ . Thus  $\sqrt{-1}$  is a computational device: we multiply complex numbers using the usual field properties of  $\mathbb{R}$ , and putting  $-1$  for  $(\sqrt{-1})^2$  wherever  $(\sqrt{-1})^2$  occurs. The rigorous foundation for complex numbers as ordered pairs of real numbers, due to W. R. Hamilton, came in the middle of the 19th century, but there was nothing basically wrong in the "definition" of complex numbers used by the earlier mathematicians. The field  $\mathbb{C}$  were constructed in this way as the extension field  $\mathbb{R}(i)$  of  $\mathbb{R}$  having a root of the polynomial  $x^2 + 1 \in \mathbb{R}[x]$ . More specifically, the complex number  $0 + 1\sqrt{-1}$  is a root of  $x^2 + 1$ .

Another example. Given the field  $\mathbb{Q}$  and the polynomial  $x^4 - 10x^2 + 1$  in  $\mathbb{Q}[x]$ , we wish to find a root of this polynomial. What can we do? As mentioned in Example 50.9(d), we invent a symbol  $a$ , subject it to the condition  $a^4 - 10a^2 + 1 = 0$  and consider all expressions  $c_0 + c_1a + c_2a^2 + c_3a^3$ , as  $c_1, c_2, c_3, c_4$  run independently over  $\mathbb{Q}$ . These expressions are new "num-bers". These new "numbers" are multiplied using the usual field properties of  $\mathbb{Q}$ , and putting  $0$  for  $a^4 - 10a^2 + 1$  wherever  $a^4 - 10a^2 + 1$  occurs (equivalently, putting  $10a^2 - 1$  for  $a^4$  wherever  $a^4$  occurs). The field  $\mathbb{Q}(a)$  is constructed from  $\mathbb{Q}$  and  $a$  as an extension field of  $\mathbb{Q}$  having a root of the polynomial  $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ . More specifically, the "number"

$0 + 1a + 0a^2 + 0a^3$  is a root of  $x^4 - 10x^2 + 1$ .

It is now clear what to do in the general case. Given a field  $K$  and an irreducible polynomial  $f(x)$  in  $K[x]$ , to find a root of  $f(x)$ , we invent a symbol  $u$ , subject it to the condition  $f(u) = 0$  and consider the  $K$ -vector space with the  $K$ -basis  $1, u, u^2, \dots, u^{n-1}$ , where  $n = \deg f(x)$  and  $1, u, u^2, \dots, u^{n-1}$  are computational symbols. We multiply the elements of this  $K$ -vector space by treating  $u$  as an indeterminate over  $K$  and writing  $0$  for  $f(u)$  wherever  $f(u)$  occurs. The rigorous method of doing is to consider the factor ring  $K[x]/(f)$ , as suggested by Theorem 50.6.

**51.1 Theorem (Kronecker's theorem):** *Let  $K$  be a field and  $f(x)$  an irreducible polynomial in  $K[x]$ . Then there is an extension field  $E$  of  $K$  such that  $f(x)$  has a root in  $E$ .*

**Proof:** Let  $E = K[x]/(f)$ , the factor ring of  $K[x]$  modulo the principal ideal generated by  $f(x)$  in  $K[x]$ . Since  $K[x]$  is a principal ideal domain and  $f(x)$  is irreducible in  $K[x]$ , the factor ring  $E = K[x]/(f)$  is a field (Theorem 32.25).

The mapping 
$$\varphi: K \longrightarrow E$$
$$k \rightarrow k + (f)$$

is a ring homomorphism because

$$(k_1 + k_2)\varphi = (k_1 + k_2) + (f) = (k_1 + (f)) + (k_2 + (f)) = k_1\varphi + k_2\varphi$$

and

$$(k_1 k_2)\varphi = k_1 k_2 + (f) = (k_1 + (f))(k_2 + (f)) = k_1\varphi \cdot k_2\varphi$$

for any  $k_1, k_2 \in K$ . Since  $f(x)$  is irreducible in  $K[x]$ , it is not a unit in  $K[x]$ , thus  $1\varphi = 1 + (f) \neq 0 + (f)$  and  $\varphi$  is one-to-one by Lemma 48.8. So  $\varphi$  is a field homomorphism. We identify  $K$  with its image  $K\varphi$  in  $E$ . So we will write  $k$  instead of  $k + (f)$  when  $k \in K$ . In this way, we regard  $K$  as a subfield of  $E$  and  $E$  as an extension field of  $K$ .

Let us write  $u = x + (f) \in E$  for brevity. We claim that  $u$  is a root of  $f(x)$ . Indeed, if  $f(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n \in K[x]$ ,  $b_n \neq 0$ , then

$$\begin{aligned} f(u) &= b_0 + b_1u + b_2u^2 + \cdots + b_nu^n \\ &= (b_0 + (f)) + (b_1 + (f))(x + (f)) + (b_2 + (f))(x + (f))^2 + \cdots + (b_n + (f))(x + (f))^n \\ &= (b_0 + (f)) + (b_1 + (f))(x + (f)) + (b_2 + (f))(x^2 + (f)) + \cdots + (b_n + (f))(x^n + (f)) \\ &= b_0 + b_1x + b_2x^2 + \cdots + b_nx^n + (f) \\ &= f + (f) \\ &= 0 + (f) \\ &= 0 \in E \end{aligned}$$

and so  $u \in E$  is a root of  $f(x)$ . Thus  $E$  is an extension field of  $K$  containing a root of  $f(x)$ . (The identification of  $K$  with  $K\varphi \subseteq E$  amounts to writing  $k$  for  $k + 0u + 0u^2 + \cdots + 0u^n \in E$  when  $k \in K$ .)  $\square$

Let us keep the notation of the preceding proof. Clearly  $K(u) \subseteq E$ . Also, any element of  $E$  has the form  $c_0 + c_1x + c_2x^2 + \cdots + c_mx^m + (f)$ , and thus equals

$$\begin{aligned} &c_0 + c_1(x + (f)) + c_2(x + (f))^2 + \cdots + c_m(x + (f))^m \\ &= c_0 + c_1u + c_2u^2 + \cdots + c_mu^m \end{aligned}$$

and belongs to  $K(u)$ . So  $E \subseteq K(u)$ . This shows that  $E = K(u)$  is a simple extension of  $K$ .

Now let  $F = K(t)$  be another simple extension of  $K$ , generated by a root  $t$  in  $F$  of  $f(x) \in K[x]$ . By Theorem 50.6, we have the field isomorphisms

$$\begin{array}{ll} \alpha: K[x]/(f) \rightarrow K(u) & \beta: K[x]/(f) \rightarrow K(t) \\ g(x) + (f) \rightarrow g(u) & g(x) + (f) \rightarrow g(t) \end{array}$$

induced from the substitution homomorphisms

$$\begin{array}{ll} T_u: K[x] \rightarrow K(u) & T_t: K[x] \rightarrow K(t) \\ g(x) \rightarrow g(u) & g(x) \rightarrow g(t) \end{array}$$

(see Theorem 30.17). Hence

$$\begin{array}{l} \alpha^{-1}\beta: K(u) \rightarrow K(t) \\ g(u) \rightarrow g(t) \end{array}$$

is a field isomorphism:  $K(u) \cong K(t)$ . Besides, since  $k\alpha = (k + (f))\alpha = kT_u = k$  and likewise  $k\beta = k$  for all  $k \in K$ , the restriction of  $\alpha^{-1}\beta$  to  $K \subseteq K(u)$  is the identity mapping on  $K$ . We proved the following strengthening of Kronecker's theorem.

**51.2 Theorem:** *Let  $K$  be a field and let  $f(x) \in K[x]$  be an irreducible polynomial in  $K[x]$ . Then there is a simple extension  $K(u)$  of  $K$  such that  $u \in K(u)$  is a root of  $f(x)$ . Moreover, if  $K(t)$  is also a simple extension of  $K$  such that  $t \in K(t)$  is a root of  $f(x)$ , then  $K(u) \cong K(t)$  and in fact there is an isomorphism  $\sigma: K(u) \rightarrow K(t)$  whose restriction to  $K$  is the identity mapping on  $K$ .  $\square$*

**51.3 Definition:** Let  $K$  be a field and let  $f(x) \in K[x]$  be an irreducible polynomial in  $K[x]$ . Then a simple extension  $K(u)$  of  $K$ , where  $u$  is a root of  $f(x)$  (which field exists and is unique to within an isomorphism whose restriction to  $K$  is the identity mapping on  $K$  by Theorem 51.2), is called the field obtained by *adjoining a root of  $f(x)$  to  $K$* .

**51.4 Remark:** Let  $K$  be a field and let  $f(x) \in K[x]$  be an irreducible polynomial in  $K[x]$ . Suppose  $K(u)$  is the field obtained by adjoining a root  $u$  of  $f(x)$  to  $K$ . Let  $c$  be the leading coefficient of  $f(x)$ . From Theorem 50.3, we learn that  $\frac{1}{c}f(x)$  is the minimal polynomial of  $u$  over  $K$ . Then it follows from Theorem 50.7 that  $|K(u):K| = \deg \frac{1}{c}f(x) = \deg f(x)$ : the degree over  $K$  of the field obtained by adjoining to  $K$  a root an irreducible polynomial  $f(x) \in K[x]$  is equal to the degree of  $f(x)$ .

**51.5 Theorem (Kronecker):** *Let  $K$  be a field and let  $f(x)$  be a polynomial in  $K[x] \setminus K$  (not necessarily irreducible over  $K$ ) with  $\deg f(x) = n$ . Then there is an extension field  $E$  of  $K$  such that  $f(x)$  has a root in  $E$  and  $|E:K| \leq n$ .*

**Proof:** From  $f(x) \notin K$ , we know that  $f(x)$  is neither the zero polynomial nor a unit in  $K[x]$ . As  $K[x]$  is a unique factorization domain, we can decompose  $f(x)$  into irreducible polynomials, and adjoin a root of one of the irreducible divisors of  $f(x)$  to  $K$ . The field  $E$  obtained in this way will have a root of (that irreducible divisor of  $f(x)$ , hence also of)  $f(x)$ . Moreover,  $|E:K|$  will be equal to the degree of that irreducible divisor of  $f(x)$ , hence will be smaller than or equal to  $\deg f(x) = n$ .  $\square$

**51.6 Examples: (a)** Consider the polynomial  $f(x) = x^2 - 2 \in \mathbb{F}_5[x]$ . It is irreducible over  $\mathbb{F}_5$ , for otherwise  $f(x)$  would have a root in  $\mathbb{F}_5$ , whereas there is no element in  $\mathbb{F}_5$  whose square is  $2 \in \mathbb{F}_5$  (in the language of elementary number theory,  $2 \in \mathbb{Z}$  is a quadratic nonresidue mod 5). Let us adjoin a root  $u$  of  $f(x)$  to  $\mathbb{F}_5$ . The resulting field  $\mathbb{F}_5(u)$  is an  $\mathbb{F}_5$ -vector space with an  $\mathbb{F}_5$ -basis  $\{1, u\}$ , and  $u^2 = 2 \in \mathbb{F}_5$ . Here are some sample computations in  $\mathbb{F}_5(u)$ :

$$(4 + 2u)(3 + u) = 12 + 4u + 6u + 3u^2 = 12 + 10u + 3 \cdot 2 = 2 + 0u + 1 = 3,$$

$$(3 + 2u)(2 + 4u) = 6 + 12u + 4u + 8u^2 = 1 + 2u + 4u + 3 \cdot 2 = 7 + 6u = 2 + u.$$

In view of the equation  $u^2 = 2 \in \mathbb{F}_5$ , we agree to write  $\sqrt{2}$  in place of  $u$  in  $\mathbb{F}_5(u)$ . We keep in mind of course that  $\sqrt{2}$  is just another name for our computational device  $u$ : here  $\sqrt{2}$  is *not* the real number 1.414... whose square is the real number 2.

Let us express  $(1 + 2\sqrt{2})(3 + \sqrt{2})$  and  $(4 + \sqrt{2})^{-1}$  in terms of the  $\mathbb{F}_5$ -basis  $\{1, \sqrt{2}\}$ .

$$(1 + 2\sqrt{2})(3 + \sqrt{2}) = 3 + \sqrt{2} + 6\sqrt{2} + 2 \cdot 2 = (3 + 4) + (1 + 6)\sqrt{2} = 2 + 2\sqrt{2},$$

$$\frac{1}{4 + \sqrt{2}} = \frac{1}{4 + \sqrt{2}} \frac{4 - \sqrt{2}}{4 - \sqrt{2}} = \frac{4 - \sqrt{2}}{16 - 2} = \frac{4 - \sqrt{2}}{14} = \frac{4 - \sqrt{2}}{4} = \frac{1}{4} (4 - \sqrt{2})$$

$$= 4(4 - \sqrt{2}) = 16 - 4\sqrt{2} = 1 + \sqrt{2}.$$

$$\text{Check: } (4 + \sqrt{2})(1 + \sqrt{2}) = 4 + 4\sqrt{2} + \sqrt{2} + 2 = 6 + 5\sqrt{2} = 1.$$

Note that  $\varphi: \mathbb{F}_5(\sqrt{2}) \rightarrow \mathbb{F}_5(\sqrt{2})$  is an automorphism of  $\mathbb{F}_5(\sqrt{2})$ , because

$$a + b\sqrt{2} \rightarrow a - b\sqrt{2}$$

$$[(a + b\sqrt{2}) + (c + d\sqrt{2})]\varphi = [(a + c) + (b + d)\sqrt{2}]\varphi$$

$$= (a + c) - (b + d)\sqrt{2}$$

$$= (a - b\sqrt{2}) + (c - d\sqrt{2})$$

$$= (a + b\sqrt{2})\varphi + (c + d\sqrt{2})\varphi$$

$$\text{and } [(a + b\sqrt{2})(c + d\sqrt{2})]\varphi = [(ac + 2bd) + (ad + bc)\sqrt{2}]\varphi$$

$$= (ac + 2bd) - (ad + bc)\sqrt{2}$$

$$= (ac + 2(-b)(-d)) + (a(-d) + (-b)c)\sqrt{2}$$

$$= (a - b\sqrt{2})(c - d\sqrt{2})$$

$$= (a + b\sqrt{2})\varphi \cdot (c + d\sqrt{2})\varphi$$

for all  $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{F}_5(\sqrt{2})$ ; and  $\varphi$  is clearly onto and  $\text{Ker } \varphi \neq \mathbb{F}_5(\sqrt{2})$ . By the binomial theorem (Theorem 29.16),

$$(a + b\sqrt{2})^5 = a^5 + 5a^4b\sqrt{2} + 10a^3b^2 \cdot 2 + 10a^2b^3 \cdot 2\sqrt{2} + 5ab^4 \cdot 4 + b^5 \cdot 4\sqrt{2}$$

$$= a^5 + 4b^5\sqrt{2} = a + 4b\sqrt{2} = a - b\sqrt{2}$$

for all  $a + b\sqrt{2} \in \mathbb{F}_5(\sqrt{2})$ . Thus  $\varphi$  can also be described as

$$\varphi: \mathbb{F}_5(\sqrt{2}) \rightarrow \mathbb{F}_5(\sqrt{2}).$$

$$t \rightarrow t^5$$

**(b)** The polynomial  $g(x) = x^2 - 3 \in \mathbb{F}_5[x]$ , too, is irreducible over  $\mathbb{F}_5$  ( $3 \in \mathbb{Z}$  is a quadratic nonresidue mod 5). Adjoining a root  $\sqrt{3}$  of  $g(x)$  to  $\mathbb{F}_5$ , we obtain the field  $\mathbb{F}_5(\sqrt{3})$ , which is an  $\mathbb{F}_5$ -vector space with a basis  $\{1, \sqrt{3}\}$  over  $\mathbb{F}_5$ , and  $(\sqrt{3})^2 = 3 \in \mathbb{F}_5$ . We do not forget, of course, that  $\sqrt{3}$  is a computational symbol only, and *not* the real number 1.732... whose square is  $3 \in \mathbb{R}$ . In  $\mathbb{F}_5(\sqrt{3})$ , we have

$$(3 + 2\sqrt{3})(1 + 4\sqrt{3}) = 3 + 12\sqrt{3} + 2\sqrt{3} + 8 \cdot 3 = 27 + 14\sqrt{3} = 2 + 4\sqrt{3},$$

$$(2 + 3\sqrt{3})(2 + 4\sqrt{3}) = 4 + 8\sqrt{3} + 6\sqrt{3} + 12 \cdot 3 = 4 + 3\sqrt{3} + \sqrt{3} + 36 = 4\sqrt{3},$$

$$\begin{aligned}\frac{1}{1+3\sqrt{3}} &= \frac{1}{1+3\sqrt{3}} \frac{1-3\sqrt{3}}{1-3\sqrt{3}} = \frac{1-3\sqrt{3}}{1-27} = \frac{1+2\sqrt{3}}{4} = \frac{1}{4}(1+2\sqrt{3}) \\ &= 4(1+2\sqrt{3}) = 4+3\sqrt{3}.\end{aligned}$$

As  $8 = 3$  in  $\mathbb{F}_5$ , we may also write  $\sqrt{8}$  for  $\sqrt{3}$ , with the understanding that  $\sqrt{8} \in \mathbb{F}_5(\sqrt{3})$  is a computational device satisfying  $(\sqrt{8})^2 = 8 = 3$ . Here  $\sqrt{8}$  is *not* the real number  $2.828\dots$  whose square is  $8 \in \mathbb{R}$ . We might be tempted to write  $\sqrt{8} = \sqrt{4 \cdot 2} = 2\sqrt{2}$ . For the time being, this is not legitimate: as  $\sqrt{8} \in \mathbb{F}_5(\sqrt{3})$  and  $2\sqrt{2} \in \mathbb{F}_5(\sqrt{2})$  are in different fields, and not in their intersection  $\mathbb{F}_5$ , it is not meaningful to write  $\sqrt{8} = 2\sqrt{2}$ .

However, this suggests that  $\psi: \mathbb{F}_5(\sqrt{3}) \rightarrow \mathbb{F}_5(\sqrt{2})$  might be an interesting

$$a + b\sqrt{3} \rightarrow a + 2b\sqrt{2}$$

mapping. Indeed,

$$\begin{aligned}[(a + b\sqrt{3}) + (c + d\sqrt{3})]\psi &= [(a + c) + (b + d)\sqrt{3}]\psi \\ &= (a + c) + 2(b + d)\sqrt{2} \\ &= (a + 2b\sqrt{2}) + (c + 2d\sqrt{2}) \\ &= (a + b\sqrt{3})\psi + (c + d\sqrt{3})\psi\end{aligned}$$

$$\begin{aligned}\text{and } [(a + b\sqrt{3})(c + d\sqrt{3})]\psi &= [(ac + 3bd) + (ad + bc)\sqrt{3}]\psi \\ &= (ac + 3bd) + 2(ad + bc)\sqrt{2} \\ &= (ac + 2 \cdot 2b \cdot 2d) + (a \cdot 2d + 2b \cdot c)\sqrt{2} \\ &= (a + 2b\sqrt{2})(c + 2d\sqrt{2}) \\ &= (a + b\sqrt{3})\psi \cdot (c + d\sqrt{3})\psi\end{aligned}$$

for all  $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{F}_5(\sqrt{3})$ , thus  $\psi$  is a ring homomorphism. As it is clearly one-to-one and onto,  $\psi$  is a field isomorphism. Hence  $\mathbb{F}_5(\sqrt{3})$  and  $\mathbb{F}_5(\sqrt{2})$  are isomorphic fields. We *identify* these two fields by the isomorphism  $\psi$ , i.e., by declaring  $a + b\sqrt{3} = a + 2b\sqrt{2}$  for all  $a, b \in \mathbb{F}_5$ . Then, but only then can we write  $\sqrt{3} = 2\sqrt{2}$ .

We could identify these fields by declaring  $a + b\sqrt{3} = a - 2b\sqrt{2}$  for all  $a, b$  in  $\mathbb{F}_5$ , which amounts to identifying them by the isomorphism

$\varphi\psi: \mathbb{F}_5(\sqrt{3}) \rightarrow \mathbb{F}_5(\sqrt{2})$ . How we identify them is not important, but we must consistently use one and the same identification.

When we identify  $\mathbb{F}_5(\sqrt{3})$  and  $\mathbb{F}_5(\sqrt{2})$  by declaring  $a + b\sqrt{3} = a + 2b\sqrt{2}$  for all  $a, b \in \mathbb{F}_5$ , we can no longer interpret  $\sqrt{18}$ , for example, merely as a computational device whose square is  $18 \in \mathbb{F}_5$ , for there are *two* elements in  $\mathbb{F}_5(\sqrt{3}) = \mathbb{F}_5(\sqrt{2})$  whose squares are 18, viz.  $2\sqrt{2}$  and  $-2\sqrt{2} =$

$3\sqrt{2}$ . We must specify which of  $2\sqrt{2}$ ,  $3\sqrt{2}$  we mean by  $\sqrt{18}$ . Otherwise we might commit such mistakes as

$$3\sqrt{2} = \sqrt{9 \cdot 2} = \sqrt{18} = \sqrt{9 \cdot 2} = \sqrt{4 \cdot 2} = 2\sqrt{2} \quad \text{in } \mathbb{F}_5(\sqrt{2})$$

which resembles the mistake

$$-7 = \sqrt{(-7)^2} = \sqrt{49} = 7 \quad \text{in } \mathbb{R}.$$

In  $\mathbb{R}$ , there are two numbers whose squares are 49, namely 7 and -7, and  $\sqrt{49}$  is understood to be the positive of the numbers 7, -7. Thus when we write  $\sqrt{49}$ , we specify which of 7, -7 we mean by  $\sqrt{49}$ . This prevents the mistake  $-7 = \sqrt{(-7)^2}$ . In  $\mathbb{F}_5(\sqrt{2})$ , specifying  $2\sqrt{2}$  or  $3\sqrt{2}$  as  $\sqrt{18}$  prevents the mistake  $3\sqrt{2} = 2\sqrt{2}$ .

### Exercises

- Adjoin a root  $u$  of  $x^3 + 2x^2 - 2 \in \mathbb{Q}[x]$  to  $\mathbb{Q}$  and construct the field  $\mathbb{Q}(u)$ . Express  $(u^2 + u - 1)(u^2 + 2u - 5)$ ,  $(u^2 - 3u + 1)/(u^2 + 2u + 3)$ ,  $(u^4 + u^3)(u^3 - 1)$  in terms of the  $\mathbb{Q}$ -basis  $1, u, u^2$  of  $\mathbb{Q}(u)$ .
- Find all monic irreducible polynomials in  $\mathbb{F}_5[x]$  of degree two (aside from  $x^2 - 2$  and  $x^2 - 3$ , there are eight of them). Adjoining a root  $u$  of these polynomials to  $\mathbb{F}_5$ , construct eight fields  $\mathbb{F}_5(u)$  of 25 elements. Prove that each of these fields is isomorphic to  $\mathbb{F}_5(\sqrt{2})$ .
- Prove that  $\mathbb{F}_5^\times$  and  $\mathbb{F}_5(\sqrt{2})^\times$  are cyclic.
- Find a field  $K$  of nine elements and show that  $K^\times$  is cyclic.
- Prove the following statements.
  - $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$  is irreducible over  $\mathbb{F}_2$ .
  - $g(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$  is irreducible over  $\mathbb{F}_2$ .

Let  $i$  be a root of  $f(x)$  and  $u$  a root of  $g(x)$ .

- $h(x) = x^2 + ix + 1 \in \mathbb{F}_2(i)[x]$  is irreducible over  $\mathbb{F}_2(i)$ .

Let  $t$  be a root of  $h(x) \in \mathbb{F}_2(i)[x]$ .

- $\mathbb{F}_2(i)(t)^\times$  and  $\mathbb{F}_2(u)^\times$  are cyclic.
- $\mathbb{F}_2(i)(t) \cong \mathbb{F}_2(u)$ .