Chapter 5

Field Theory

Abstract field theory emerged from three theories, which we would now call Galois theory, algebraic number theory and algebraic geometry.

Field theoretic notions appeared, even though still implicitly, in the modern theory of solvability of polynomial equations, as introduced by Abel and Galois in the early nineteenth century. Galois had a good insight into fields obtained by adjoining roots of polynomials, and he proved what we call now the Primitive Element Theorem.

Independently, Dedekind and Kronecker came up with the notion of algebraic number fields, arising from three major number -theoretic problems: Fermat's Last Theorem, reciprocity laws and representation of integers by binary quadratic forms.

Algebraic geometry is the study of algebraic curves and their generalizations to higher dimensions, namely, algebraic varieties. Dedekind and Weber carried over to algebraic functions the ideas which Dedekind had earlier introduced for algebraic numbers, that is, define an algebraic function field as a finite extension of the field of rational functions.

At the end of the nineteenth century, abstraction and axiomatics started to take place. Cantor (1883) defined the real numbers as equivalence classes of Cauchy sequences,von Dyck (1882) gave an abstract definition of group (about thirty years after Cayley had defined a finite group). Weber's definition of a field appeared in 1893, for which he gave number fields and function fields as examples. In 1899, Hensel initiated a study of p-adic numbers, taking as starting point the analogy between function fields and number fields. It is the work of Steinitz in 1910 that initiated the abstract study of fields as an independent subject. A few examples of his results are: classification of fields into those of characteristic zero and those of characteristic p, development of the theory of transcendental extensions, recognition that it is precisely the finite, normal, separable extensions to which Galois theory applies, proof of the existence of the algebraic closure of any field.

Major developments in field theory and related areas that followed Steinitz's work include valuation theory, class field theory, infinite Galois theory and finite fields.

5.1 Field extension and minimal polynomial

Definition 5.1. If F and E are fields, and $F \subseteq E$, we say that E is an extension of F, and we write either $F \leq E$ or E/F.

Examples 5.1. Here are some classical examples:

1. $\mathbb{C} = \{a + bi,\ a, b \in \mathbb{R}\}$ is a field extension of $\mathbb{R}$.
2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$ is a field extension of $\mathbb{Q}$.
3. $\mathbb{Q}(i) = \{a + bi,\ a, b \in \mathbb{Q}\}$ is a field extension of $\mathbb{Q}$.

If E is an extension of F, then in particular E is an abelian group under addition, and we may multiply $x \in E$ by $\lambda \in F$. We can see that this endows E with a structure of F-vector space (the elements of E are seen as vectors, those of F as scalars). It then makes sense to speak of the dimension of E over F.

Definition 5.2. Let E/F be a field extension. The dimension of E as F-vector space is called the degree of the extension, written $[E : F]$. If $[E : F] < \infty$, we say that E is a finite extension of F, or that the extension E/F is finite.

Let us get back to our examples:

Examples 5.2.

1. Consider the field extension $\mathbb{C}/\mathbb{R}$. We have that $\mathbb{C}$ is a vector space of dimension 2 over $\mathbb{R}$. It is thus an extension of degree 2 (with basis $\{1, i\}$).
2. The field extension $\mathbb{Q}(\sqrt(2))/\mathbb{Q}$ is of degree 2, it is called a quadratic extension of $\mathbb{Q}$.
3. The field extension $\mathbb{Q}(i)/\mathbb{Q}$ is a also a quadratic field extension of $\mathbb{Q}$.
4. Both $\mathbb{Q}(\sqrt(2))/\mathbb{Q}$ and $\mathbb{Q}(i)/\mathbb{Q}$ are finite field extensions of $\mathbb{Q}$. Finite extensions of $\mathbb{Q}$ are called number fields.

If we look at $\mathbb{C}$, we see it is obtained by adding i to $\mathbb{R}$, and i is a root of the polynomial $X^2 + 1$. Similarly, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is obtained by adding a root of the polynomial $X^2 - 2$. In what follows, we will make formal the connection between roots of polynomials and field extensions.

Before we start, recall that if we have two fields E, F and a field homomorphism between them (that is, a ring homomorphism between two fields), then f is a monomorphism. We have seen the argument in the previous chapter already: the kernel of a ring homomorphism is an ideal, and a field has only trivial ideals, namely $\{0\}$ and itself, and it cannot be that the whole field is the kernel.

Theorem 5.1. *Let f be a non-constant polynomial over a field F. Then there is an extension E/F and an element $\alpha \in E$ such that $f(\alpha) = 0$.*

Proof. Recall that $F[X]$ is a unique factorization domain, thus f can be factored into a product of irreducible polynomials, and we may assume without loss of generality that f is itself irreducible. Consider now the ideal

$$\mathcal{I} = (f(X))$$

in $F[X]$, the ring of polynomials with indeterminate X and coefficients in F. Again using that $F[X]$ is a unique factorization domain, we have that $f(X)$ is irreducible and equivalently prime, implying that $(f(X))$ is prime. Now $F[X]$ is furthermore a principal ideal domain. This means that $\mathcal{I} = (f(X))$ is contained in a principal maximal ideal $(q(X))$, so that $q(X)$ divides the prime $f(X)$. Since $f(X) = q(X)g(X)$ for some $g(X)$, and $q(X)$ cannot be a unit because $f(X)$ is irreducible, $f(X)$ and $q(X)$ are associates, and $(f(X)) = (q(X))$, proving that $(p(X)) = \mathcal{I}$ is maximal. Thus by the characterization of maximal ideals with respect to their quotient ring, we have that

$$E = F[X]/\mathcal{I}$$

is a field. We now place an isomorphic copy of F inside E via the monomorphism

$$h : F \to E,\ a \mapsto a + \mathcal{I}.$$

This thus gives a field extension E/F. Now let

$$\alpha = X + \mathcal{I} \in E.$$

We are left to prove that α is a root of $f(X)$. If $f(X) = a_0 + a_1X + \ldots + a_nX^n$, then

$$\begin{aligned} f(\alpha) &= (a_0 + \mathcal{I}) + a_1(X + \mathcal{I}) + \ldots + a_n(X + \mathcal{I})^n \\ &= a_0 + \mathcal{I} + a_1X + a_1\mathcal{I} + \ldots + a_nX^n + \ldots + a_n\mathcal{I}^n \\ &= (a_0 + a_1X + \ldots + a_nX^n) + \mathcal{I} \\ &= f(X) + \mathcal{I} \end{aligned}$$

which is zero in E. □

The extension E is sometimes said to be obtained from F by adjoining a root of f.

Remark. Note that in the above proof, we have shown that a prime ideal in a principal ideal domain is maximal.

Definition 5.3. If E is an extension of F, an element $\alpha \in E$ is said to be algebraic over F if there is a non-constant polynomial $f \in F[X]$ such that $f(\alpha) = 0$. If α is not algebraic over F, it is said to be transcendental over F. If every element of E is algebraic over F, then E is said to be an algebraic extension of F.

Suppose that $\alpha \in E$ is algebraic over F. Thus there exists by definition a polynomial $f \in F[X]$ with $f(\alpha) = 0$. It thus makes sense to consider the set $\mathcal{I}$ of all polynomials $g \in F[X]$ such that $g(\alpha) = 0$. Clearly

- if g_1, g_2 are in $\mathcal{I}$, so does $g_1 \pm g_2$,
- if $g \in \mathcal{I}$ and $h \in F[X]$, then $gh \in \mathcal{I}$.

This tells us that $\mathcal{I} = \{g \in F[X],\ g(\alpha) = 0\}$ is an ideal of $F[X]$.

Since $F[X]$ is a principal ideal domain, we have

$$\mathcal{I} = (m(X))$$

for some $m(X)$ in $F[X]$. Any two generators of $\mathcal{I}$ are thus multiple of each others, so they must be of same degree, and since $m(X)$ is monic, it has to be unique. This polynomial $m(X)$ has the following properties:

1. If $g \in F[X]$, then $g(\alpha) = 0$ if and only if $m(X)$ divides $g(X)$. This is clear from the definition of $\mathcal{I}$.

2. $m(X)$ is the monic polynomial of least degree such that $m(\alpha) = 0$, which follows from the above property.

3. $m(X)$ is the unique monic irreducible polynomial such that $m(\alpha) = 0$. Indeed, if $m(X) = h(X)k(X)$ with $\deg h < \deg m$, $\deg k < \deg m$, then either $h(\alpha) = 0$ or $k(\alpha) = 0$, so that either $h(X)$ or $k(X)$ is a multiple of $m(X)$ by the first property, which is impossible. Thus $m(X)$ is irreducible. We are left to prove the unicity of $m(X)$. This comes from the fact that since $m(X)$ is monic, then if there were two irreducible monic polynomials $m(X)$ and $m'(X)$ such that $m(\alpha) = m'(\alpha) = 0$, they have α as common root, and thus $m(X)$ and $m'(X)$ cannot be distinct (see the proposition below).

Definition 5.4. The polynomial $m(X)$ is called the minimal polynomial of α over F. It may be denoted by $\min(\alpha, F)$ or $\mu_{\alpha,F}$.

Example 5.3. The polynomial $X^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$. It also the minimal polynomial of i over $\mathbb{R}$.

Proposition 5.2. *1. Let f and g be polynomials over the field F. Then f and g are relatively prime if and only if f and g have no common root in any extension of F.*

2. If f and g are distinct monic irreducible polynomials over F, then f and g have no common roots in any extension of F.

Proof. 1. If f and g are relatively prime, their greatest common divisor is 1, so there are polynomials $a(X)$ and $b(X)$ over F such that

$$a(X)f(X) + b(X)g(X) = 1.$$

If there is a common root say α, then we get that $0 = 1$, a contradiction.

Conversely, let us assume that the greatest common divisor $d(X)$ of $f(X)$ and $g(X)$ is non-constant and show that then $f(X)$ and $g(X)$ have a common root. By the above proposition, there exists E an extension of F in which $d(X)$ has a root α. Since $d(X)$ divides both $f(X)$ and $g(X)$, α is a common root of f and g in E.

2. By the first part, it is enough to show that f and g are relatively prime. Assume to the contrary that h is a non-constant divisor of the polynomials f and g which are irreducible. Then $f = f'h$ and $g = g'h$ with f', g' non-zero constant, and $h = \frac{f}{f'} = \frac{g}{g'}$, that is, $f = \frac{f'}{g'}g$. It is impossible for f to be a constant multiple of g, because f and g are monic and distinct.

□

If E is an extension of F and $\alpha \in E$ is a root of a polynomial $f \in F[X]$, one may consider the field $F(\alpha)$ generated by F and α, which is the smallest subfield of E containing both F and α. Alternatively, $F(\alpha)$ can be described as the intersection of all subfields of E containing F and α, or the set of all rational functions

$$\frac{a_0 + a_1\alpha + \cdots + a_m\alpha^m}{b_0 + b_a 1\alpha + \ldots + b_n\alpha^n}$$

with $a_i, b_j \in F$, $m, n = 0, 1, \ldots$ and the denominator is different from 0.

Theorem 5.3. *Let $\alpha \in E$ be algebraic over F, with minimal polynomial $m(X)$ over F of degree n.*

1. *We have $F(\alpha) = F[\alpha] = F_{n-1}[\alpha]$ where $F_{n-1}[\alpha]$ denotes the set of all polynomials of degree at most $n-1$ with coefficients in F.*

2. *$\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a basis for the vector space $F(\alpha)$ over the field F. Consequently $[F(\alpha) : F] = n$.*

Proof. Let us first prove that $F_{n-1}[\alpha]$ is a field. Let $f(X)$ be any non-zero polynomial over F of degree at most $n-1$. Since $m(X)$ is irreducible with $\deg f < \deg m$, $f(X)$ and $m(X)$ are relatively prime, and there exist polynomials $a(X)$ and $b(X)$ over F such

$$a(X)f(X) + b(X)m(X) = 1.$$

Using that α is a root of m, we get

$$a(\alpha)f(\alpha) = 1$$

so that any non-zero element of $F_{n-1}[\alpha]$ has an inverse, and $F_{n-1}[\alpha]$ is a field.

1. Any field containing F and α must contain all polynomials in α, and in particular all those of degree at most $n-1$. Thus

$$F_{n-1}[\alpha] \subset F[\alpha] \subset F(\alpha).$$

But $F(\alpha)$ is the smallest field containing F and α, so

$$F(\alpha) \subset F_{n-1}[\alpha]$$

and we conclude that

$$F(\alpha) = F[\alpha] = F_{n-1}[\alpha].$$

2. Now $1, \alpha, \ldots, \alpha^{n-1}$ certainly span $F_{n-1}[\alpha]$, and they are linearly independent because if a non-trivial linear combination of them were zero, this would yield a non-zero polynomial of degree less than that of $m(X)$ with α as a root, a contradiction.

□

Example 5.4. Let ζ_5 denote a primitive 5th root of unity (that is, $\zeta_5^5 = 1$ and $\zeta_5^k \neq 1$ for $1 \leq k \leq 4$). We have that $\zeta_5 \in \mathbb{Q}(\zeta_5)$ is algebraic over $\mathbb{Q}$, with minimal polynomial $X^4 + X^3 + X^2 + X + 1 = 0$ of degree 4 over $\mathbb{Q}$. A $\mathbb{Q}$-basis is given by $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ and $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$.

Once we have a field extension K/F, we can take again K as base field and get another field extension E/K, yielding a tower of extensions $E/K/F$.

Proposition 5.4. *Consider the field extensions $E/K/F$.*

1. *If α_i, $i \in I$, form a basis for E over K, and β_j, $j \in J$ form a basis for K over F, then $\alpha_i\beta_j$, $i \in I$, $j \in J$, form a basis for E over F.*
2. *The degree is multiplicative, namely*

$$[E : F] = [E : K][K : F].$$

In particular, $[E : F]$ is finite if and only if $[E : K]$ and $[K : F]$ are finite.

Proof. 1. Take $\gamma \in E$. Then

$$\begin{aligned} \gamma &= \sum_{i \in I} a_i \alpha_i,\ a_i \in K \\ &= \sum_{i \in I} (\sum_{j \in J} b_{ij} \beta_j) \alpha_i,\ b_{ij} \in F. \end{aligned}$$

Thus $\alpha_i\beta_j$ span E over F. We now check the linear independence.

$$\sum_{i,j} \lambda_{ij} \alpha_i \beta_j = 0 \Rightarrow \sum_i \lambda_{ij} \alpha_i = 0$$

for all j and consequently $\lambda_{ij} = 0$ for all i, j which concludes the proof.

2. It is enough to use the first part, with

$$[E : K] = |I|,\ [K : F] = |J|,\ [E : F] = |I||J|.$$

□

Example 5.5. Consider the field extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ where ζ_8 is a primitive 8th root of unity. We have that

$$\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

and $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ is the same field extension as $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$. We have

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

Recall that an algebraic extension is a field extension where every element is algebraic. The result below describes families of algebraic extensions.

Theorem 5.5. *If E is a finite extension of F, then E is an algebraic extension of F.*

Proof. Let $\alpha \in E$ with degree $[E : F] = n$. Then $1, \alpha, \dots, \alpha^n$ are $n+1$ elements while the dimension is n, so they must be linearly dependent, say

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0,\ a_i \in F.$$

Take $p(X) = a_0 + a_1X + \ldots + a_nX^n \in F[X]$, α is a root of $p(X)$ and by definition α is algebraic over F. □

Examples 5.6.
1. By definition, a number field is a finite extension of $\mathbb{Q}$. Thus a number field is an algebraic extension of $\mathbb{Q}$.
2. The converse is not true. There are infinite algebraic extensions, for example, the field of all algebraic numbers over the rationals is algebraic and of infinite degree.

5.2 Splitting fields and algebraic closures

For $\alpha \in E$, an extension of F, we have introduced above $F(\alpha)$ as the intersection of all the subfields of E containing F and α. This can be of course generalized if we pick $\alpha_1, \dots, \alpha_k \in E$, and $F(\alpha_1, \dots, \alpha_k)$ is the intersection of all the subfields of E containing F and $\alpha_1, \dots, \alpha_k$.

Definition 5.5. If E is an extension of F and $f \in F[X]$, we say that f splits over E if f can be written as $\lambda(X - \alpha_1)\cdots(X - \alpha_k)$ for some $\alpha_1, \dots, \alpha_k \in E$ and $\lambda \in F$.

Definition 5.6. If K is an extension of F and $f \in F[X]$, we say that K is a splitting field for f over F is f splits over K but not over any proper subfield of K containing F.

Example 5.7. Consider the polynomial $f(X) = X^3 - 2$ over $\mathbb{Q}$. Its roots are

$$\sqrt[3]{2},\ \sqrt[3]{2}\left(-\frac{1}{2} + i\frac{1}{2}\sqrt{3}\right),\ \sqrt[3]{2}\left(-\frac{1}{2} - i\frac{1}{2}\sqrt{3}\right).$$

Alternatively, if ζ_3 denotes a primitive 3rd root of unity, we can write the roots as

$$\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}.$$

The polynomial f is irreducible (for example using Eisenstein's criterion). Since it is also monic, it is the minimal polynomial of $\sqrt[3]{2}$, and

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

Now since $\sqrt[3]{2}$ and $i\sqrt{3}$ (or ζ_3) generate all the roots of f, the splitting field of f is

$$K = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3).$$

We finish by computing the degree of K over $\mathbb{Q}$. Clearly $i\sqrt{3}$ cannot belong to $\mathbb{Q}(\sqrt[3]{2})$ which is a subfield of $\mathbb{R}$, thus $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})]$ is at least 2. Since $i\sqrt{3}$ is a root of $X^2+3 \in \mathbb{Q}(\sqrt[3]{2})[X]$, this degree is exactly 2. By multiplicativity of the degrees, we get that

$$[K : \mathbb{Q}] = 6.$$

Using that ζ_3 is a root of $X^2 + X + 1$ stays irreducible over $\mathbb{Q}(\sqrt{2})$ gives the same result.

Equivalently, K is a splitting field for f over F if f splits over K and K is generated over F by the roots $\alpha_1, \dots, \alpha_k$ of f, that is $K = F(\alpha_1, \dots, \alpha_k)$.

If $f \in F[X]$ and f splits over the extension E of F, then E contains a unique splitting field for f, namely $F(\alpha_1, \dots, \alpha_k)$.

Here is a result on the degree of splitting fields. Note that the above example shows that this bound is tight.

Proposition 5.6. *If $f \in F[X]$ and $\deg f = n$, then f has a splitting field K over F with $[K : F] \leq n!$.*

Proof. First we may assume that $n \geq 1$, for if $n = 0$, then f is constant, and we take $K = F$ with $[K : F] = 1$.

Thus f has at least one root α_1, and by Theorem 5.1, there is an extension E_1 of F containing α_1. Since $f(\alpha_1) = 0$, the minimal polynomial $m_1(X)$ of α_1 divides $f(X)$, that is $f(X) = m_1(X)f'(X)$ for some $f'(X)$, and since $\deg f = n$, $\deg m_1(X) \leq n$, implying that $F(\alpha_1)/F$ has degree at most n.

We may then further write $f(X) = (X - \alpha_1)^{r_1}g(X)$ where $g(\alpha_1) \neq 0$ and $\deg g \leq n - 1$. If g is constant, then $f(X)$ has no other root than α_1, and its splitting field is $F(\alpha_1)/F$ whose degree is at most n which is indeed smaller than $n!$.

Now if g is non-constant, we can iterate on g the reasoning we did on f. Namely, we have that g has degree at least 1, and thus it has at least one root α_2. Invoking again Theorem 5.1, there is an extension of $F(\alpha_1)$ containing α_2 and the extension $F(\alpha_1, \alpha_2)$ has degree at most $n-1$ over $F(\alpha_1)$ (corresponding to the case where $r_1 = 1$). Thus we have

$$\begin{aligned}[F(\alpha_1, \alpha_2) : F] &= [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F] \\ &\leq (n-1)n.\end{aligned}$$

We can now continue inductively to reach that if $\alpha_1, \dots, \alpha_n$ are all the roots of f, then

$$[F(\alpha_1, \alpha_2, \dots, \alpha_n) : F] \leq n!.$$

□

If $f \in F[X]$ and f splits over E, then we may take any root α of f and adjoin it to F to get the extension $F(\alpha)$. More precisely:

Theorem 5.7. *If α and β are roots of the irreducible polynomial $f \in F[X]$ in an extension E of F, then $F(\alpha)$ is isomorphic to $F(\beta)$.*

Proof. If f is not monic, start by dividing f by its leading coefficient, so that we can assume that f is monic. Since f is monic, irreducible and $f(\alpha) = f(\beta) = 0$, f is the minimal polynomial of α and β, say of degree n. Now if $a \in F(\alpha)$, then a can be uniquely written as

$$a = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}.$$

The map

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1\beta + \dots + a_{n-1}\beta^{n-1}$$

defines a field isomorphism between $F(\alpha)$ and $F(\beta)$. □

When discussing field isomorphisms, one may want to emphasize the base field.

Definition 5.7. If E and E' are extensions of F, and $\iota : E \to E'$ is an isomorphism, we say that ι is an F-isomorphism if ι fixes F, that is, if

$$\iota(a) = a,\ a \in F.$$

Given a polynomial $f \in F[X]$, we have discussed its splitting field, namely the smallest field over which f splits. If F is $\mathbb{Q}$, $\mathbb{R}$ or more generally $\mathbb{C}$, not only we can find a splitting field for each polynomial, but we know that there is a field C with the property that any polynomial in $\mathbb{C}[X]$ splits over C, namely $C = \mathbb{C}$ itself.

We now would like to express this property in general, without having to assume that F is $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. Namely, for a general field F, we want an extension C of F such that any polynomial in $C[X]$ splits over C. We will later on add the requirement that this extension is algebraic.

Proposition 5.8. *If C is a field, the following conditions are equivalent.*

1. *Every non-constant polynomial $f \in C[X]$ has at least one root in C.*
2. *Every non-constant polynomial $f \in C[X]$ splits over C.*
3. *Every irreducible polynomial $f \in C[X]$ is linear.*

4. C has no proper algebraic extension.

Proof. We prove 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 4. $\Rightarrow$ 1.

1. $\Rightarrow$ 2. Take $f \in C[X]$ a non-constant polynomial. Since f has at least one root, we write $f = (X - \alpha_1)g$ for g some polynomial in $C[X]$. If g is constant, we are done since f splits. If g is non-constant, then again by assumption it has one root and $g = (X - \alpha_2)h$ for some h. We conclude by repeating inductively.

2. $\Rightarrow$ 3. Take $f \in C[X]$ which is irreducible, thus non-constant. By assumption it is a product of linear factors. But f is irreducible, so there can be only one such factor.

3. $\Rightarrow$ 4. Let E be an algebraic extension of C. Take $\alpha \in E$ with minimal polynomial f over C. Then f is irreducible and of the form $X - \alpha \in C[X]$ by assumption. Thus $\alpha \in C$ and $E = C$.

4. $\Rightarrow$ 1. Let f be a non-constant polynomial in $C[X]$, with root α. We can adjoin α to C to obtain $C(\alpha)$. But by assumption, there is no proper algebraic extension of C, so $C(\alpha) = C$ and $\alpha \in C$. Thus f has at least one root in C and we are done.

□

Definition 5.8. A field C as described in the above equivalent properties is said to be algebraically closed.

Examples 5.8. 1. The field $\mathbb{R}$ is not algebraically closed, since $X^2 + 1 = 0$ has not root in $\mathbb{R}$.

2. No finite field $\mathbb{F}$ is algebraically closed, since if $a_1, \ldots, a_n$ are all the elements of F, then the polynomial $(X - a_1) \ldots (X - a_n) + 1$ has no zero in $\mathbb{F}$.

3. The field $\mathbb{C}$ is algebraically closed, this is the fundamental theorem of algebra.

4. The field of all algebraic numbers is algebraically closed. (We will not prove this here, but for a proof that algebraic numbers in a field extension indeed form a field, see Corollary 5.11 below.)

We can embed an arbitrary field F in an algebraically closed field as follows.

Definition 5.9. An extension C of F is called an algebraic closure if C is algebraic over F and C is algebraically closed.

Examples 5.9. To get examples of algebraic closures, we thus need to start with known algebraically closed fields.

1. The field $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

2. The field of all algebraic numbers is the algebraic closure of $\mathbb{Q}$.

Note that C is minimal among algebraically closed extensions of F. Indeed, let us assume that there is an algebraically closed field K such that $C/K/F$. Let $\alpha \in C$ but $\alpha \notin K$ (it exists if we assume that $C \neq K$). Then α is algebraic over F, and consequently algebraic over K. But since $\alpha \notin K$, the minimal polynomial of α over K cannot contain the factor $X - \alpha$, which contradicts that K is an algebraically closed field.

We can prove the following theorems (we will omit the proof).

Theorem 5.9. *1. Every field F has an algebraic closure.*

2. Any two algebraic closures C and C' of F are F-isomorphic.

3. If E is an algebraic extension of F, C is an algebraic closure of F, and ι is an embedding of F into C. Then ι can be extended to an embedding of E into C.

Let us now prove the first transitivity property of field extensions. Several will follow later on in this chapter.

Proposition 5.10. *1. If E is generated over F by finitely many elements $\alpha_1, \ldots, \alpha_n$ algebraic over F, then E is a finite extension of F.*

2. **(Transitivity of algebraic extensions).** *If E is algebraic over K, and K is algebraic over F, then E is algebraic over F.*

Proof. 1. Set $E_0 = F$, $E_k = F(\alpha_1, \ldots, \alpha_k)$, $1 \leq k \leq n$, in particular $E_n = F(\alpha_1, \ldots, \alpha_n) = E$ by definition of E. Then $E_k = E_{k-1}(\alpha_k)$, where α_k is algebraic over F, and hence over E_{k-1}. Now $[E_k : E_{k-1}]$ is the degree of the minimal polynomial of α_k over E_{k-1}, which is finite. By multiplicativity of the degrees, we conclude that

$$[E : F] = \prod_{k=1}^{n} [E_k : E_{k-1}] < \infty.$$

2. Let $\alpha \in E$ with minimal polynomial

$$m(X) = b_0 + b_1 X + \ldots + b_{n-1} X^{n-1} + X^n$$

over K since by assumption α is algebraic over K. The coefficients b_i are in K and thus are algebraic over F. Set $L = F(b_0, b_1, \ldots, b_{n-1})$, by the first part, L is a finite extension of F. Therefore $m(X) \in L[X]$, α is algebraic over L, and $L(\alpha)$ is a finite extension of L. This gives us the following tower of field extensions:

$$L(\alpha)/L = F(b_0, b_1, \ldots, b_{n-1})/F.$$

By transitivity of the degrees, since $[L : F] < \infty$ and $[L(\alpha) : L] < \infty$, we get that $[L(\alpha) : F] < \infty$. We conclude since we know that all finite extensions are algebraic, and thus α is algebraic over F.

□

Corollary 5.11. *If E is an extension of F and A is the set of all elements in E that are algebraic over F, then A is a subfield of E.*

Proof. If $\alpha, \beta \in A$, then the sum, difference, product and quotient (if $\beta \neq 0$) of α and β belong to $F(\alpha, \beta)$, which is a finite extension of F by the first part of the above proposition. This is thus an algebraic extension since all finite extensions are, and thus $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and α/β are in A, proving that A is a field. □

5.3 Separability

If f is a polynomial in $F[X]$, we have seen above that we can construct a splitting field K for f over F, and K is such that all roots of f lie in it. We can thus study the multiplicity of the roots of f in K.

Definition 5.10. An irreducible polynomial $f \in F[X]$ is separable if f has no repeated roots in a splitting field. It is called inseparable otherwise. Note that if f is not necessarily irreducible, then we call f separable if each of its irreducible factors is separable.

For example $f(X) = (X-1)^2(X-2) \in \mathbb{Q}$ is separable, since its irreducible factors $X - 1$ and $X - 2$ are separable.

We start by computing a criterion to test if a polynomial has multiple roots.

Proposition 5.12. *Consider*

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$$

and its formal derivative

$$f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Then f has a repeated root in a splitting field if and only if the degree of the greatest common divisor of f and f' is at least 1.

Proof. Let us assume that f has a repeated root in its splitting field, say α. Then we can write

$$f(X) = (X-\alpha)^r h(X)$$

where $r \geq 2$ since we consider a repeated root. Now we compute the derivative of f:

$$f'(X) = r(X-\alpha)^{r-1}h(X) + (X-\alpha)^r h'(X)$$

and since $r - 1 \geq 1$, we have that $(X - \alpha)$ is a factor of both f and f'.

Conversely, let us assume that the greatest common divisor g of f and f' has degree at least 1, and let α be a root of g (in a splitting field). By definition of g, $X - \alpha$ is then a factor of both f and f'. We are left to prove that α is a repeated root of f. Indeed, if it were not the case, then $f(X)$ would be of the form $f(X) = (X - \alpha)h(X)$ where $h(\alpha) \neq 0$ and by computing the derivative, we would get (put $r = 1$ in the above expression for f') $f'(\alpha) = h(\alpha) \neq 0$ which contradicts the fact that $X - \alpha$ is a factor of f'. □

As a corollary of this result, we can exhibit two classes of separable polynomials.

Corollary 5.13. *1. Over a field of characteristic zero, every polynomial is separable.*

2. Over a field F of prime characteristic p, an irreducible polynomial f is inseparable if and only if f' is the zero polynomial (equivalently f is in $F[X^p]$).

Proof. 1. Without loss of generality, consider f an irreducible polynomial in $F[X]$, where F is of characteristic zero. If f is a polynomial of degree n, then its derivative f' is of degree less than n, and it cannot possibly be the zero polynomial. Since f is irreducible, the greatest common divisor of f and f' is either 1 or f, but it cannot be f since f' is of smaller degree. Thus it is 1, and f is separable by the above proposition.

2. We now consider the case where F is of characteristic p. As above, we take f an irreducible polynomial of degree n in $F[X]$ and compute its derivative f'. If f' is non-zero, we can use the same argument. But f' could also be zero, in which case the greatest common divisor of f and f' is actually f, and by the above proposition, f has a multiple root and is then not separable. That $f' = 0$ means that $f \in F[X^p]$ since we work in characteristic p.

□

Example 5.10. Polynomials over $\mathbb{R}[X]$ and $\mathbb{Q}[X]$ are separable.

Another class of separable polynomials are polynomials over finite fields, but this asks a little bit more work.

Lemma 5.14. *Let F be a finite field of characteristic p. Consider the map*

$$f : F \to F, \; f(\alpha) = \alpha^p.$$

Then f is an automorphism (called the Frobenius Automorphism). In particular, we have for all $\alpha \in F$ that

$$\alpha = \beta^p$$

for some $\beta \in F$.

Proof. We have that f is a ring automorphism since

$$\begin{aligned} f(1) &= 1 \\ f(\alpha+\beta) &= (\alpha+\beta)^p = \alpha^p + \beta^p = f(\alpha) + f(\beta) \\ f(\alpha\beta) &= (\alpha\beta)^p = \alpha^p\beta^p = f(\alpha)f(\beta). \end{aligned}$$

The second set of equalities uses the binomial expansion modulo p. Now f is a monomorphism since F is a field, and an injective map from a finite set to itself is necessarily surjective. □

Proposition 5.15. *Every polynomial is separable over a finite field F (of prime characteristic).*

Proof. Suppose that f is an irreducible polynomial which, by contradiction, has multiple roots in a splitting field. Using the criterion of the corollary, $f(X)$ must be in $F[X^p]$, namely

$$f(X) = a_0 + a_1 X^p + \cdots + a_n X^{np},\ a_i \in F.$$

Using the bijectivity of the Frobenius automorphism, we can write $a_i = b_i^p$, yielding

$$(b_0 + b_1 X + \cdots + b_n X^n)^p = b_0^p + b_1^p X^p + \cdots + b_n^p X^{np} = f(X)$$

which contradicts the irreducibility of f. □

Definition 5.11. If E is an extension of F and $\alpha \in E$, then α is said to be separable over F if α is algebraic over F and its minimal polynomial $\mu_{\alpha,F}$ is a separable polynomial. If every element of E is separable over F, we say that E is a separable extension of F or that E/F is separable.

Examples 5.11. 1. Typical examples of separable extensions are finite fields and number fields.

2. If F is a field with algebraic closure C, then C contains a smallest field containing all finite separable extensions of F, called the separable closure of F. It is a separable extension of F.

Here is a first result on how separability behaves in a tower of extensions.

Lemma 5.16. *If $E/K/F$ and E is separable over F, then K is separable over F and E is separable over K.*

Proof. K/F **is separable.** Since K is a subfield of E, every element $\beta \in K$ belongs to E, and every element of E is separable over F by assumption.

E/K **is separable.** Take $\alpha \in E$. Since E is separable over F, it is in particular algebraic over F and we may consider the minimal polynomial $\mu_{\alpha,F}$ of α over F. Denote by $\mu_{\alpha,K}$ the minimal polynomial of α over K, we have

$$\mu_{\alpha,K} \mid \mu_{\alpha,F}.$$

Since $\mu_{\alpha,F}$ has no repeated root, neither has $\mu_{\alpha,K}$, and E/K is separable. □

The converse is also true, and gives the transitivity of separable extensions: If K/F and E/K are separable, then E/F is separable.

It is less easy to construct inseparable extensions, but here is a classical example.

Example 5.12. Let $\mathbb{F}_p$ denote the finite field of integers modulo p. Consider the field $F = \mathbb{F}_p(t)$ of rational functions in t with coefficients in the finite field with p elements $\mathbb{F}_p$. We get a field extension of E/F by adjoining to F a root of the polynomial $X^p - t$ (one has to check that $X^p - t$ is irreducible over $\mathbb{F}_p[t]$). The extension E/F is inseparable since

$$X^p - t = X^p - (\sqrt[p]{t})^p = (X - \sqrt[p]{t})^p,$$

which has multiple roots.

Let E/F be a separable extension of F and let C be an algebraic closure of E. We next count the number of embeddings of E in C that fix F, that is, the number of F-monomorphisms of E into C. We start with a lemma.

Lemma 5.17. *Let $\sigma : E \to E$ be an F-monomorphism and assume that $f \in F[X]$ splits over E. Then σ permutes the roots of f, namely, if α is a root of f in E then so is $\sigma(\alpha)$.*

Proof. Write $f(X)$ as

$$f(X) = b_0 + b_1X + \cdots + b_nX^n,\ b_i \in F.$$

If α is a root of f in E, then

$$f(\alpha) = b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0.$$

Apply σ to the above equation, and use that σ is a field homomorphism that fixes F to get

$$b_0 + b_1\sigma(\alpha) + \cdots + b_n\sigma(\alpha)^n = 0,$$

showing that $\sigma(\alpha)$ is a root. □

Theorem 5.18. *Let E/F be a finite separable extension of degree n, and let σ be an embedding of F into an algebraic closure C. Then σ extends to exactly n embeddings of E in C. Namely, there are exactly n embeddings τ of E into C, such that the restriction $\tau|_F$ of τ to F coincides with σ. In particular, taking σ to be the identity on F, there are exactly n F-monomorphisms of E into C.*

Proof. We do a proof by induction. If $n = 1$, then $E = F$ and σ extends to exactly 1 embedding, namely itself.

We now assume that $n > 1$ and choose $\alpha \in E$, $\alpha \notin F$. Let $f = \mu_{\alpha,F}$ be the minimal polynomial of α over F of degree say r. It is irreducible and separable (E/F is separable by assumption). In order to use the induction hypothesis, we need to split the field extension E/F, which we do by considering the field extension $F(\alpha)$, which satisfies

$$E/F(\alpha)/F,\ [E : F(\alpha)] = n/r,\ [F(\alpha) : F] = r.$$

We first take care of the extension $F(\alpha)/F$. Let σ be an embedding of F into C, and define the polynomial $g = \sigma(f)$, where σ is applied on all the coefficients of f. The polynomial g inherits the property of being irreducible and separable from f. Let β denotes a root of g. We can thus define a unique isomorphism

$$F(\alpha) \to (\sigma(F))(\beta),\ b_0 + b_1\alpha + \ldots + b_r\alpha^r \mapsto \sigma(b_0) + \sigma(b_1)\beta + \ldots + \sigma(b_r)\beta^r$$

and restricted to F it indeed coincides with σ. This isomorphism is defined by the choice of β, and there are exactly r choices for it, corresponding to the r roots of g (note that this is here that the separability of g is crucial). For each of these r isomorphisms, using the induction hypothesis on $[E : F(\alpha)] = n/r < n$, we can extend them to exactly n/r embeddings of E into C. This gives us a total of $n/r \cdot r$ distinct embeddings of E into C extending σ. We conclude by noting that we cannot have more than n such embeddings. □

We conclude by giving a nice description of finite separable field extensions.

Theorem 5.19. (Theorem of the Primitive Element). *If E/F is a finite separable extension, then*

$$E = F(\gamma)$$

for some $\gamma \in E$. We say that γ is a primitive element of E over F.

Proof. Since we have not studied finite fields yet, let us assume that F is an infinite field. (If you have already studied finite fields, then you know we can take γ to be any generator of the cyclic group $E^\times$).

We proceed by induction on the degree n of the extension E/F. If $n = 1$, then $E = F$ and we can take any element for α.

Let us thus assume $n > 1$, the assumption true up to $n - 1$, and say the degree of E/F is n. Choose $\alpha \in E$ but not in F. We now look at the field extension $E/F(\alpha)$. By induction hypothesis, there is a primitive element β such that

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

We are now going to prove that there exists a $c \in F$ such that

$$E = F(\alpha + c\beta),$$

that is

$$\gamma = \alpha + c\beta$$

will be the primitive element. We will show that it is enough to take $c \notin S$, where S is a finite subset of F defined as follows: let f be the minimal polynomial of α over F, and let g be the minimal polynomial of β over F, the exceptional set S consists of all $c \in F$ such that

$$c = \frac{\alpha' - \alpha}{\beta - \beta'}$$

for α' a root of f and β' a conjugate of β (we extend $F(\alpha, \beta)$ to a field L in which f and g both split to be able to speak of all their roots).

To show that γ is primitive for $c \notin S$, it is enough to prove that $F(\alpha + c\beta)$ contains β and $\alpha = \gamma - c\beta$ (clearly the reverse inclusion holds: $F(\alpha + c\beta) \subseteq F(\alpha, \beta)$). To this end, it is enough to show that the minimal polynomial of β over $F(\gamma)$ cannot have degree greater or equal to 2, implying that β is in $F(\gamma)$.

Note first that if we take the polynomial $h(X)$ defined by

$$h(X) = f(\gamma - cX) \in F(\gamma)[X]$$

and evaluate it in β, we get

$$h(\beta) = f(\gamma - c\beta) = f(\alpha + c\beta - c\beta) = 0.$$

Thus β is a root of h and the minimal polynomial of β over $F(\gamma)$ divides both g and h, so we are done if we show that the greatest common divisor of g and h in $F(\gamma)[X]$ cannot have degree greater or equal to 2.

Suppose the greatest common divisor does have degree≥ 2. Then g and h have as common root in L not only β, but also $\beta' \neq \beta$ in L. This is where we use the separability of g, since otherwise β could be a root with multiplicity 2. Then

$$f(\gamma - c\beta') = 0 \Rightarrow \gamma - c\beta' = \alpha'$$

for some root α' of f, which can be rewritten as

$$\alpha + c\beta - c\beta' = 0 \Rightarrow c = \frac{\alpha' - \alpha}{\beta - \beta'}$$

which is exactly what was ruled out by choosing $c \notin S$. □

Definition 5.12. A simple extension is a field extension which is generated by the adjunction of a single element.

Thus the primitive element Theorem above provides a characterization of the finite extensions which are simple.

Example 5.13. Number fields are simple extensions.

5.4 Normality

So far, we have considered two properties of field extensions (both of them being transitive): being algebraic and separable. We now introduce a third property, which is not transitive, the one of being normal.

Definition 5.13. An algebraic extension E/F is normal if every irreducible polynomial over F that has at least one root in E splits over E. If we call the other roots of this polynomial the conjugates of α, we can rephrase the definition by saying that if $\alpha \in E$, then all conjugates of α over F are in E.

Note that this definition assumes that we start with an algebraic extension.

Example 5.14. Consider the field extension $E = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. The roots of the irreducible polynomial $f(X) = X^3 - 2$ are

$$\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2},$$

where ζ_3 is a primitive 3rd root of unity (for example $\zeta_3 = e^{2\pi i/3}$). Thus E is not a normal extension.

We can give another characterization in terms of monomorphisms of E.

Theorem 5.20. *The finite extension E/F is normal if and only if every F-monomorphism of E into an algebraic closure C is actually an F-automorphism of E. (Finite could be replaced by algebraic, which we will not prove).*

Proof. If E/F is normal, then an F-monomorphism of E into C must map each element of E to one of its conjugates (as is the case in the proof of Lemma 5.17). Thus $\tau(E) \subseteq E$, but $\tau(E)$ is an isomorphic copy of E and thus has the same degree as E and $E = \tau(E)$, showing that τ is indeed an F-automorphism of E.

Conversely, consider $\alpha \in E$ and let β be a conjugate of α over F. There exists an F-monomorphism of E into C that carries α to β (the construction is given in the proof of Theorem 5.18). If all such embeddings are F-automorphisms of E, that means β must be in E, and we conclude that E/F is normal. □

Here is another characterization of normal extensions in terms of splitting fields.

Theorem 5.21. *The finite extension E/F is normal if and only if E is a splitting field for some polynomial f in $F[X]$.*

Proof. Let E/F be a finite normal extension of degree n, and let $\alpha_1, \dots, \alpha_n$ be a basis for E over F. Consider for each α_i its minimal polynomial f_i over F. By definition of normal extension, since f_i has a root in E, then f_i splits over E, and so does the polynomial

$$f = f_1 \cdots f_n.$$

To prove that E is a splitting field, we are left to prove it is the smallest field over which f splits. This is here that we understand why we take such an f. If f were to split over a subfield K, that is K such that

$$F \subset K \subset E$$

then each $\alpha_i \in K$, and $K = E$ (this is a conclusion we cannot reach if we take for f only one f_i or a subset of them). This proves that E is a splitting field for f over F.

Conversely, let E be a splitting field for some f over F, whose roots are denoted by $\alpha_1, \dots, \alpha_n$. Let τ be an F-monomorphism of E into an algebraic closure, that is τ takes each α_i into another root of f.

Since E is a splitting field for f, we have

$$F(\alpha_1, \ldots, \alpha_n) = E$$

and $\tau(E) \subset E$. Thus since E and $\tau(E)$ have same dimension, we get that

$$\tau(E) = E$$

and τ is actually an automorphism of E, and by the above theorem, we conclude the E/F is normal. □

As a corollary, we see how a subextension inherits the property of normality.

Corollary 5.22. *Let $E/K/F$ be a finite extension ($[E : F] < \infty$). If E/F is normal, so is E/K.*

Proof. Since E/F is normal, E is a splitting field for some polynomial $f \in F[X]$, that is E is generated over F by the roots of f. Since $f \in F[X] \subset K[X]$, f can also be seen as a polynomial in $K[X]$ and E is generated over K by the roots of f, and again by the above theorem, E/K is normal. □

There is no reason for an arbitrary field extension E/F to be normal. However, if E/F is finite (or more generally algebraic) one can always embed it in normal extension.

Definition 5.14. Let E/F be an algebraic extension. The normal closure of E/F is an extension field N of E such that N/E is normal and N is minimal with this property.

If E/F is finite, we can see it as follows: E is finitely generated over F, so it can be written as $E = F(\alpha_1, \ldots, \alpha_n)$. Let now K be a normal extension of F that contains E:

$$K/E/F.$$

Since K is normal, it must contain not only all the α_i but also all their conjugates. Let f_i be the minimal polynomial of α_i, $i = 1, \ldots, n$. Then we can rephrase the last statement and say that K must contain all the roots of f_i, $i = 1, \ldots, n$. Consider the polynomial

$$f = f_1 \cdots f_n.$$

Then K must contain the splitting field N for f over F. But N/F is normal, so N must be the smallest normal extension of F that contains E. Thus N is a normal closure of E over F.

The main definitions and results of this chapter are

- **(3.1).** Definitions of: field extension, minimal polynomial, degree of a field extension, field homomorphism, algebraic, transcendental. That the degree is multiplicative.
- **(3.2).** Definitions of: to split, splitting field, algebraically closed, algebraic closure. Transitivity of algebraic extensions.
- **(3.3).** Definition of separability, typical separable extensions, separability in extension towers, number of embeddings into an algebraic closure, primitive element Theorem.
- **(3.4).** Definition of normality, two equivalent characterizations of normal extensions.

Chapter 6

Exercises for Field Theory

Exercises marked by (*) are considered difficult.

6.1 Field extension and minimal polynomial

Exercise 88. 1. For which of the following $p(X)$ do there exist extensions $K(\alpha)$ of K for which α has minimal polynomial $p(X)$?

- $p(X) = X^2 - 4$, $K = \mathbb{R}$.
- $p(X) = X^2 + 1$, $K = \mathbb{Z}_5$ (integers modulo 5).
- $p(X) = X^3 + 2$, $K = \mathbb{Q}$.

In the case where you obtain a field extension, what is the degree of the extension?

2. Find an irreducible polynomial of degree 2 over the integers modulo 2. Use it to construct a field with 4 elements. Describe the obtained field.

Answer.

1. $p(X) = X^2 - 4 = (X-2)(X+2)$, it is not irreducible so it cannot be a minimal polynomial. Then $p(X) = X^2 + 1 = (X-2)(X+2)$ modulo 5, so it is not irreducible, and cannot be a minimal polynomial. Finally $X^3 + 2$ is irreducible, monic, we obtain the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, it is of degree 3.

2. Take the polynomial $X^2 + X + 1$, it has no root modulo 2 and is thus irreducible. We can construct a field using the generic construction that we know. The field $\mathbb{Z}_2[X]/(X^2+X+1)$ contains a root α of the polynomial, it is a field containing 4 elements. Indeed, it is of degree 2 (degree of the minimal polynomial), and a basis is given by $\{1, \alpha\}$, thus every element

can be written as $a + b\alpha$, $a, b \in \mathbb{Z}_2$. That makes 4 possible elements, and the field is described by

$$\mathbb{Z}_2[X]/(X^2 + X + 1) \simeq \{a + b\alpha, a, b \in \mathbb{Z}_2\}.$$

Exercise 89. 1. Show that $\mathbb{C}/\mathbb{R}$ is an algebraic extension.

2. Compute the degree of the following extensions: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}+\sqrt{2})/\mathbb{Q}$.

3. Let $E = \mathbb{Q}(\sqrt{2})$ and $F = \mathbb{Q}(i\sqrt{2})$. Show that -1 is a sum of 2 squares in F. Deduce that E and F are not isomorphic.

Answer.

1. $\mathbb{C}/\mathbb{R}$ is an extension of degree 2 (a $\mathbb{R}$-basis is $\{1, i\}$), it is thus finite, thus algebraic.

2. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (a $\mathbb{Q}$-basis is $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$), $[\mathbb{Q}(\sqrt{3} + \sqrt{2}) : \mathbb{Q}] = 4$ (a $\mathbb{Q}$-basis is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, because $\mathbb{Q}(\sqrt{3} + \sqrt{2}) = \mathbb{Q}(\sqrt{3}, \sqrt{2})$).

3. In F, we have that $(i\sqrt{2})^2 + 1^2 = -1$. Since both fields have the same degree and knowing that a field homomorphism is always injective, we try to build a ring homomorphism f from F to E. Thus

$$f((i\sqrt{2})^2 + 1^2) = f(-1) \Rightarrow f((i\sqrt{2})^2) + f(1) = -f(1)$$

since f is a ring homomorphism, furthermore, it must send $f(1)$ to 1, thus we must have

$$f((i\sqrt{2}))^2 = -2$$

that is there must be an element of E whose square is negative which is not possible.

Exercise 90. Consider the extension $\mathbb{C}/\mathbb{R}$. What are all the $\mathbb{R}$-automorphisms of $\mathbb{C}$? Justify your answer.

Answer. Write an element $x \in \mathbb{C}$ as $x = a + ib$, $a, b \in \mathbb{R}$, and let σ be an $\mathbb{R}$-automorphisms. Thus

$$\sigma(x) = \sigma(a) + \sigma(i)\sigma(b) = a + \sigma(i)b$$

using for the first equality the property of ring homomorphism, and for the second one that σ fixes $\mathbb{R}$. Thus $\sigma(x)$ is determined by $\sigma(i)$. Since $i^2 = -1$, we have that $\sigma(i^2) = \sigma(-1)$, that is

$$\sigma(i)^2 + 1 = 0.$$

Thus either $\sigma(i) = i$ or $\sigma(i) = -i$, which are the only two possible $\mathbb{R}$-automorphims of $\mathbb{C}$.

Exercise 91. Prove that if $[K(u):K]$ is odd, then $K(u) = K(u^2)$.

Answer. We first notice that $K(u^2) \subset K(u)$, thus

$$[K(u):K] = [K(u):K(u^2)][K(u^2):K].$$

Since u is a root of the polynomial $X^2 - u^2$ in $K(u^2)[X]$, we have that $[K(u):K(u^2)] \leq 2$, and it cannot be 2 because $[K(u):K]$ is odd, thus $[K(u):K(u^2)] = 1$ and the conclusion follows.

6.2 Splitting fields and algebraic closures

Exercise 92. What is the splitting field of the following polynomials?

1. $f(x) = (x^2-3)(x^3+1) \in \mathbb{Q}(x)$.
2. $f(x) = x^2+x+1 \in \mathbb{F}_2[x]$.

Answer.

1. We have that $f(X) = (x-\sqrt{3})(x+\sqrt{3})(x-1)(x^2+x+1)$, thus the splitting field of f must contain $\sqrt{3}$ and ζ_3, the primitive third root of unity. This then must be $\mathbb{Q}(i, \sqrt{3})$.
2. We have that x^2+x+1 is irreducible over $\mathbb{F}_2$, we can construct $\mathbb{F}_4$ as $\mathbb{F}_2[x]/(f(x))$, that is $\mathbb{F}_4 \simeq \mathbb{F}_2(w)$ where $w^2+w+1 = 0$. Thus the splitting field of f is $\mathbb{F}_4$.

6.3 Separability

6.4 Normality

Exercise 93. Show that $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ is not normal.

Answer. The roots of x^3-5 are $\sqrt[3]{5}, \zeta_3\sqrt[3]{5}, \zeta_3^2\sqrt[3]{5}$, where ζ_3 denote a primite 3rd root of unity. Since $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ is totally real, it cannot contain the complex roots.

Exercise 94. Are the following claims true or false? Justify your answer.

1. Every polynomial splits over some field.
2. The polynomial x^3+5 is separable over $\mathbb{F}_7$.
3. Every finite extension is normal.
4. Every separable extension is normal.
5. Every finite normal extension is a splitting field for some polynomial.

6. A reducible polynomial cannot be separable.

Answer.

1. This is true, for every root of the polynomial, there is a field that will contain this root, so that we can build a field extension containing all the roots (if the polynomial has coefficients in $\mathbb{R}$, then one can use $\mathbb{C}$, but $\mathbb{C}$ will not work if the polynomial has coefficients in a finite field).
2. True since $\mathbb{F}_7$ is a finite field.
3. False, $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ is finite but not normal.
4. False, $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ is separable (because $\mathbb{Q}$ is of characteristic zero) but not normal.
5. True, we proved this.
6. False, when a polynomial is reducible, the definition of separability applies on its irreducible factors, which may or may not be separable.

Exercise 95. True/False.

Q1. Every field has non-trivial extensions.

Q2. Every field has non-trivial algebraic extensions.

Q3. Extensions of the same degree are isomorphic.

Q4. Every algebraic extension is finite.

Q5. Every algebraic extension of $\mathbb{Q}$ is finite.

Q6. Every extension of a finite field is finite.

Q7. The polynomial $X^3 + 5$ is separable over Z_7 (= integers modulo 7).

Q8. Every finite extension is normal.

Q9. Every separable extension is normal.

Q10. Every K-monomorphism is a K-automorphism.

Q11. Every extension of a field of characteristic 0 is normal.

Answer.

Q1. That's true! We are not speaking of algebraic extensions necessarily. Even if you take $\mathbb{C}$, you can for example get function fields over $\mathbb{C}$ by adding an indeterminate.

Q2. We know that one of the characterizations of algebraically closed fields is that they have no non-trivial algebraic extensions! So that is one counter example.

Q3. False! It's the other way round: if two extensions are isomorphic, then they have the same degree.

Q4. False, it is the other way round! If an extension is finite, it is algebraic. If it is algebraic it does not have to be finite (take an algebraic closure).

Q5. Still false. Taking $\mathbb{Q}$ as the base field does not change anything to the problem. The same counter example as in the previous question holds: you can take an algebraic closure of $\mathbb{Q}$, it is algebraic and infinite.

Q6. This is still false! You can build a function field as a counter example.

Q7. It is true. We have proved this result in general for fields of characteristic zero and finite fields.

Q8. It's false! There is no connection between both concepts. For example, we know that $\mathbb{Q}(\alpha)$ with $\alpha^3 = 2$ is finite and not normal.

Q9. It is false! There is no connection, you can take as above $\mathbb{Q}(\alpha)$ with $\alpha^3 = 2$, it is separable and not normal.

Q10. This is false! For a counter example, take any extension which is not normal. You'll find a K-monomorphism which is not a K-automorphism.

Q11. This is wrong! Imagine this were true, then all number fields would be normal, this is surely not the case!!