MA3D5 Galois Theory

Daan Krammer

May 13, 2009

Contents

1 Symmetric functions

1.1 Reminders on rings

Rings. All our rings are commutative with one. Thus, a **ring** is a set A together with two specified elements $0 = 0_A \in A$, $1 = 1_A \in A$ and two binary operations $A \times A \to A$ written $(a, b) \mapsto a + b$ and $(a, b) \mapsto ab$ with the following properties, for all $a, b, c \in A$:

$$\begin{gathered} a+b=b+a, \qquad (a+b)+c=a+(b+c), \qquad a+0=a, \qquad (1) \\ ab=ba, \qquad (ab)c=a(bc), \qquad a\cdot 1=a, \\ a(b+c)=ab+ac. \end{gathered}$$

Note that (1) says that $(A, +, 0)$ is an abelian group.

Zero divisors and integral domains. An **integral domain** is a ring A such that for all $a, b \in A$, if $ab = 0$ then $a = 0$ or $b = 0$; and such that $0 \neq 1$.

A nonzero element a of a ring A is called **zero divisor** if $ab = 0$ for some $b \in A$. Thus, an integral domain is the same as a ring without zero divisors, such that $0 \neq 1$.

Units and fields. An element a of a ring A is called **invertible** or a **unit** if there exists $b \in A$ such that $ab = 1$. If A is a ring, we write $A^\times$ for the set of units in A. Then $(A^\times, \cdot, 1)$ is an abelian group. A **field** is a ring in which all nonzero elements are invertible, and $0 \neq 1$. Equivalently, it is a ring A such that $A^\times = A \smallsetminus \{0\}$.

Irreducible. An element a in a ring A is called **irreducible** if it is not a unit, and for all $b, c \in A$ such that $a = bc$ one has that b or c is a unit.

Ring homomorphisms. Let A, B be rings. A map $f \colon A \to B$ is a **ring homomorphism** if $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ for all $a, b \in A$ and $f(1_A) = 1_B$.

Polynomials. Let A be a ring and choose a symbol, say, X. We shall define a new ring $A[X]$. The elements of $A[X]$ are called **polynomials** over A in one variable X and $A[X]$ is called the polynomial ring.

An element of $A[X]$ is a sequence $(a_0, a_1, \ldots)$ of elements of A with only finitely many nonzero entries. An alternative and more usual notation is

$$(a_0, a_1, \ldots) = a_0 + a_1X + a_2X^2 + \cdots = \sum_{k\geq 0} a_kX^k.$$

We define addition and multiplication on $A[X]$ by

$$\begin{aligned} (a_0, a_1, \ldots) + (b_0, b_1, \ldots) &= (a_0 + b_0, a_1 + b_1, \ldots), \\ (a_0, a_1, \ldots)(b_0, b_1, \ldots) &= (c_0, c_1, \ldots) \end{aligned}$$

where $c_n = \sum_{k=0}^{n} a_k\, b_{n-k}$. In the usual notation:

$$\sum a_k X^k + \sum b_k X^k = \sum (a_k + b_k)\, X^k, \qquad \big(\sum a_k X^k\big)\big(\sum b_k X^k\big) = \sum c_k\, X^k$$

with c_n as before.

Let $f = \sum_k a_k X^k \in A[X]$. The elements $a_i \in A$ are called the **coefficients** of f. The **degree** $\deg f$ of f is the greatest $n \geq 0$ such that $a_n \neq 0$. The degree of the zero polynomial is defined to be $-\infty$. Note that nonzero constant polynomials have degree 0. If f is of degree n then a_n is called the **leading coefficient** and $a_n X^n$ the **leading term** of f. We call f **monic** if its leading term is 1.

There is an injective ring homomorphism $f \colon A \to A[X]$ defined by $f(a) = (a, 0, 0, 0, \ldots)$ in the unusual notation. We usually identify $f(a)$ with $a \in A$. The elements of $f(A)$ are called the constant polynomials in $A[X]$.

Examples. Every field is an integral domain, and every integral domain is a ring:

$$\{\text{fields}\} \subset \{\text{integral domains}\} \subset \{\text{rings}\}.$$

Theorem 2: division with remainder for polynomials. Let $f, g \in K[X]$ be polynomials over a field K with $g \neq 0$. Then there are unique $q, r \in K[X]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.

Proof. Existence. There exist $q, r \in K[X]$ such that $f = gq + r$ because one can put $q = 0$, $r = f$. Choose now q, r such that r has minimal degree and write $\deg(g) = \ell$, $\deg(r) = m$. We claim that $m < \ell$. Suppose that on the contrary $m \geq \ell$ and write $g = \sum_k a_k X^k$, $r = \sum_k b_k X^k$. Put

$$r_1 = r - g\, b_m\, a_\ell^{-1}\, X^{m-\ell}, \qquad q_1 = q + b_m\, a_\ell^{-1}\, X^{m-\ell}.$$

Then $f = g_1 q + r_1$ but $\deg(r_1) < \deg(r)$, contradicting the minimality of $\deg(r)$. This proves that $\deg(r) < \deg(g)$ and finishes the proof of the existence.

Uniqueness. Let (q_i, r_i) (for $i \in \{1, 2\}$) both satisfy the conditions of the proposition. Then $g \mid gq_1 - gq_2 = (f - r_1) - (f - r_2) = r_2 - r_1$ and $\deg(r_2 - r_1) < \deg(g)$. This implies $r_1 = r_2$ and thus proves uniqueness. □

1.2 Exercises

(1.1) Prove that every field is an integral domain.

(1.2) Give an example of a ring which is not an integral domain. Give an example of an integral domain which is not a field. Give an example of a field.

(1.3) Let A be a ring. Prove that $A[X]$ is a ring. What are 0 and 1 in $A[X]$?

(1.4) Explicitly divide $X^5 - X^3$ by $X^2 + 2$ with remainder. Also divide X^5 by $X^3 + 2X + 1$.

(1.5) Let $f\colon A \to B$ be a ring homomorphism.

(a) Prove that $f(0_A) = 0_B$.

(b) Prove that f is injective if and only if $f^{-1}(0_B) = \{0_A\}$.

(c) Prove that if A is a field and B is nonzero, then f is injective.

(1.6) Prove that every finite integral domain is a field.

1.3 Solving by radicals

Let K be a field and $f \in K[X]$. If $\alpha \in K$ is such that $f(\alpha) = 0$ then we call α a **zero** or a **root** of f.

Definition 3. A field K is **algebraically closed** if every nonconstant polynomial $f \in K[X]$ has a root in K.

So $\mathbb{R}$ is not algebraically closed (choose $f = X^2 + 1$).

Theorem 4. The field $\mathbb{C}$ of complex numbers is algebraically closed. □

This cannot be proved here. Clearly the proof needs some analysis, because the *definition* of $\mathbb{R}$ and $\mathbb{C}$ is analytic. The most common proof belongs to complex analysis and uses the Cauchy residue theorem.

Exercise 6.19 outlines an almost entirely algebraic proof. The only analytic part of it is the knowledge that every polynomial $f \in \mathbb{R}[X]$ of odd degree has a real zero.

Lemma 5. Let K be an algebraically closed field. Let $f \in K[X]$ be monic of degree n. Then there exist $\alpha_1, \dots, \alpha_n \in K$ such that

$$f = \prod_{i=1}^{n} (X - \alpha_i). \tag{6}$$

Moreover, $\alpha_1, \dots, \alpha_n$ are unique up to reordering.[1]

Proof. Existence. Induction on n. It's true for $n = 0$. Let $n > 0$. As K is algebraically closed, there exists $\alpha_n \in K$ such that $f(\alpha_n) = 0$. By division with remainder (theorem 2) we can write

$$f = (X - \alpha_n) \cdot g + r \tag{7}$$

with $g, r \in K[X]$ and $\deg r < \deg(X - \alpha_n) = 1$. So r is constant. Plugging α_n in for X in (7) gives $0 = f(\alpha_n) = r(\alpha) = r$. So $r = 0$ and $f = (X - \alpha_n) \cdot g$. By the induction hypothesis, we can write $g = \prod_{i=1}^{n-1} (X - \alpha_i)$ and we find (6).

Uniqueness. Induction on n. It's true for $n = 0$. Let $n > 0$ and assume

$$\prod_{i=1}^{n} (X - \alpha_i) = \prod_{i=1}^{n} (X - \beta_i). \tag{8}$$

[1] That is, if also $f = \prod_{i=1}^{n} (X - \beta_i)$ with $\beta_i \in K$ then there exists $\pi \in S_n$ such that $\beta_i = \alpha_{\pi(i)}$ for all i.

Choose here $X = \alpha_n$ to obtain $\prod_{i=1}^{n}(\alpha_n - \beta_i)$. So there exists i such that $\alpha_n = \beta_i$. After reordering the β_j we may assume that $\alpha_n = \beta_n$. Dividing (1.19) by $X - \alpha_n$ yields $\prod_{i=1}^{n-1}(X - \alpha_i) = \prod_{i=1}^{n-1}(X - \beta_i)$. By the induction hypothesis, $\beta_1, \ldots, \beta_{n-1}$ is a reordering of $\alpha_1, \ldots, \alpha_{n-1}$. Therefore, $\beta_1, \ldots, \beta_n$ is a reordering of $\alpha_1, \ldots, \alpha_n$. □

Note that in lemma 118 the α_i are not required to be distinct.

If $\alpha, \beta \in K$, $n > 0$ are such that $\alpha^n = \beta$ then we say that α is a **root** or **radical** of β.

Definition 9. Let K be a field. A subfield $L \subset K$ is called **radically closed** in K if for all $\alpha \in K$, $n > 0$, if $\alpha^n \in L$ then $\alpha \in L$.

In words, all radicals in K of elements of L are again in L.

If K is a field and $A \subset K$ any subset then there clearly exists a smallest radically closed subfield L of K containing A. Indeed, it is the intersection of all radically closed subfields of K containing A. We say that L is the **radical closure** in K of A.

A polynomial of degree (respectively) $2, 3, 4, 5$ is called (respectively) a quadric, cubic, quartic, quintic.

Example 10. You know that the roots of a quadric $aX^2 + bX + c$ are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{11}$$

The expression (11) is obtained from a, b, c and field operations $(+, -, \times, \div)$ and radicals. More precisely, the expression (11) is in the radical closure of $\{a, b, c\}$.

Definition 12. Let K be an algebraically closed field and let $f \in K[X]$. We say that f is **solvable** or **solvable by radicals** if the radical closure of the set of coefficients of f contains all roots in K of f.

So example 10 shows that every quadric is solvable. In this chapter, we prove that all cubics and quartics are solvable. Later on we prove that some (most) quintics are not.

1.4 Symmetric polynomials

Let A be a ring and consider $A[T_1, \ldots, T_n]$, the ring of polynomials over A in n variables.

Definition 13. The kth **elementary symmetric function** $\sigma_k \in A[T_1, \ldots, T_k]$ is defined by

$$\sigma_k = \sum_{1 \le i_1 < \cdots < i_k \le n} \prod_{j=1}^{k} T_{i_j}. \qquad \square$$

Examples:

$$\sigma_0 = 1 = \text{a single choice of the empty product,}$$

$$\sigma_1 = T_1 + \cdots + T_n, \qquad \sigma_2 = \sum_{1\le i<j\le n} T_i\,T_j, \qquad \sigma_n = T_1 \cdots T_n.$$

It is clear that

$$\prod_{i=1}^{n} (X + T_i) = \sum_{k=0}^{n} \sigma_k\, X^{n-k}.$$

The monic polynomial with roots $T_1, \ldots, T_n$ is therefore

$$\prod_{i=1}^{n} (X - T_i) = \sum_{k=0}^{n} (-1)^k \sigma_k\, X^{n-k}.$$

Definition 14. A polynomial $f \in A[T_1, \ldots, T_n]$ is called **symmetric** if $f = f\big(u(T_1), \ldots, u(T_n)\big)$ for all permutations u of $\{T_1, \ldots, T_n\}$.

It is clear that, as the name already suggests, the elementary symmetric polynomials σ_k are symmetric.

Remark 15. Let us say a bit more about definition 14.

Let $U = \mathrm{Sym}(\{T_1, \ldots, T_n\})$ be the symmetric group on $\{T_1, \ldots, T_n\}$, also known as the group of permutations of $\{T_1, \ldots, T_n\}$ (see **). For $f \in A[T_1, \ldots, T_n]$ and $u \in U$ we write $f \circ u := f\big(u(T_1), \ldots, u(T_n)\big)$. The map $f \mapsto f \circ u$ is then a ring automorphism of $A[T_1, \ldots, T_n]$ which extends the permutation u of the variables T_i.

The map

$$\begin{aligned} A[T_1, \ldots, T_n] \times U &\longrightarrow A[T_1, \ldots, T_n], \\ (f, u) &\longmapsto f \circ u = f\big(u(T_1), \ldots, u(T_n)\big) \end{aligned}$$

is an example of a **group action.** We say that the group U acts on $A[T_1, \ldots, T_n]$ by ring automorphisms. In a nutshell, this means that $f \circ (uv) = (f \circ u) \circ v$ and $(f \bigtriangledown g) \circ u = (f \circ u) \bigtriangledown (g \circ u)$ for all $f, g \in A[T_1, \ldots, T_n]$, $u, v \in U$, $\bigtriangledown \in \{+, \times\}$.

Another way of saying that f is symmetric is that it is invariant under the U-action.

Theorem 16: Main theorem on symmetric polynomials. Consider a symmetric polynomial $P \in A[T_1, \ldots, T_n]$. Then there exists a polynomial $f \in A[U_1, \ldots, U_n]$ such that

$$P = f\big(\sigma_1(T_1, \ldots, T_n), \sigma_2(T_1, \ldots, T_n), \ldots, \sigma_n(T_1, \ldots, T_n)\big).$$

In words, P is a polynomial in the elementary polynomials in the T_i.

Example 17. Before proving theorem 16, we look at an example. The polynomial $\sum_i T_i^3$ is clearly symmetric. By theorem 16, it can be expressed in terms of the $\sigma_k = \sigma_k(T_1, \ldots, T_n)$. Let's do that explicitly. We have

$$\sigma_1^3 = \Big(\sum_i T_i\Big)^3 = \Big(\sum_i T_i^3\Big) + 3\,\Big(\sum_{i\neq j} T_i^2\, T_j\Big) + 6\,\sigma_3,$$

$$\sigma_1\,\sigma_2 = \Big(\sum_i T_i\Big)\Big(\sum_{j<k} T_j\,T_k\Big) = \Big(\sum_{i\neq j} T_i^2\,T_j\Big) + 3\,\sigma_3$$

so

$$\sigma_1^3 - 3\,\sigma_1\,\sigma_2 = \Big(\sum_i T_i^3\Big) - 3\,\sigma_3 \quad\text{and}\quad \sum_i T_i^3 = \sigma_1^3 - 3\,\sigma_1\,\sigma_2 + 3\,\sigma_3.$$

Proof of theorem 16. We need some terminology. A **monomial** of degree k is an expression $T_1^{k_1}\cdots T_n^{k_n}$ such that $k=\sum_i k_i$. An A-linear combination of degree k monomials is called a homogeneous polynomial of degree k.

It is enough to prove the theorem if P is homogeneous, so suppose it is.

We define a total ordering $<$ on the set of degree k monomials as follows. It is called the lexicographic ordering. We put $T_1 < \cdots < T_n$. Write

$$u = u_1\cdots u_k, \qquad v = v_1\cdots v_k$$

where $u_i, v_i \in \{T_1,\ldots,T_n\}$ and $u_i \le u_{i+1}$, $v_i \le v_{i+1}$ for all i. Then $u < v$ if there exists j such that $(u_1,\ldots,u_{j-1}) = (v_1,\ldots,v_{j-1})$ but $u_j < v_j$.

We may write $P = \sum_u a_u\,u$ (a sum over degree k monomials u with $a_u \in A$). The **leading monomial** of P is the least u such that $a_u \neq 0$. Suppose the theorem is false. Among the counterexamples, let P be one with maximal leading monomial. This is a high-brow way of doing induction and works because there are only finitely many degree k monomials.

Let $u = T_1^{k_1}\cdots T_n^{k_n}$ be the leading monomial in P. We have $k_i \ge k_{i+1}$ for all i (interchanging T_i and T_{i+1} in the term $a_u u$ yields some term $a_v v$ with $a_v = a_u$ and $v \ge u$; this implies $k_i \ge k_{i+1}$).

We aim to compare the leading monomial of P with that of $Q := \sigma_1^{\ell_1}\cdots\sigma_n^{\ell_n}$. The leading monomial of Q is the product of the leading monomials of the factors which is

$$T_1^{\ell_1}(T_1T_2)^{\ell_2}\cdots(T_1\cdots T_n)^{\ell_n} = T_1^{\ell_1+\cdots+\ell_n}\,T_2^{\ell_2+\cdots+\ell_n}\cdots T_n^{\ell_n}$$

and which becomes equal to $u = T_1^{k_1}\cdots T_n^{k_n}$ by putting

$$\ell_n := k_n, \qquad \ell_i := k_i - k_{i+1} \quad (i<n).$$

Now P, Q have equal leading monomials. So $P - a_uQ$ has greater leading monomial than P. Therefore, $P - a_uQ$ is a polynomial in the σ_k. Also, Q is and therefore, P is. This contradiction finishes the proof. □

Definition 18. A tuple $(g_1,\ldots,g_k)$ with $g_i \in A[T_1,\ldots,T_n]$ for all i is called a **symmetric tuple** of polynomials if for every $u \in \mathrm{Sym}(t_1,\ldots,t_n)$ there exists $v \in S_k$ such that $g_i \circ u = g_{v(i)}$ for all i.

In words, the effect on the g_i of permuting the variables T_j is no more than a permutation of the g_i.

If g_i is symmetric for every i, then $(g_1,\ldots,g_k)$ is a symmetric tuple of polynomials; the converse is of course false.

The following is an obvious and very useful lemma.

Lemma 19: plugging in a symmetric tuple. Let $(g_1,\ldots,g_k)$ be a symmetric tuple of polynomials, where $g_i \in A[T_1,\ldots,T_n]$ for all i. If $f \in A[U_1,\ldots,U_k]$ is symmetric then so is the element $f(g_1,\ldots,g_k)$ of $A[T_1,\ldots,T_n]$. □

1.5 Quartic equations

Easier than proving that cubic equations are solvable is deducing from it that quartic equations are solvable. So we begin with the latter. In the rest of this chapter we work in $\mathbb{C}$.

Theorem 20. Assume that cubic equations over $\mathbb{C}$ are solvable. Then so are quartic ones.

Proof. Let $f = \sum_k a_k X^k$ be a monic polynomial of degree 4 over an algebraically closed field K. Let $L \subset K$ be the radical closure of the coefficients a_0, a_1, a_2, a_3. We need to prove that all roots of f are in L.

Call those roots $\alpha, \beta, \gamma, \delta$ (see lemma 118). So $f = (X-\alpha)(X-\beta)(X-\gamma)(X-\delta)$. We now view $\alpha\,\beta, \gamma, \delta$ as variables. Define polynomials $k_1, k_2, k_3 \in L[\alpha, \beta, \gamma, \delta]$ by

$$k_1 = (\alpha+\beta-\gamma-\delta)^2, \quad k_2 = (\alpha-\beta+\gamma-\delta)^2, \quad k_3 = (\alpha-\beta-\gamma+\delta)^2.$$

One immediately sees that (k_1, k_2, k_3) is a symmetric tuple of polynomials. For example, the permutation (α, β) takes k_2 to $(-\alpha+\beta+\gamma-\delta)^2 = k_3$, thanks to the second power! Lemma 19 tells us now that whenever $h \in L[u_1, u_2, u_3]$ is a symmetric polynomial, $h(k_1, k_2, k_3)$ is symmetric in $\alpha, \beta, \gamma, \delta$.

Consider the **auxiliary polynomial** $g = (X-k_1)(X-k_2)(X-k_3)$. Every coefficient of g is, up to a sign, an (elementary) symmetric polynomial in the k_i. Therefore, every coefficient of g is symmetric in $\alpha, \beta, \gamma, \delta$.

By the main theorem of symmetric polynomials (theorem 16) every coefficient of g is a polynomial in $\{\sigma_k(\alpha, \beta, \gamma, \delta)\}_k$, that is, in $\{a_k\}_k$ (because the coefficients a_k of f are, up to signs, the elementary symmetric polynomials in $\alpha, \beta, \gamma, \delta$). So $g \in L[X]$.

By the assumption that cubics are solvable, the roots k_i of g are in L. Define ℓ_1, ℓ_2, ℓ_3, m by

$$\begin{cases} \alpha+\beta-\gamma-\delta = \ell_1 \\ \alpha-\beta+\gamma-\delta = \ell_2 \\ \alpha-\beta-\gamma+\delta = \ell_3 \\ \alpha+\beta+\gamma+\delta = m. \end{cases} \tag{21}$$

Then ℓ_i is a square root of k_i and is therefore in L. Also, $m \in L$ because it is a symmetric polynomial in $\alpha, \beta, \gamma, \delta$.

The system (21) is a non-degenerate system of linear equations over L in unknowns $\alpha, \beta, \gamma, \delta$ and solving it shows that $\alpha, \beta, \gamma, \delta \in L$ as required. □

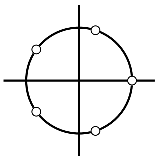
1.6 Roots of unity

For $n \geq 1$ we have

$$\left\{x \in \mathbb{C} \,\middle|\, x^n = 1\right\} = \left\{\exp\left(\frac{2\pi i k}{n}\right) \,\middle|\, 0 \leq k < n\right\}.$$

This set is written μ_n and its elements are called the nth (complex) roots of unity. See figure 1.

Figure 1. The five complex fifth roots of unity.



Note that $\mu_n \in \mathbb{C}^\times$ is a subgroup. It is a cyclic group of order n. Equivalently, it is isomorphic to the additive group of $\mathbb{Z}/n\mathbb{Z}$.

Definition 22. A **primitive n-th complex root of unity** is an $\alpha \in \mu_n$ which generates μ_n as a group.

The following are equivalent for a complex number α:

(a) α is a primitive n-th complex root of unity.

(b) $\alpha^n = 1$ but $\alpha^k \neq 1$ whenever $0 < k < n$.

(c) α is of the form $\exp\left(\frac{2\pi i k}{n}\right)$ with $k \in \mathbb{Z}$ coprime to n.

The number of primitive n-th complex roots of unity is written $\phi(n)$ and ϕ is known as the Euler totient function. In elementary number theory you learn that

$$\phi(n) = n \prod_{p|n} \frac{p-1}{p}$$

where the product is over the prime factors of n.

Definition 23. Let $n \geq 1$. The n-th **cyclotomic polynomial** ϕ_n is

$$\phi_n = \phi_n(X) := \prod_{\langle\alpha\rangle = \mu_n} (X - \alpha)$$

(product over the primitive n-th complex roots of unity). □

In exercise 1.13 you prove that $\phi_n \in \mathbb{Q}[X]$. It can be proved that ϕ_n is irreducible in $\mathbb{Q}[X]$ but we shall not use this result.

1.7 Cubic equations

Theorem 24. Cubic polynomials over $\mathbb{C}$ are solvable. More precisely, every degree 3 polynomial over an algebraically closed field is solvable.

Corollary 25. Quartics over $\mathbb{C}$ are solvable.

Proof of corollary 25 This is immediate from theorems 20 and 24. □

First proof of theorem 24 Our first proof is not entirely correct and mainly meant as something to marvel at. Consider a monic cubic $X^3 + aX^2 + bX + c$.

On replacing X by $X - a/3$ one obtains a cubic of the form $f = X^3 + 3pX + 2q$ which it is therefore enough to solve. We claim that

$$\sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}$$

is a root of f. Try it out and see that it works! Why aren't we entirely happy with this?

Second proof of theorem 24 The second proof is more correct and also shows how one might have discovered it.

As in the first proof, we only need to solve $f = X^3 + 3pX + 2q$. By lemma 118 there are (unique) $\alpha, \beta, \gamma \in K$ such that $f = (X - \alpha)(X - \beta)(X - \gamma)$. We need to prove that α, β, γ are in the radical closure $L \subset K$ of $\{p, q\}$. Let $\omega \in K$ be a primitive cube root of unity. Of course, $\omega \in L$.

We next treat α, β, γ as variables. Consider polynomials $u, v \in L[\alpha, \beta, \gamma]$ defined by

$$u = \alpha + \omega\beta + \omega^2\gamma, \quad v = \alpha + \omega^2\beta + \omega\gamma.$$

Claim: (u^3, v^3) is a symmetric tuple of polynomials (see definition 19). Proof of claim. It is (assumed to be) known that the symmetric group on α, β, γ is generated by $\{\pi_2, \pi_3\}$ where π_2 is the 2-cycle (β, γ) and π_3 is the 3-cycle (α, β, γ). Therefore, it is enough to show that u^3, v^3 are (at most) permuted under π_3 and π_2.

We have $u \circ \pi_2 = v$ and $v \circ \pi_2 = u$. That is, π_2 interchanges u with v. So it interchanges u^3 with v^3 as required.

We have

$$\begin{aligned} u \circ \pi_3 &= (\alpha + \omega\beta + \omega^2\gamma) \circ \pi_3 \\ &= \beta + \omega\gamma + \omega^2\alpha = \omega^2(\alpha + \omega\beta + \omega^2\gamma) = \omega^2 u \end{aligned}$$

and likewise $v \circ \pi_3 = \omega v$. In particular, π_3 preserves u^3 and v^3. The claim is proved.

Lemma 19 and the claim imply that whenever $h \in A[y_1, y_2]$ is a symmetric polynomial, $h(u^3, v^3)$ is symmetric in α, β, γ.

Consider the **auxiliary polynomial** $g = (X - u^3)(X - v^3) \in K[x]$. Any coefficient of g is, up to a sign, an elementary symmetric function in u^3, v^3 and therefore symmetric in α, β, γ. By the main theorem on symmetric functions (theorem 16) we find $g \in L[\sigma_2(\alpha, \beta, \gamma), \sigma_3(\alpha, \beta, \gamma)][X] = L[p, q][X] = L[X]$.

From now we treat α, β, γ as numbers. The polynomial g has degree 2 and is therefore solvable by example 10, that is, $u^3, v^3 \in L$. As L is closed under taking cube roots we have $u, v \in L$. We have a non-degenerate system of linear equations over L in unknowns α, β, γ

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha + \omega\beta + \omega^2\gamma = u \\ \alpha + \omega^2\beta + \omega\gamma = v \end{cases}$$

and "solving" it for α, β, γ shows that $\alpha, \beta, \gamma \in L$ as well as required. □

1.8 How to use Maple

This is not part of the course, but I recommend doing it. At a unix terminal, type maple; you get a clever logo, and the prompt >. For example, you can calculate $\sum T_i^3$ in terms of elementary symmetric functions by the following few lines:

```
> s1:=a+b+c; s2:=a*b+a*c+b*c; s3:=a*b*c;

                 s1 := a + b + c
                 s2 := a b + a c + b c
                 s3 := a b c

> expand(a^3+b^3+c^3-s1^3);

       2       2         2                 2     2         2
  - 3 a b - 3 a c - 3 a b - 6 a b c - 3 a c - 3 b c - 3 b c

> expand(%+3*s1*s2);

                  3 a b c

> evalb(expand(s1^3-3*s1*s2+3*s3) = a^3+b^3+c^3);

                   true
```

Mathematica is very similar.

1.9 Exercises

(1.7) If $f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$ has roots $\alpha_1, \ldots, \alpha_n$, what polynomial has roots $c\alpha_1, \ldots, c\alpha_n$?

(1.8) Let $a, b, c \in \mathbb{C}$. Let K be the radical closure of $\{a, b, c\}$ (that is, the smallest subfield of $\mathbb{C}$ containing a, b, c and such that for all $\alpha \in \mathbb{C}$, $n > 0$, if $\alpha^n \in K$ then $\alpha \in K$). Let L be the radical closure of $\{ab, bc, ca\}$. Prove $K = L$.

(1.9) Prove that $X^5 - 3X^3 - 8$ is solvable by radicals.

(1.10) Let $T_1, \ldots, T_n$ be variables. Express the polynomial

$$S = \sum_{1 \le i < j < k \le n} T_i \, T_j \, T_k \, (T_i + T_j + T_k)$$

in terms of the elementary symmetric polynomials $\sigma_k(T_1, \ldots, T_n)$.

(1.11) Express each of the following in terms of the σ_k:

$$\sum_i T_i^2, \qquad \sum_{i,j} T_i^2 \, T_j, \qquad \sum_{i<j} T_i^2 \, T_j^2.$$

(1.12) Let α, β, γ be the roots of the equation $X^3 + pX^2 + q = 0$. Find the cubic polynomial equation whose roots are α^3, β^3, γ^3.

(1.13) Recall the cyclotomic polynomial $\phi_n(X) := \prod(X-\alpha)$ where the product is over the complex primitive n-th roots of unity.

(a) Prove $\prod_{d|n}\phi_d(X) = X^n - 1$ for all $n \geq 1$. Here, the product is over the positive divisors d of n.

(b) Prove $\phi_n(X) \in \mathbb{Q}(X)$.

(c) Prove $\phi_n(X) \in \mathbb{Q}[X]$.

(1.14) Write $\varepsilon := \exp(2\pi i/5)$ for the natural primitive 5th root of 1; it is a root of the quartic $f(X) = X^4 + X^3 + X^2 + X + 1$. Find the quadratic equation whose two roots are $\varepsilon + \varepsilon^4$ and $\varepsilon^2 + \varepsilon^3$, and hence give radical formulas for $\cos(2\pi/5)$ and $\cos(4\pi/5)$.

(1.15) Let $S_k = \sum_i T_i^k$ be the power sum. Express S_k in terms of the elementary symmetric polynomials if $k = 4, 5$. Do it for $k = 6, 7$ if you know how to use Maple or Mathematica.

(1.16)

(a) Put $f = X^6 + a\,X^5 + a\,X + 1 \in \mathbb{C}[X]$. Find an explicit $g \in \mathbb{C}[y]$ such that $X^{-3}f(X) = g(X + X^{-1})$. Prove that f can be solved by radicals.

(b) Prove or disprove the following. Put $h = X^5 + a\,X^4 + a\,X + 1 \in \mathbb{C}[X]$. Then h can be solved by radicals.

(1.17) Let $L = \mathbb{C}(T_1, \dots, T_n)$ be the field of rational functions in n variables. Let the symmetric group S_n act on L by permutation of the variables T_i. Let $\sigma_k \in L$ be the elementary symmetric polynomials in the T_i. Put

$$\begin{aligned} K &= \{f \in L \mid r(f) = f \text{ for all } r \in S_n\}, \\ M &= \mathbb{C}(\sigma_1, \dots, \sigma_k) \subset L. \end{aligned}$$

In other words, M is the smallest subfield of L containing $\mathbb{C}$ and the T_i. Prove that $K = M$.

(1.18) Prove Newton's rule $\sum_{k=0}^{n}(-1)^k\sigma_k\,S_{n-k} = 0$ where $S_k = \sum_i T_i^k$ is the power sum.

(1.19) Let σ_i be the elementary symmetric functions of $T_1, \dots, T_n$ and τ_i the elementary symmetric functions of $T_1^2, \dots, T_n^2$. Prove:

$$\tau_k = \sum_{i=0}^{2k}(-1)^{k+i}\,\sigma_i\,\sigma_{2k-i}.$$

(1.20) Suppose that the polynomial $f = x^2 + px + q \in \mathbb{C}[x]$ factorizes as $f = (x+\alpha)(x+\beta)$. Compute $g = (x + \alpha + \beta^2)(x + \beta + \alpha^2)$ explicitly, giving its coefficients in terms of p, q.

2 Background on rings, fields and groups

Keywords: Field of fractions, rational function, ideal, generators of an ideal, kernel, coset, prime ideal, maximal ideal, quotient ring, principal ideal, PID, UFD, first isomorphism theorem for rings, characteristic, prime field, Frobenius, left action, right action, permutation, symmetric group, faithful action.

This chapter is a reminder and reference on rings, fields and groups. You're supposed to know most or all of this chapter already, and this chapter is not detailed enough to learn the material if you haven't seen it before. We use the material in this chapter throughout the rest of the notes. If you're not yet familiar with the material in this chapter but still want to follow the module then you'll have to work very hard to catch up. A good place to learn this material is chapter 3 in *Concrete Abstract Algebra* by Niels Lauritzen.

2.1 *Fields of fractions*

Exercise (2.1) Let A be an integral domain. Put

$$B = \{(a,b) \in A \times A \mid b \neq 0\}$$

and let $\sim$ be the binary relation on B defined by $(a,b) \sim (c,d)$ if and only if $ad = bc$.

(a) Prove that $\sim$ is an equivalence relation. We denote the equivalence class of (a,b) by a/b.

(b) Prove that the following are well-defined operations on $B/\sim$:

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{a\,c}{b\,d}, \qquad \frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}.$$

Prove that this makes $B/\sim$ into a field. It is called the **field of fractions** of A and sometimes written $\operatorname{Frac} A$.

(c) What goes wrong in the above if A is a ring which is not an integral domain?

If K is a field, the field of fractions $\operatorname{Frac} K[X]$ of the polynomial ring is written $K(X)$. An element of $K(X)$ is called a **rational function**, in analogy with the observation that $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$.

2.2 *Ideals and factorisation*

A nonzero subset I of a ring A is said to be an **ideal** if

$$x - y \in I \quad \text{for all} \quad x, y \in I; \tag{26}$$

$$ax \in I \quad \text{for all} \quad a \in A, \quad x \in I. \tag{27}$$

Note that (26) means precisely that $I \subset A$ is an additive subgroup.

Exercise (2.2) Let A be a ring.

(a) If $x_1, \dots, x_n \in A$ then $I := \{\sum_{k=1}^{n} a_k x_k \mid a_1, \dots, a_n \in A\}$ is an ideal in A.

(b) Suppose that J is an ideal containing $x_1, \dots, x_n$. Prove that $I \subset J$. Thus, I is the smallest ideal containing $\{x_1, \dots, x_n\}$. We call it the ideal **generated by $x_1, \dots, x_n$**. It is written $(x_1, \dots, x_n)$ or $x_1 A + \cdots + x_n A$.

The **kernel** of a ring homomorphism $f\colon A \to B$ is defined to be $\ker(f) := \{a \in A \mid f(a) = 0\}$. Then $\ker(f)$ is an ideal in A.

Let A be a ring and $I \subset A$ an ideal. For $a \in A$ we write $a + I := \{a + x \mid x \in I\}$ (this is called a **coset**) and $A/I := \{a + I \mid x \in I\}$. We have $a + I = b + I$ if and only if $a - b \in I$. We put a ring structure on the set A/I by $(a + I) + (b + I) := (a + b) + I$ and $(a + I)(b + I) := (ab) + I$. One should prove that this is well-defined, that is, if $a_1 + I = a_2 + I$ then $a_1 b + I = a_1 b + I$, and likewise for addition. One should also prove that this makes A/I into a ring. This is the unique ring structure on the set A/I such that the natural map $A \to A/I$, $a \mapsto a + I$ is a ring homomorphism. Its kernel is precisely I. This proves:

Proposition 28. Let I be an ideal in a ring A. Then there exists a ring B and a surjective ring homomorphism $A \to B$ whose kernel is I. □

We call A/I the **quotient ring** of A by I.

Definition 29. Let I be an ideal in a ring A such that $I \neq A$. We call I a **prime ideal** if $ab \in I$ implies $a \in I$ or $b \in I$. We call it a **maximal ideal** if for every ideal J such that $I \subset J \subset A$ we have $I = J$ or $J = A$.

Proposition 30. Let I be an ideal in A.

(a) Then, I is a prime ideal if and only if A/I is an integral domain.

(b) Also, I is a maximal ideal if and only if A/I is a field. □

Definition 31. Let A be a ring. A **principal ideal** in A is an ideal of the form aA with $a \in A$, that is, an ideal generated by a single element a. A **principal ideal domain** or PID is an integral domain all of whose ideals are principal.

Proposition 32. The ring $\mathbb{Z}$ is a PID. If K is a field then $K[X]$ is a PID. □

Exercise (2.3) Prove the second half of proposition 32, namely, that $K[X]$ is a PID for any field K. Hint: if $I \subset K[X]$ is a nonzero ideal, let $f \in I$ be a nonzero of minimal degree. Use theorem 2 (division with remainder) to prove that $I = (f)$.

Proposition 33. Let A be a PID. Then for all nonzero $a \in A$, the following are equivalent.

(1) The ideal (a) is a maximal ideal in A.

(2) The ideal (a) is a prime ideal in A.

(3) a is irreducible.

Proof. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are clear. Proof of (3) $\Rightarrow$ (1). Consider an ideal I such that $(a) \subset I \subset A$, say, $I = (b)$. Then $a \in I$, that is, $a = bc$ for some $c \in A$. By irreducibility of a, one among b, c is a unit in A. If b is a unit then $I = A$. If c is a unit then $(a) = I$. □

Definition 34. Let A be an integral domain. We say that A is a **unique factorisation domain** or UFD if the following holds. Every nonzero element of A which is not a unit can be written $a_1 \cdots a_n$ where a_i is an irreducible element of A, for all i. Moreover, if $b_1 \cdots b_m$ is another such factorisation, then $m = n$ and there exists $\pi \in S_n$ such that for all i, we have an equality of ideals $(a_i) = (b_{\pi(i)})$.

Proposition 35. Every PID is a UFD. In particular, so are $\mathbb{Z}$ and $K[X]$ for K a field. □

2.3 Prime fields

Theorem 36: First isomorphism theorem for rings. Let $f\colon A \longrightarrow B$ be a ring homomorphism with kernel I and image C. Then C is a subring of B, and there exists an isomorphism $A/I \longrightarrow C$ defined by $a + I \mapsto f(a)$. □

Let A be a ring. Then there is a unique ring homomorphism $\theta\colon \mathbb{Z} \longrightarrow A$. Indeed, we must have $\theta(1) = 1$ and therefore, if $n \in \mathbb{Z}_{\geq 0}$ then $\theta(n) = 1 + \cdots + 1$ (n terms) and $\theta(-n) = -\theta(n)$. Conversely, it should be clear that this defines a homomorphism θ.

The kernel of θ is an ideal in $\mathbb{Z}$, and therefore of the form $n\mathbb{Z}$ for a unique $n \in \mathbb{Z}_{\geq 0}$; see proposition 32. We call n the **characteristic** of A.

Proposition 37. Let A be a ring. Then A contains a smallest subring. It is isomorphic to $\mathbb{Z}/n$ where n is the characteristic of A.

Proof. First one proves that the image of $f_A\colon \mathbb{Z} \longrightarrow A$ is the smallest subring of A. By theorem 36, the first isomorphism theorem for rings, the image of f_A is isomorphic to $\mathbb{Z}/\ker(f_A) = \mathbb{Z}/n\mathbb{Z}$. □

Definition 38. Let K be a field. It is clear that there exists a smallest subfield of K. It is called the **prime subfield** of K. A **prime field** is a field equal to its own prime subfield.

Proposition 39.

(a) The fields $\mathbb{Q}$ and $\mathbb{Z}/p$ (for p a prime number) are prime fields. They are the only prime fields up to isomorphism.

(b) Let K be a field of characteristic n and prime subfield K_0. Then either $n = 0$ or n is a prime number. If $n = 0$ then $K_0 \cong \mathbb{Q}$. If $n = p$ is a prime number then $K_0 \cong \mathbb{Z}/p$. □

2.4 Exercises

(2.4) Let R be a ring. Prove that R is an integral domain if and only if it can be embedded into a field. (We say that R can be embedded into a field if it is isomorphic to a subring of a field).

(2.5) Suppose that $f = X^{n-1} + X^{n-2} + \cdots + 1 \in \mathbb{Q}[X]$ is irreducible, with $n \geq 1$. Prove that n is a prime number.

(2.6) Let A be a ring of characteristic p (a prime number).

(a) Prove that the binomial coefficient $\binom{p}{k}$ is divisible by p if $0 < k < p$.

(b) Prove that $F\colon A \to A$ defined by $F(a) = a^p$ is a ring homomorphism. It is called the **Frobenius ring homomorphism**. Hint: use the binomial theorem.

(c) Is F necessarily injective? Surjective? Give a proof or a counterexample. Same question if A is a field.

(d) Prove $(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p$ for all $a_i \in A$.

(e) Prove Fermat's theorem that $p \mid n^p - n$ for all integers n.

(2.7) Let $\mathbb{F}_q$ be a finite field of q elements. Prove the following identity in $\mathbb{F}_q[X]$:

$$\prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X^q - X.$$

[Hint: $\mathbb{F}_q^\times$ is a group of $q - 1$ elements.]

(2.8) Prove that the polynomial ring $K[X]$ over any field K has infinitely many irreducible polynomials. Hint: Imitate Euclid's proof that there are infinitely many prime numbers.

(2.9) Let $f\colon \mathbb{R} \to \mathbb{R}$ be a ring homomorphism. Prove that f is the identity. (You may use that $f(1) = 1$ but not that f is continuous). This result is quite curious, since there are uncountably many homomorphisms $\mathbb{C} \to \mathbb{C}$.

2.5 Group actions

Here is some simple background on group actions.

Definition 40. Let G be a group and X a set. A **left G-action on X** is a map $G \times X \to X$ written $(g, x) \mapsto g(x) = gx$ such that $(gh)x = g(hx)$ for all $g, h \in G$, $x \in X$.

Similarly, a **right G-action on X** is a map $X \times G \to X$ written $(x, g) \mapsto (x)g = xg$ such that $x(gh) = (xg)h$ for all $g, h \in G$, $x \in X$.

If $(g, x) \mapsto gx$ is a left G-action then $(x, g) \mapsto gx$ is *not* necessarily a right action; but $(x, g) \mapsto g^{-1}x$ is.

Let X be a set. A bijective map $X \to X$ is sometimes called a **permutation** of X. The set of permutations of X forms a group $\mathrm{Sym}(X)$ called the **symmetric group on X**. Analogous to the distinction between left and right actions, one can and should choose whether to write sx or xs for all $x \in X$ and $s \in \mathrm{Sym}(X)$.

We write S_n for $\mathrm{Sym}(\{1, \dots, n\})$. Thus $\mathrm{Sym}(X)$ is isomorphic to S_n if X has n elements.

The following proposition says that G-actions on X are 'the same things' as homomorphisms $G \to \mathrm{Sym}(X)$.

Proposition 41. Let G be a group and X a set. There exists a unique bijection between the set of left G-actions on X and the set of homomorphisms $G \to \mathrm{Sym}(X)$ (with permutations of X acting on the left) such that whenever the action $(g, x) \mapsto g \circ x$ corresponds to the homomorphism $s\colon G \to \mathrm{Sym}(X)$ then $(sg)x = g \circ x$ for all $g \in G$, $x \in X$.

Proof. Exercise. □

A G-action on X is said to be **faithful** if the corresponding homomorphism $G \to \mathrm{Sym}(X)$ is injective.

Exercise (2.10) Prove that a left G-action on X is faithful if and only if for all nontrivial $g \in G$ there exists $x \in X$ such that $gx \neq x$.

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 42. 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 43: 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

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

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

$$\sum_{k=0}^{r+s} g_k h_{r+s-k} = \Big(\sum_{k=0}^{r-1} g_k h_{r+s-k}\Big) + g_r h_s + \Big(\sum_{k=r+1}^{r+s} g_k h_{r+s-k}\Big). \tag{44}$$

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 (44) 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 45. Prove that $f = X^3 + 2X + 7 \in \mathbb{Q}[X]$ is irreducible.

Solution. By proposition 43b (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 46. 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 47. 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 43b (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 48: Irreducible polynomials over $\mathbb{F}_2$. We will compute all irreducible polynomials in $\mathbb{F}_2[X]$ of degree $d \leq 4$.

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

$\boldsymbol{d = 2}$**.** 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.

$\boldsymbol{d = 3}$**.** 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.

$\boldsymbol{d = 4}$**.** 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 47 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 49: 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 $0 \le i \le m-1$,

(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 50. 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 51. 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 52. 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 $A[x_1, \dots, x_n] \subset A(x_1, \dots, x_n)$ because every field is a ring. If $A(x_1, \dots, x_n)$ is defined then it equals $\operatorname{Frac} A[x_1, \dots, x_n]$.

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

Example 53. 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 54. As we saw in example 53, $\{1, \sqrt{2}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2})$ and therefore $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Example 55. 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 56. 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 57. 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 58. 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 $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ 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 $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ 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 59. 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 58a) 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.

Exercise (3.2) Let $K \subset L$ be fields. Let $f \in K[X]$ be irreducible and let $\alpha \in L$ be a root of f. Prove that f is the minimum polynomial of α over K.

Example 60. 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 58d. Thus α^{-2} is of the form $c_0 + c_1\alpha + c_1\alpha^2$ for unique c_0, c_1, c_2 in $\mathbb{Q}$. 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 61. 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 extend to extensions in the wide sense. We won't always make the generalisations explicit and you should be able to reconstruct and use the generalisations yourself when necessary.

In order to be complete and consistent one would have to state and prove everything about extensions in the wide sense rather than the narrow sense. On the other hand, for field extensions in the narrow sense the notation is simpler.

For example, the generalisation of definition 61 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 $\sigma_2 \circ f = \sigma_1$.

The following easy result shows a crucial property of ring homomorphisms and an analogous property of K-homomorphisms. Parts (a) and (b) are analogous.

Lemma 62.

(a) Let $s \colon A \to B$ be a homomorphism of rings and $f \in \mathbb{Z}[X]$ a polynomial. Then $s(f(a)) = f(s(a))$ for all $a \in A$.

(b) Let L_1/K and L_2/K be field extensions. Let $s \colon L_1 \to L_2$ be a K-homomorphism and let $f \in K[X]$ be a polynomial. Then $s(f(a)) = f(s(a))$ for all $a \in L_1$.

(c) Let $K(\alpha)/K$ and $K(\beta)/K$ be field extensions with α and β algebraic over K. Let $s \colon K(\alpha) \to K(\beta)$ be a K-isomorphism such that $s(\alpha) = \beta$. Then α and β have the same minimum polynomial over K.

Proof. (a). Write $f = \sum_i c_i X^i$ with $c_i \in \mathbb{Z}$. Then

$$\begin{aligned} s(f(a)) &= s \sum_i c_i a^i = \sum_i s(c_i a^i) = \sum_i s(c_i)\, s(a^i) \\ &= \sum_i c_i\, s(a^i) = \sum_i c_i\, s(a)^i = f(s(a)). \end{aligned}$$

(b). Write $f = \sum c_i X^i$ with $c_i \in K$. Then

$$\begin{aligned} s(f(a)) &= s \sum c_i a^i = \sum s(c_i)\, s(a)^i && \text{because } s \text{ is a ring homomorphism} \\ &= \sum c_i\, s(a)^i && \text{because } s \text{ is a } K\text{-homomorphism} \\ &= f(s(a)). \end{aligned}$$

(c). Let f be the minimum polynomial of α over K. By (b) we have $0 = s(0) = s(f(\alpha)) = f(s(\alpha)) = f(\beta)$. By exercise 3.2, f is the minimum polynomial of β as well. □

A strong converse to (c) is proposition 63b below.

Note that every minimum polynomial is irreducible by proposition 58b. A converse to this is part (a) of the following proposition.

Proposition 63. 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 over K 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 with α algebraic over 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 $\phi(g) = g(\alpha)$.

Remark 64. The polynomial $X^2 + 1 \in \mathbb{R}[X]$ is irreducible. By proposition 63a there exists an extension $\mathbb{R}(\alpha)$ of $\mathbb{R}$ such that the minimum polynomial of α is $X^2 + 1$. Of course, we know this field: it is $\mathbb{C}$.

Usually we define $\mathbb{C}$ to be $\mathbb{R} \times \mathbb{R}$ (as a set) with specific ring structure. If you try to prove proposition 63a by a similar method (that is, first you define $K(\alpha)$ to be K^n as a set, and then you give it some ring structure) you end up in a mess. The right way to prove it is given below and is a first highlight of abstract ring theory.

In Galois theory the proof of this proposition is not relevant though; we can and will use proposition 63 without understanding its proof. We provide the proof for completeness' sake.

Proof. Proof of (a). By proposition 58b, 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 58c we have $I = (f)$. Also, $\theta(K[X]) = K[\alpha] = K(\alpha)$ by proposition 58f. 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 $f = \mathrm{mp}_K(\alpha)$. Firstly, note that $\phi(g)$ is always a root of f by lemma 62c.

That ϕ is injective is proved the way unicity is in part (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 say ***K*-basis, spanning over *L*** and so on.

Theorem 65: 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 66. Recall that we proved in example 53d 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 67. 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

$$\begin{aligned} 2 = (\sqrt{2})^2 = (\alpha - \sqrt{5})^2 &= \alpha^2 - 2\sqrt{5}\,\alpha + 5, \\ 2\sqrt{5}\,\alpha &= \alpha^2 + 5 - 2, \\ 20\alpha^2 &= (\alpha^2+3)^2 \end{aligned} \tag{68}$$

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

(b). The inclusion $\supset$ is obvious. By (68) 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 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(\alpha) \arrow[dd, dash, "4"] \\ \mathbb{Q}(\sqrt{2}) \arrow[ur, dash, "2"'] \arrow[dr, dash, "2"'] & \\ & \mathbb{Q} \end{tikzcd}$$

By the tower law we find $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. By proposition 58 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

(3.3) In example 48 we computed the irreducible polynomials in $\mathbb{F}_2[X]$ of degree ≤ 4. Compute those of degree 5.

(3.4)

(a) Prove that $h := X^3 + 6\,X - 11 \in \mathbb{Z}[X]$ 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 $f := X^7 + 6\,X^3 + 12 \in \mathbb{Z}[X]$ is Eisenstein. Deduce that it is irreducible in $\mathbb{Z}[X]$ and in $\mathbb{Q}[X]$.

(e) Prove that $g := 2\,X^{10} + 4\,X^5 + 3 \in \mathbb{Q}[X]$ is irreducible. Hint: which related polynomial is Eisenstein? Use the result of exercise (3.5) below.

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

(3.5) 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.

(3.6) Prove that the cyclotomic polynomial ϕ_n is irreducible over $\mathbb{Q}$ if n is power of a prime number.

(3.7) 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.

(3.8) Let A be an integral domain containing a field K. Let $a \in A$ be nonzero. Recall from exercise (3.7) 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.

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

(3.10) 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 $c_i \in \mathbb{Q}$.

(3.11) 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 $h(\alpha) = g(\alpha)^{-1}$.

(3.12) 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.

(3.13) 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.

(3.14) 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 $\beta^2 \in K$.

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

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

(3.17) (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 $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

(3.18) 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 $\mathbb{Q}$.

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

(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).

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

(3.21) 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.]

(3.22) 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 (3.21).]

(3.23) 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.

4 Foundations of Galois theory

4.1 Closure correspondences

In this subsection, we fix two disjoint sets A, B and a subset $R \subset A \times B$, often known as a **binary relation.** For all $X \subset A$ and $Y \subset B$ we define

$$\begin{aligned} X^\dagger &:= \{b \in B \mid (a,b) \in R \quad \text{for all } a \in X\}, \\ Y^* &:= \{a \in A \mid (a,b) \in R \quad \text{for all } b \in Y\}. \end{aligned} \tag{69}$$

Let $P(A)$ be the **power set**, that is, the set of subsets of A. We have thus two maps $\dagger\colon P(A) \to P(B)$ and $*\colon P(B) \to P(A)$.

Remark 70. A better but somewhat pedantic approach is to replace $P(A)$ by $P(A) \times \{1\}$ and $P(B)$ by $P(B) \times \{2\}$. Here 1 and 2 are labels indicating whether we're thinking of a subset of A or one of B. The empty set is a subset of both A and B, but that's the only ambiguity not ruled out by our assumption that A and B are disjoint.

Proposition 71.

(a) For all $X \subset A$, we have $X \subset X^{\dagger *}$.

(b) For all $Y \subset B$, we have $Y \subset Y^{*\dagger}$.

(c) For all $X_1 \subset X_2 \subset A$, we have $X_1^\dagger \supset X_2^\dagger$.

(d) For all $Y_1 \subset Y_2 \subset B$, we have $Y_1^* \supset Y_2^*$.

(e) For all $X \subset A$, we have $X^\dagger = X^{\dagger * \dagger}$, or briefly, $\dagger * \dagger = \dagger$.

(f) For all $Y \subset B$, we have $Y^* = Y^{* \dagger *}$, or briefly, $* \dagger * = *$.

Proof. These are almost trivial as we shall see. We write out the proofs in detail.

Proof of (a). Let $a \in X$ and $b \in X^\dagger$. Then $(a,b) \in R$ by definition of $\dagger$. As this is true for all such b, it implies that $a \in X^{\dagger *}$ by definition of $*$.

Proof of (c). Let $b \in X_2^\dagger$. Then $(a,b) \in R$ for all $a \in X_2$, by definition of $\dagger$. So $(a,b) \in R$ for all $a \in X_1$ (because $X_1 \subset X_2$). This means that $b \in X_1^\dagger$ as required.

Proof of (e). By (a) we have $X \subset X^{\dagger *}$. Applying (c) with $X_1 = X$ and $X_2 = X^{\dagger *}$ gives $X^\dagger \supset X^{\dagger * \dagger}$. In order to prove the reverse inclusion, let $b \in X^\dagger$. By definition of $*$ then, $(a,b) \in R$ for all $a \in X^{\dagger *}$. In other words, $b \in X^{\dagger * \dagger}$.

The remaining three parts follow by interchanging $(A, \dagger)$ and $(B, *)$. □

The $(A, \dagger)$–$(B, *)$ symmetry mentioned in the above proof is often useful.

We call a subset $X \subset A$ **closed** if and only if it is of the form Y^*. This is equivalent to saying that $X = X^{\dagger *}$, by proposition 71f. Closed subsets of B are defined likewise.

Proposition 72. There is a bijection from the set of closed subsets of A to the set of closed subsets of B, given by $X \mapsto X^\dagger$, and whose inverse is $Y \mapsto Y^*$.

Proof. Almost immediate from proposition 71. □

Of course, $X^\dagger$ is defined for *all* subsets X of A. But the formula $X \mapsto X^\dagger$ in proposition 72 assumes that X is closed.

Let us call the bijection given by proposition 72 the **closure correspondence**. Each time we have two sets A, B and a subset $R \subset A \times B$, there is a closure correspondence.

There are lots of closure correspondences in mathematics, and we touch upon some of them in exercises 4.2–4.4. But the most famous of all is a particular closure correspondence called the Galois correspondence which is at the centre of Galois theory.

Exercises

(4.1) Use the notation of this subsection.

(a) Prove that A is closed. Is $\varnothing \subset A$ necessarily closed?

(b) Prove that if $X_1, X_2 \subset A$ are closed, then so is $X_1 \cap X_2$. What about any number of X_i?

(c) Give an example where $X_1, X_2 \subset A$ are closed but $X_1 \cup X_2$ is not.

— ∼ —

To get a feel for closure correspondences in general, we look at a few examples not used later on in the lectures.

(4.2) [Standard representation of $\mathrm{GL}(n)$]. Let K be a field of at least 3 elements. Let $V = K^n$, $G = \mathrm{GL}(n, K)$ and consider the binary relation $R = \{(v, g) \in V \times G \mid g(v) = v\}$. Prove that the closed subsets of V are precisely the vector subspaces of V. If K has 2 elements, describe the closed subsets of V in similar terms.

(4.3) [Downsets]. Let $(P, \leq)$ be an ordered set. (Some people say *partially ordered set* when we say *ordered set*). Let $A = B = P$ and let $R \subset A \times B$ be the binary relation given by $R = \{(a, b) \in A \times B \mid a < b\}$. Prove that a subset $X \subset A$ is closed if and only if for all $x, y \in A$, if $y \in X$ and $x \leq y$ then $x \in X$. Also, if $X \subset A$ is closed, then $X^\dagger$ equals the complement $P \setminus X$.

(4.4) [Affine varieties]. Let $A = \mathbb{C}^n$ and let $B = \mathbb{C}[X_1, \ldots, X_n]$ be the ring of polynomials in n variables. If $a = (a_1, \ldots, a_n) \in A$ and $f \in B$, we can evaluate f at a to obtain a complex number $f(a) = f(a_1, \ldots, a_n)$. Consider the binary relation $R = \{(a, f) \in A \times B \mid f(a) = 0\}$. Prove that if a subset $I \subset B$ is closed, then it is a radical ideal (an ideal J in a ring S is said to be radical if for all $f \in S$ and all $n > 0$, if $f^n \in J$ then $f \in J$).

The converse is also true and known as Hilbert's Nullstellensatz: see the book *Undergraduate algebraic geometry* by Miles Reid for a one-page proof.

4.2 The Galois correspondence

Definition 73. Let $K \subset M$ be fields. The **Galois group** $\mathrm{Gal}(M/K)$ is the group of field automorphisms of M which fix every element of K.

It is not hard to show that $\mathrm{Gal}(M/K)$ is a group under composition.

Example 74. Here are some examples of Galois groups $\mathrm{Gal}(M/K)$.

(a). If $K = M$ then the Galois group is trivial.

(b). Suppose $K = \mathbb{R}$, $M = \mathbb{C}$. Then the Galois group has order 2, and consists of the trivial element and complex conjugation.

(c). Suppose $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. Again the Galois group has order 2 as we proved in example 53.

(d). Suppose $K = \mathbb{Q}$ and $M = \mathbb{Q}(\alpha)$ where $\alpha = 2^{1/3}$ is the real cube root of 2. We claim that $\mathrm{Gal}(M/K)$ is trivial. Let $s \in \mathrm{Gal}(M/K)$. Then $s(\alpha)$ is a cube root of 2 and is in $\mathbb{R}$ because $M \subset \mathbb{R}$. But α is the only cube root of 2 in $\mathbb{R}$ so $s(\alpha) = \alpha$. It follows that $s = 1$ because M is generated by α.

(e). Let $n \geq 1$. Then the Galois group $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(X^n))$ is cyclic of order n and generated by $s\colon X \mapsto \exp(2\pi i/n)\, X$.

(f). Let K be a field. It can be shown that $\mathrm{Gal}(K(X)/K)$ consists of those K-automorphisms of $K(X)$ taking X to a rational function of the form

$$\frac{aX+b}{cX+d}$$

with $a, b, c, d \in K$, $ad - bc \neq 0$. This group is usually denoted $\mathrm{PGL}(2, K)$.

For the rest of this section, we fix a field extension N/K and write $G = \mathrm{Gal}(N/K)$. We now introduce some notation that we use nearly always when considering a field extension.

We define a binary relation $R \subset G \times N$ by

$$R = \{(g, x) \in G \times N \mid g(x) = x\}.$$

Let $\dagger\colon P(G) \to P(N)$ and $*\colon P(N) \to P(G)$ be the maps as in (69). Explicitly: for $H \subset G$ and $L \subset N$ we define

$$\begin{aligned} H^\dagger &:= \{x \in N \mid g(x) = x \quad \text{for all } g \in H\}, \\ L^* &:= \{g \in G \mid g(x) = x \quad \text{for all } x \in L\}. \end{aligned}$$

Definition 75. As in section 4.1, we can talk about closed subsets of G and closed subsets of N. Let $\mathcal{F}$ denote the set of closed subsets of N and $\mathcal{G}$ the set of closed subsets of G.

As a particular case of proposition 72 we get:

Proposition 76. There exists a bijection $\mathcal{F} \to \mathcal{G}$ given by $H \mapsto H^\dagger$ and whose inverse is $L \mapsto L^*$. □

Of course, proposition 76 is virtually worthless unless we can determine which subsets of G or N are closed. Two easy restrictions are as follows:

Exercise (4.5) Prove that every element of $\mathcal{G}$ is a subgroup of G. Prove that every element of $\mathcal{F}$ is a subfield of N containing K.

Because of exercise 4.5, an element of $\mathcal{G}$ (that is, a closed subset of G) is called a **closed subgroup** of G. Also, an element of $\mathcal{F}$ is called a **closed intermediate field.** In general, if $P \subset Q \subset R$ are fields then we say that Q is an **intermediate field** of the extension $P \subset R$.

4.3 The closed fields and subgroups

Proposition 77. Let $K \subset L \subset M \subset N$ be fields. If $[M : L] = n < \infty$ then $[L^* : M^*] \leq n$.

Proof. Induction on n, the case $n = 1$ being trivial. If there exists a field L_0 properly between L and M, then the induction hypothesis tells us that $[L^* : L_0^*] \leq [L_0 : L]$ and $[L_0^* : M^*] \leq [M : L_0]$. Therefore

$$[L^* : M^*] = [L^* : L_0^*][L_0^* : M^*] \leq [L_0 : L][M : L_0] = [M : L].$$

So suppose now that there are no fields between L and M. Then M is of the form $L(\alpha)$ for some $\alpha \in M$. Let $f \in L[X]$ be the minimum polynomial for α over L. By proposition 58 we have $\deg(f) = [M : L] = n$. Consider the set Y of roots of f in M. Then $\#Y \leq n$. We define a map $E\colon L^*/M^* \to N$ (evaluation at α) by

$$E(gM^*) := g(\alpha).$$

We need to show that this is well-defined, that is, if $gM^* = hM^*$ then $g(\alpha) = h(\alpha)$. Indeed, if $g = hk$ with $k \in M^*$, then $g(\alpha) = h(k(\alpha)) = h(\alpha)$, showing that E is well-defined.

For all $g \in L^*$ we have

$$\begin{aligned} 0 &= g(0) && \text{because } g \text{ is a field automorphism} \\ &= g(f(\alpha)) && \text{because } f(\alpha) = 0 \\ &= f(g(\alpha)) && \text{because } g \in L^* \text{ and } f \in L[X] \end{aligned}$$

which proves that E takes values only in Y. If we can prove that $E\colon L^*/M^* \to Y$ is *injective*, then it follows that $[L^* : M^*] = \#(L^*/M^*) \leq \#Y \leq n$ and we will be done.

In order to prove that E is injective, assume that $E(gM^*) = E(hM^*)$, that is, $g(\alpha) = h(\alpha)$. Then $g^{-1}h(\alpha) = \alpha$. Now $g^{-1}h$ preserves L pointwise (as both g and h do) and it preserves α, so it preserves $L(\alpha) = M$ pointwise. So $g^{-1}h \in M^*$, that is, $gM^* = hM^*$. This proves that E is injective and the proof is finished. □

Proposition 78. Let $G = \mathrm{Gal}(N/K)$ and let $J \subset H \subset G$ be subgroups such that $[H : J] = n < \infty$. Then $[J^\dagger : H^\dagger] \leq n$.

Proof. Let $g \in H$ and $x \in J^\dagger$. Then $g(x)$ depends only on the coset $C := gJ$ (and x) and we shall write $C(x) := g(x)$ in the proof that follows.

Let $u_0, \ldots, u_n \in J^\dagger$. We need to prove that $u_0, \ldots, u_n$ are $H^\dagger$-dependent, that is, we need to find $a_0, \ldots, a_n \in H^\dagger$, not all zero, such that $\sum_i a_i\, u_i = 0$.

Write $H/J = \{C_1, \ldots, C_n\}$. Consider the equations

$$\sum_{i=0}^{n} a_i \cdot C_j(u_i) = 0 \qquad \text{for all } j \in \{1, \ldots, n\}. \tag{79}$$

These are n linear equations (with coefficients in $J^\dagger$) in $n+1$ unknowns a_i which for the moment are allowed to be in $J^\dagger$. By linear algebra, there is a nonzero solution $(a_i)_i$ to (79). Pick a nonzero solution with $\#\{i \mid a_i = 0\}$ maximal. After rescaling and renumbering we may suppose that $a_0 = 1$. The proof will be finished by proving that $a_i \in H^\dagger$ for all i. To this end, let $g \in H$. We need to show that $g(a_i) = a_i$ for all i.

Applying g to (79) gives

$$\sum_{i=0}^{n} g(a_i) \cdot g(C_j(u_i)) = 0 \qquad \text{for all } j \in \{1, \ldots, n\}.$$

Now $\{gC_1, \ldots, gC_n\} = \{C_1, \ldots, C_n\}$; only the order may be different. So

$$\sum_{i=0}^{n} g(a_i) \cdot C_j(u_i) = 0 \qquad \text{for all } j \in \{1, \ldots, n\}.$$

This means that $(g(a_i))_i$ is another solution to (79). Put $b_i := g(a_i) - a_i$. Then $(b_i)_i$ is a solution to (79) with more zero entries than $(a_i)_i$ because $b_0 = g(a_0) - a_0 = g(1) - 1 = 1 - 1 = 0$ (and $b_i = 0$ whenever $a_i = 0$). But we took $\{i \mid a_i = 0\}$ to be maximal, so $b_i = 0$ for all i. So $g(a_i) = a_i$ for all i and the proof is finished. □

4.4 The main theorem of Galois theory

For a group G acting on a field M we write

$$M^G := \{x \in M \mid g(x) = x \text{ for all } g \in G\}.$$

The automorphism group of a field M is written $\mathrm{Aut}(M)$.

Definition 80. The field extension M/K is said to be a **Galois extension** if there exists a subgroup $G \subset \mathrm{Aut}(M)$ such that $K = M^G$. We also say that M is Galois over K in this case.

Let us repeat this important definition in different words. The extension M/K is Galois if and only if, for all $x \in M$ not in K, there exists $g \in \mathrm{Gal}(M/K)$ such that $g(x) \neq x$. Also, M/K is Galois if and only if K is a closed intermediate field of the extension M/K.

The most important theorem in the course is the following:

Theorem 81. Let M/K be a finite Galois extension and let G, $\mathcal{F}$, $\mathcal{G}$, $\dagger$, $*$ be as usual, as explained in section 4.2.

(a) The set of subgroups of G is precisely $\mathcal{G}$. The set of intermediate fields of M/K is precisely $\mathcal{F}$.

(b) (Main theorem of Galois theory). There exists a bijection from the set of subgroups of G to the set of intermediate fields of M/K given by $H \mapsto H^\dagger$ and whose inverse is $L \mapsto L^*$.

(c) Let $H \subset J \subset G$ be subgroups. Then $[J : H] = [H^\dagger : J^\dagger]$.

Proof. Proof of (a). Recall that every element of $\mathcal{F}$ is an intermediate field of M/K by exercise 4.5. In order to prove the converse, let L be a subfield of M containing K. Note that $K = K^{*\dagger}$ because M/K is Galois. Therefore

$$\begin{aligned}[L^{*\dagger} : K] &= [L^{*\dagger} : K^{*\dagger}] \\ &\leq [K^{*} : L^{*}] && \text{by proposition 78} \\ &\leq [L : K] && \text{by proposition 77.}\end{aligned}$$

Also, $L \subset L^{*\dagger}$ by proposition 71b and $[L : K] < \infty$. Therefore $L = L^{*\dagger}$ and $L \in \mathcal{F}$. The proof that every subgroup of G is closed is similar. This finishes the proof of (a). Part (b) follows immediately from part (a) and proposition 76. Part (c) is an exercise. □

Remark 82. Theorem 81 can be extended to infinite field extensions but this is not on our syllabus. It turns out that again all intermediate fields are closed, but the subgroups of G are not necessarily closed. Instead, G becomes a topological group and a subgroup of G is closed in our sense if and only if it is closed in the topological sense.

4.5 Examples

There are three ways to obtain examples of field extensions M/K:

(a) Let M be a known field and let G be a subgroup of $\mathrm{Aut}(M)$. Then put $K = M^G$.

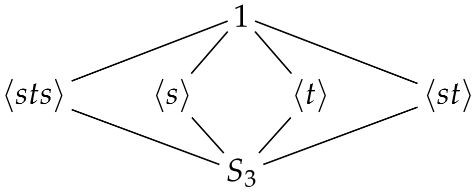
(b) Let N be a known field, for example $\mathbb{C}$. Define $M, K \subset N$ by specifying generators.

(c) Let K be a known field. Let M be obtained by adjoining a root of a specified irreducible polynomial in $K[X]$ as can be done in an essentially unique way by proposition 63. Make a tower of fields if necessary by repeating the process.

The techniques provided by this chapter suffice to deal with examples as in (a). Examples of (b) and (c) (which are essentially equivalent to each other) are best dealt with after the next two chapters though we shall already work out one such example below.

Example 83: Subgroups of S_3. If you deal with a Galois extension whose Galois group isomorphic to S_3, the symmetric group on 3 objects, it may be useful to know its subgroups and some more properties which we collect here without proof.

Let G be a group generated by s, t and suppose that s, t have order 2 and st has order 3. Then G is isomorphic to S_3. An isomorphism is given by $\phi\colon G \to S_3$, $\phi(s) = (12)$, $\phi(t) = (23)$. Here are all subgroups of S_3.



Example 84. Let $K = \mathbb{C}(X)$ be the field of rational functions in z over $\mathbb{C}$. Let $\omega = \exp(2\pi i/3)$. Define $s, t \in \mathrm{Gal}(K/\mathbb{C})$ by

$$s(X) = X^{-1}, \qquad t(X) = \omega X^{-1}.$$

Put $G := \langle s, t\rangle$, the group generated by s and t. By theorem 81b, there exists a bijection between the subgroups of G and the fields between K and K^G: the intermediate field corresponding to a subgroup H of G is K^H.

(a) Prove $K^{\langle s\rangle} = \mathbb{C}(X + X^{-1})$.

(b) Prove $G \cong S_3$.

(c) List the subgroups of G (by giving generators) and the corresponding fields between K, K^G (by generators).

Warning. The symbols s, t are not functions of one variable. If they were then one would have, for example,

$$s(1 + X) = (1 + X)^{-1} \qquad (???)$$

which is wrong. Correct is

$$s(1 + X) = s(1) + s(X) = 1 + X^{-1}$$

because s is a field automorphism.

Solution. (a). Write $u = X + X^{-1}$. We have $\mathbb{C}(u) \subset K^{\langle s\rangle}$ because

$$s(u) = s(X + X^{-1}) = s(X) + s(X^{-1}) = X^{-1} + X = u.$$

By theorem 81c we have $[K : K^{\langle s\rangle}] = \#\langle s\rangle = 2$. On writing $d = [K : \mathbb{C}(u)]$ we have $d \leq 2$ because X is a root of the degree 2 polynomial

$$Y^2 - uY + 1$$

in $\mathbb{C}(u)[Y]$. By the tower law we must have $d = 2$ and $K^{\langle s\rangle} = \mathbb{C}(u)$.

$$\begin{tikzcd}
& \mathbb{C}(X) = K \arrow[dd, dash, "d"] \\
K^{\langle s\rangle} \arrow[ur, dash, "2"] \arrow[dr, dash] & \\
& \mathbb{C}(w)
\end{tikzcd}$$

(b). We have $st(X) = s(\omega X^{-1}) = \omega X$ so st has order 3. Now G is generated by s, t and the orders of s, t, st are $2, 2, 3$, so $G \cong S_3$.

(c). The subgroups of G were listed in example 83. Each subgroup $H \subset G$ corresponds to an intermediate field K^H by theorem 81. We claim that each intermediate fields is generated over $\mathbb{C}$ by a single function f as follows.

subgroup	1	$\langle s\rangle$	$\langle t\rangle$	$\langle sts\rangle$	$\langle st\rangle$	G
f	X	$X + X^{-1}$	$X + \omega X^{-1}$	$X + \omega^2 X^{-1}$	X^3	$X^3 + X^{-3}$

Let us explain an **algorithm** for finding K^H by the example of $H = G$. We immediately see that $\mathbb{C} \subset K^G$. But K^G is bigger than $\mathbb{C}$ and we need to find more elements in K^G.

Step 1. *Choose any element α of K.* Let us choose $\alpha = X$.

Step 2. *Compute the orbit $A = \{h(\alpha) \mid h \in H\}$.* In our case, this is

$$\{X, \quad \omega X, \quad \omega^2 X, \quad X^{-1}, \quad \omega X^{-1}, \quad \omega^2 X^{-1}\}.$$

Step 3. *Choose a symmetric function f in $\#A$ variables and substitute the elements of the orbit A for those variables. The result is an element of K^H.* In our example, let us choose $f = U_1 + \cdots + U_6$, the sum of six variables. Plugging the elements of A in gives $f(A) = 0$.

Step 4. *Find out if K^H is generated by the element(s) we found.* Well, K^G is not generated by $\mathbb{C} \cup \{0\}$.

In unsuccesful cases like this we go back to step 3 or step 1 and repeat. Let us next take f to be the sum of the squares. The sum of the squares of the elements of A is again 0. Still no luck! But the sum of the cubes is $3(X^3 + X^3)$. Therefore we have $\mathbb{C}(X^3 + X^{-3}) \subset K^G$. In fact, these fields are equal. In part (a) we saw an example of how to prove that two fields like this are equal. □

Example 85. Here is a baby example of things discussed at length in chapter 6. Let L/K be an extension of degree 2 and suppose that K has characteristic $\neq 2$. Prove that L/K is Galois and that its Galois group is of order 2.

Solution. Let α be an element of L but not of K. Then $L = K(\alpha)$ (by the tower law for example). Let $f \in K[X]$ be the minimum polynomial of α over K. Then $\deg f = 2$ by proposition 58. Since $X - \alpha$ divides f in $L[X]$ there exists $\beta \in L$ such that $f = (X - \alpha)(X - \beta)$. Therefore the minimum polynomial of β is also f. By uniqueness of field extensions (proposition 63b) there exists $h \in \mathrm{Gal}(L/K)$ such that $h(\alpha) = \beta$. We have $\alpha \neq \beta$ because otherwise $K[X] \ni f = (X - \alpha)^2 = X^2 - 2\alpha X + \alpha^2$ so $2\alpha \in K$ so $\alpha \in K$ because 2 is invertible in K, a contradiction. It follows that L/K is Galois. The Galois group is of order 2 by theorem 81c. □

4.6 Exercises

(4.6) In this exercise you will fill some gaps in example 84.

(1) Prove that $K^{\langle st \rangle} = \mathbb{C}(X^3)$.

(2) Prove that $K^G = \mathbb{C}(v)$ where $v = X^3 + X^{-3}$.

(3) Compute the minimum polynomial of $u = X + X^{-1}$ over $\mathbb{C}(v)$.

(4.7) Let K be a field and $M = K(Z)$ the field of rational functions in a variable Z. Let $G \subset \mathrm{Gal}(M/K)$ be the subgroup generated by

$$s\colon Z \mapsto 1 - Z \qquad \text{and} \qquad t\colon Z \mapsto Z^{-1}$$

and $L = M^G$.

(a) Prove that the orders of (respectively) s, t, st are (respectively) $2, 2, 3$. [It follows that there is an isomorphism $G \to S_3$, $s \mapsto (12)$, $t \mapsto (23)$, don't prove this.]

(b) Write
$$y = \frac{Z^3 - 3Z + 1}{Z(Z-1)}.$$
Prove $M^{\langle st \rangle} = K(y)$.

(c) Prove $y + s(y) = 3$.

(d) Deduce from (c) that $L = K(w)$ where $w = y\,s(y)$. [This can be done without many calculations.]

(e) List all subgroups of G (by group generators) and the corresponding intermediate fields (by field generators). Proofs are not necessary.

(f) Let $P \subset Q$ be fields. Let $a \in P$ and write
$$f = (X^3 - 3X + 1) - a\,X(X-1) \in P[X].$$
Suppose that f has a root $u \in Q$. Prove that there are $v, w \in Q$ such that $f = (X-u)(X-v)(X-w)$. Prove also that if $\operatorname{char} P \neq 3$ then Q/P is Galois.

(4.8) Finish the proof of theorem 81a, that is, prove that every subgroup of G is closed.

(4.9) Prove theorem 81c, that is, $[J : H] = [H^\dagger : J^\dagger]$.

(4.10) Let M/K be an extension of degree $d < \infty$. Suppose that $\mathrm{Gal}(M/K)$ has t elements. Prove that $t \leq d$. Prove that $t = d$ if and only if M/K is Galois.

(4.11) Let $n \geq 1$. Prove that the extension $\mathbb{C}(X)/\mathbb{C}(X^n)$ is Galois. Prove that $\mathbb{Q}(X)/\mathbb{Q}(X^3)$ is not.

(4.12) In this exercise you prove that every finite group is (isomorphic to) a Galois group. Let G be a finite group.

(a) Suppose that G acts faithfully on a field M (recall that faithful means that if $g \in G$ is such that $g(x) = x$ for all $x \in M$ then $g = 1$). Let $K = M^G := \{x \in M \mid g(x) = x \text{ for all } g \in G\}$. Prove that M/K is Galois and that $\mathrm{Gal}(M/K) \cong G$.

(b) Prove that there exists a field M and a faithful G-action on it. Hint: Let G act on $\mathbb{Q}(X_1, \ldots, X_n)$ for appropriate n by permuting the variables.

(4.13) Let $K \subset N$ be fields and write $G = \mathrm{Gal}(N/K)$.

(a) Suppose that $K \subset L \subset M \subset N$ are fields. Suppose that L is closed and that $[M : L] = n < \infty$. Then M is also closed, and $[L^* : M^*] = n$

(b) Let $H \subset J \subset G$ be subgroups. Suppose that H is closed and that $[J : H] = n < \infty$. Then J is also closed, and $[H^\dagger : J^\dagger] = n$.

(4.14) Let $K \subset M$ be fields and write $G = \mathrm{Gal}(M/K)$.

(a) Prove that all finite subgroups of G are closed.

(b) Suppose that M/K is Galois and let L be an intermediate field of M/K with $[L : K]$ finite. Prove that M/L is Galois.

(4.15) Let K be an infinite field, $M = K(X)$, $G = \mathrm{Gal}(M/K)$.

(a) Prove that M is Galois over K.

(b) Prove that the only closed subgroups of G are the finite subgroups and G itself.

(4.16) Consider the field extension $\mathbb{Q}(X)/\mathbb{Q}$. Prove that the intermediate field $\mathbb{Q}(X^2)$ is closed but $\mathbb{Q}(X^3)$ is not.

(4.17) Let $K \subset L \subset M$ be fields with L/K and M/L Galois. Assume that any automorphism of L/K can be extended to M. Prove that M/K is Galois.

(4.18) Let M/K be a finite extension and let G, $\mathcal{F}$, $\mathcal{G}$, $\dagger$, $*$ be as usual. Prove that all subgroups of G are closed. Describe all closed intermediate fields.

(4.19) Let K be a field and $n \geq 1$. Let $\mathrm{GL}(n, K)$ be the group of invertible $n \times n$ matrices or equivalently, the group of invertible K-linear maps from K^n to itself.

(a) Prove that there exists a $\mathrm{GL}(2, K)$-action on the field $K(X)$ by K-automorphisms, defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (X) = \frac{aX + b}{cX + d}.$$

(b) Prove that an element of $\mathrm{GL}(2, K)$ acts trivially on $K(X)$ if and only if it is scalar. Notation: we let H denote the group of scalar elements and put

$$\mathrm{PGL}(2, K) := \mathrm{GL}(2, K)/H.$$

We have shown that $\mathrm{PGL}(2, K)$ is a subgroup of $\mathrm{Gal}(K(X), K)$.

(c) Prove that $\mathrm{PGL}(2, K) = \mathrm{Gal}(K(X)/K)$. Notation: as usual, $\mathrm{PGL}(2, K)$ acts on the set of 1-dimensional linear subspaces of K^2. Instead of the subspaces

$$K\binom{a}{1}, \text{ respectively, } K\binom{1}{0}$$

where $a \in K$ we simply write a, respectively, ∞. Thus we obtain a $\mathrm{Gal}(K(X)/K)$-action on $K \cup \{\infty\}$. Roughly, it is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (t) = \frac{at + b}{ct + d}$$

for all $t \in K \cup \{\infty\}$.

(4.20) Let K be a field. The **degree** of a rational function $r \in K(X)$ is defined to be $\max(\deg p, \deg q)$ where $p, q \in K[X]$ are any coprime polynomials such that $p/q = r$.

(a) Prove that if $r \in K(X)$ is not in K then $[K(X) : K(r)]$ is the degree of r in the above sense.

(b) Deduce that if $r, s \in K(X)$ then $\deg(r \circ s) = \deg(r) \deg(s)$ where $\circ$ denotes composition (s substituted for X in r).

(4.21) Let K be a field of characteristic $\neq 3$ and write $L = K(X)$. Let $\alpha \in K$ be a primitive cube root of unity. Define $s, t \in \mathrm{Gal}(K(X)/K)$ by

$$s(X) = \alpha X, \qquad t(X) = \frac{-X+1}{2X+1}$$

and write $G = \langle s, t \rangle$. (You may wish to skip parts (a) and (b) and instead simply assume that G has 12 elements).

(a) Prove: G preserves $\{0, 1, \alpha, \alpha^2\}$ where we use the $\mathrm{Gal}(K(X)/K)$-action on $K \cup \{\infty\}$ constructed in exercise 4.19.

(b) Prove that G is isomorphic to the alternating group A_4.

(c) Find $p, q \in K[X]$ of degree at most 12 such that $r := p/q$ is in L^G but not in K. Hint: why does the G-orbit of X^3 have at most 4 elements?

(d) Deduce that $L = K(r)$.

(4.22) Let K be a finite field of q elements. Recall that $G := \mathrm{Gal}(K(X)/K)$ consists of the elements taking X to

$$\frac{aX+b}{cX+d}$$

for some $a, b, c, d \in K$ with $ad - bc \neq 0$. Define $s \in G$ by $s(X) = X + 1$ and $H \subset G$ by

$$H = \big\{ X \mapsto aX + b \;\big|\; a, b \in K,\ a \neq 0 \big\}.$$

(a) Prove $K(X)^{\langle s \rangle} = K(f)$ where $f = X^q - X$. Hint: either use that the characteristic of K is a prime number dividing q, or that $X^q - X = \prod_{a \in K}(X - a)$.

(b) Prove $K(X)^H = K(f^{q-1})$.

(c) Find g such that $K(X)^G = K(g)$.

5 Normal subgroups and stability

Keywords: Algebraic extensions; finite extensions; finitely generated; normal subgroup; stable intermediate field.

5.1 *Algebraic field extensions*

Definition 86. A field extension $K \subset L$ is said to be **algebraic** if every element of L is algebraic over K. A field extension $K \subset L$ is called **finite** if its degree $[L : K]$ is finite.

Proposition 87. Every finite field extension is an algebraic extension.

Proof. Let L/K be a finite extension, say, of degree n. Let $\alpha \in L$. We must prove that α is algebraic over K. Now $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n+1$ elements in the n-dimensional vector space L over K and are therefore independent. That is, we have $\sum_{i=0}^{n} c_i \alpha^i = 0$ for some $c_i \in K$, not all zero. Write $f = \sum_{i=0}^{n} c_i X^i \in K[X]$. Then $f(\alpha) = 0$ and f is nonzero. This proves that α is algebraic over K as required. □

Proposition 88. Let M/K be fields. Let L be the set of elements of M that are algebraic over K. Then L is a subfield of M.

Proof. Let $\alpha, \beta \in L$. We must prove $K(\alpha, \beta) \subset L$. As α is algebraic over K, we have $[K(\alpha), K] < \infty$ by proposition 58e. Since β is algebraic over K it certainly is over $K(\alpha)$ and it follows that $[K(\alpha, \beta) : K(\alpha)]$ is finite. By the tower law, $[K(\alpha, \beta) : K]$ is finite as well. By proposition 87, $K(\alpha, \beta)$ is algebraic over K. This implies $K(\alpha, \beta) \subset L$ as promised. □

5.2 *Exercises*

(5.1) Let $\alpha \in \mathbb{C}$ be a root of $X^3 + \sqrt{3}\,X + \sqrt{5}$. Which of our theorems guarantee(s) that α is algebraic over $\mathbb{Q}$? Find a nonzero $f \in \mathbb{Q}[X]$ explicitly such that $f(\alpha) = 0$.

(5.2) Let K be a field and let α be an element of a larger field. Prove that α is algebraic over K if and only if $[K(\alpha) : K] < \infty$.

(5.3) Give an example of an infinite algebraic extension.

(5.4) Prove that a field extension is finite if and only if it is algebraic and finitely generated. (A field extension is said to be **finitely generated** if it is of the form $K \subset K(\alpha_1, \ldots, \alpha_n)$).

(5.5) Let $K \subset L \subset M$ be fields. Let $\alpha \in M$ and suppose that L/K is algebraic. Prove: if α is algebraic over L then it is algebraic over K.

5.3 Normal subgroups and stability

Let $K \subset M$ be fields and $f \in K[X]$. We say that f **factors completely over M** or **splits into linear factors over M** if all monic irreducible divisors of f in $M[X]$ have degree 1. Equivalently, f is of the form $c(X-a_1)\cdots(X-a_k)$ for some $c \in K^\times$ and $a_i \in M$.

If in addition to this $a_i \neq a_j$ whenever $i \neq j$ then we say that f **splits into distinct linear factors over M.**

Proposition 89. Suppose that M/K is Galois and f is a monic irreducible polynomial over K having a root u in M. Then f splits into distinct linear factors over M.

Proof. Let $u_1, \dots, u_r$ be the distinct elements of $\{\phi(u) \mid \phi \in \mathrm{Gal}(M/K)\}$. Each u_i is a root of f and so we have $r \leq \deg f$. Write $g = (X-u_1)\cdots(X-u_r)$. In order to show that $g \in K[X]$, observe that any automorphism of M/K merely permutes the u_i. It follows that any coefficient of g is fixed by all automorphisms of M/K, hence is in K because M/K is Galois. By proposition 58 it follows that f divides g in $K[X]$. Since also $\deg g \leq \deg f$ we deduce $f = g$. By construction, g factors over M into distinct linear factors; hence so does f. □

Recall that a subgroup H of a group G is called **normal** if $gHg^{-1} = H$ for all $g \in G$. If H is a normal subgroup of G then G/H is a group.

Definition 90. Let $K \subset L \subset M$ be fields. We say that L is **stable (relative to K and M)** if $\phi(L) \subset L$ for all $\phi \in \mathrm{Gal}(M/K)$.

Although for stable L the definition only gives $\phi(L) \subset L$ it is even true that $\phi(L) = L$ because also $\phi^{-1}(L) \subset L$.

Theorem 91. Let $K \subset L \subset M$ be fields. Suppose that M/K is finite and Galois and write $G = \mathrm{Gal}(M/K)$. Then the following are equivalent.

(a) L^* is a normal subgroup of G.

(b) L is stable (relative to K and M).

(c) L is Galois over K.

If these are true then G/L^* is isomorphic to $\mathrm{Gal}(L/K)$.

Proof. Proof of (b) ⇒ (a). We must show that if $s \in G$ and $t \in L^*$ then $s^{-1}ts \in L^*$. That is, given $x \in L$ we must prove $s^{-1}ts(x) = x$ or its equivalent $ts(x) = s(x)$. But this is true since $x \in L$ and L is stable, whence $s(x) \in L$.

Proof of (a) ⇒ (b). The proof is essentially the above read backwards. Given any $x \in L$ and $s \in G$ we must prove $s(x) \in L$. That is, we must show $ts(x) = s(x)$ for all $t \in H$ or its equivalent $s^{-1}ts(x) = x$. But this is true because $x \in L$ and $s^{-1}ts \in L^*$.

Proof of (b) ⇒ (c). Let $x \in L$. We must find $\phi \in \mathrm{Gal}(L/K)$ such that $\phi(x) \neq x$. As M/K is Galois, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(x) \neq x$. We have $\sigma(L) = L$ because L is stable. Define ϕ to be the restriction of σ to

L. Then ϕ has the required properties.

Proof of (c) $\Rightarrow$ (b). Note that L/K is finite and therefore algebraic by proposition 87. Let $u \in L$ and $s \in \mathrm{Gal}(M/K)$. We know that u is algebraic over K; let f be its minimum polynomial over K. By proposition 89, f factors completely in L. Since $s(u)$ is a root of f, it must be in L.

Proof of the final statement. We shall define a group homomorphism $h\colon G = \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$. If $s \in G$ then $h(s)$ will be the restriction of s to L. It is clear that h is a group homomorphism. The kernel of h is L^* so by the first isomorphism theorem for groups, the image of h is isomorphic to G/L^*. Also, G/L^* and $\mathrm{Gal}(L/K)$ have equal (finite) cardinalities by theorem 81c and the result follows. □

5.4 Exercises

(5.6) Let $t \in \mathrm{Gal}(N/K)$. Let L, M be intermediate fields and $H, J \subset G$ be subgroups.

(a) If $M = t(L)$ then $L^* = t^{-1}M^*t$.

(b) If $t^{-1}Ht = J$ then $H^\dagger = t(J^\dagger)$.

(5.7) Let $G = \mathrm{Gal}(M/K)$ and L a closed intermediate field. Show

$$\{g \in G \mid g(L) = L\} = \{g \in G \mid gL^* = L^*g\}.$$

(5.8) Give an example of fields $K \subset L \subset M$ such that M/K is Galois, L is closed, L/K is Galois, yet L is not stable.

6 Splitting fields

Keywords: Splitting field; derivative; separable.

6.1 *Splitting fields*

Definition 92. Let $K \subset M$ be fields and let $f \in K[X]$. We say that M is a **splitting field** for f over K if f factors completely over M and M is generated by K and the roots of f in M.

This is the usual name though it would be more consistent to call it a *splitting extension.*

If there is no need to call attention to the polynomial we shall simply say that M is a splitting field over K.

Note that by exercise 5.4, any splitting field over K is of finite degree over K.

Example 93. Consider $f = X^3 - 2$. The complex roots of f are α, $\alpha\varepsilon$, $\alpha\varepsilon^2$ where $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\varepsilon = \exp(2\pi i/3) \in \mathbb{C}$. It follows that $L := \mathbb{Q}(\alpha, \alpha\varepsilon, \alpha\varepsilon^2)$ is a splitting field for f over $\mathbb{Q}$. We only need two generators: $L = \mathbb{Q}(\alpha, \varepsilon)$. So far we have no method of proving that L is Galois over $\mathbb{Q}$; from the results in this chapter, it will follow almost immediately that it is.

Proposition 94: Existence and uniqueness of splitting fields.

(a) Let f be a polynomial over a field K. Then there exists a splitting field for f over K.

(b) For all $i \in \{1,2\}$, let M_i/K_i be a splitting field for $f_i \in K_i[X]$ over K_i. Let $s\colon K_1[X] \to K_2[X]$ be an isomorphism such that $s(K_1) = K_2$, $s(X) = X$ and $s(f_1) = f_2$. Then the restriction of s to K_1 extends to an isomorphism $M_1 \to M_2$.

Proof. Proof of (a). Induction on the degree of f. If f is constant then $M = K$ will do. Suppose now that the degree of f is positive. Let g be an irreducible factor of f. By proposition 63 there exists an extension $K(\alpha)/K$ such that $g(\alpha) = 0$. There exists a polynomial h with coefficients in $K(\alpha)$ such that $f = (X - \alpha) \cdot h$. By the induction hypothesis, there exists a splitting field L for h over $K(\alpha)$. We claim that L is a splitting field for f over K. Indeed, f factors completely over L because h does. Moreover, L is generated by $K(\alpha)$ and the roots of h; it follows that L is generated by the roots of f. This proves that our claim that L is a splitting field for f over K.

Proof of (b). Induction on $d = [M_1 : K_1]$. If $d = 1$ then f_1 factors completely over K_1. Therefore so does f_2 over K_2 and $M_2 = K_2$.

Let now $d > 1$. We may assume that f_1 has an irreducible factor g_1 of degree greater than 1. Write $g_2 = s(g_1)$. For all $i \in \{1,2\}$, let α_i be a root of g_i in M_i. By proposition 63 the isomorphism $s\colon K_1 \to K_2$ can be extended to an isomorphism $K_1(\alpha_1) \to K_2(\alpha_2)$. Then M_i is a splitting field for f_i over $K(\alpha_i)$ for all $i \in \{1,2\}$ (exercise). Since $[M_1 : K_1(\alpha_1)] < [M_1 : K_1]$

the induction hypothesis implies that our isomorphism $K_1(\alpha_1) \to K_2(\alpha_2)$ extends to an isomorphism $M_1 \to M_2$. □

Definition 95. The **derivative** of a polynomial $f \in K[X]$ in one variable is defined as follows: writing $f = \sum_{\geq 0} a_n X^n$ we put $f' = \sum_{\geq 1} n\, a_n\, X^{n-1}$.

Exercise (6.1) Let $f, g \in K[X]$, $a, b \in K$. Prove that $(af + bg)' = af' + bg'$ and $(fg)' = f'g + fg'$.

(This is a straightforward calculation. You shouldn't use anything you may have learned in analysis about differentiation.)

Proposition 96. Let K be a field, $a \in K$ and $f \in K[X]$. Then $(X-a)^2$ divides f in $K[X]$ if and only if $X - a$ divides both f and f'.

Proof. Proof of $\Rightarrow$. If $f = (X-a)^2 g$ then $f' = (X-a)\big(2g + (X-a)g'\big)$, which is divisible by $X - a$ and of course so is f.

Proof of $\Leftarrow$. Suppose that $X - a$ divides both f and f'. By theorem 2 there are $q, r \in K[X]$ such that $f = (X-a)^2 q + r$ and $\deg r < 2$. Since $X - a \mid f$ we have $r = (X-a)c$ for some constant $c \in K$. Differentiation gives $f' = (X-a)\big(2g + (X-a)g'\big) + c$. Since $X - a \mid f'$ we find $c = 0$. It follows that $f = (X-a)^2 q$ as required. □

Proposition 97. Let K be a field let $f \in K[X]$ be irreducible. Then the following are equivalent.

(1) Let a be an element of a larger field L. Then f is not divisible by $(X-a)^2$ in $L[X]$. In words: f has no multiple root in any larger field.

(2) In some splitting field of f over K, f factors into distinct linear factors.

(3) $f' \neq 0$.

Proof. (1) $\Rightarrow$ (2) is clear.

Proof of (2) $\Rightarrow$ (3). Suppose on the contrary that $f' = 0$. Let L/K be a splitting field for f. As f is not constant, it has a root $a \in L$. Therefore $X - a$ divides both f and f' in $L[X]$. By proposition 96, $(X-a)^2$ divides f, a contradiction.

Proof of (3) $\Rightarrow$ (1). Since f is irreducible over K it generates a maximal ideal $(f) \subset K[X]$ by proposition 33. We have $f' \notin (f)$ by the assumption that $f' \neq 0$. Therefore there are $p, q \in K[X]$ such that $pf + qf' = 1$. It follows that in $L[X]$, f, f' have no common factor of the form $X - a$. By proposition 96, $(X-a)^2$ does not divide f. □

Definition 98. An irreducible polynomial $f \in K[X]$ is called **separable** if it satisfies the equivalent conditions of proposition 97. An element α, algebraic over K, is said to be **separable** over K if its minimum polynomial is separable over K. An algebraic field extension L/K is said to be **separable** if all elements of L are separable over K. To avoid ambiguity we shall not define separability over K of a polynomial unless it is irreducible over K.

Example 99. Here is the simplest example of a nonseparable extension.

Let p be a prime number and F a field of characteristic p. Let $L = F(T)$, the field of rational functions in a variable T. Put $K = F(T^p)$. Write $g = X^p - T^p \in K[X]$. We shall prove that g is irreducible over K and not separable.

In order to prove that g is irreducible over K, it is helpful to write U instead of T^p. We get $g = X^p - U$ which is Eisenstein at U in $F[U] = F[T^p]$ and is therefore irreducible over K.

On the other hand, $g = (X - T)^p$ so g has multiple roots in its splitting field. Therefore, g is not separable.

Notice also that L is a splitting field for g over K. The Galois group for L/K is trivial because if $s \in \mathrm{Gal}(L/K)$ then s takes the root T of g to a root of g; the only possibility is $s(T) = T$.

Exercise (6.2) Let $f \in K[X]$ be irreducible.

(a) Suppose that the characteristic of K is 0. Then f is separable.

(b) Suppose that the characteristic of K is a prime number p. Then f is inseparable if and only if there exists a polynomial g such that $f = g(X^p)$.

The following is the second most important result in our course. The implications [2 ⇒ 1] and [3 ⇒ 1] are often used in applications.

Theorem 100. Let M/K be a finite field extension. The following are equivalent:

(1) M/K is Galois.

(2) M/K is separable and a splitting field.

(3) M/K is a splitting field for a polynomial f whose irreducible factors are separable.

Proof. Proof of (1) ⇒ (2). Let u be an element of M and f its minimum polynomial over K. By proposition 89, f factors over M into distinct linear factors. Therefore u is separable over K. As this is true for every $u \in M$, the extension M/K is separable.

Let $v_1, \ldots, v_r$ be a K-basis of M, let f_i be the minimum polynomial of v_i over K, and write $g = f_1 \cdots f_r$. By proposition 89 again, each f_i factors completely in M and hence so does g. This shows that M is a splitting field of g over K.

Proof of (2) ⇒ (3). Suppose that M is a splitting field of f over K. Let $f = f_1 \cdots f_r$ be the factorisation of f into irreducible factors over K. Each f_i is the minimum polynomial for an element in M which is by assumption separable over K. Hence each f_i is separable over K.

Proof of (3) ⇒ (1). Suppose that M is a splitting field over K of a polynomial f whose irreducible factors are separable. Let $G = \mathrm{Gal}(M/K)$. By exercise 4.10, in order to prove that M/K is Galois, it suffices to prove that $\#G \geq [M : K]$. We shall show this by induction on $d = [M : K]$. If $d = 1$ there is nothing to prove.

Suppose now that $d > 1$. Let g be an irreducible factor of f of degree greater than 1; such a g exists because $d > 1$. Let $u \in M$ be a root of g. Let $u_1, \ldots, u_r$ be the roots of g in M (say, $u = u_1$), and let i be such that $1 \leq$

$i \leq r$. By proposition 63 (uniqueness of primitive extensions) there exists a K-isomorphism h_i: $K(u) \to K(u_i)$ taking u to u_i. Now $[M : K(u_i)] = d/r < d$ so by the induction hypothesis, there are at least d/r ways to extend h_i to a K-automorphism of M. As i varies this yields d distinct elements of G as required. □

6.2 *Actions of Galois groups*

In order to determine the structure of a Galois group in practice, it is useful to embed it into S_n. This can be done as follows. See section 2.5 for the basics on group actions.

Lemma 101. Let L/K be an extension and write $G = \mathrm{Gal}(L/K)$. Let $U \subset L$ be a G-invariant subset of L; then the G-action on L restricts to a G-action on U, that is, to a homomorphism s: $G \to \mathrm{Sym}(U)$.

(a) Suppose that $L = K(U)$, that is, L is generated over K by U. Then s is injective.

(b) Suppose that L/K is a splitting field for $f \in K[X]$ and that U is the set of roots in L of f. Then U is G-invariant and $L = K(U)$. In particular, G acts faithfully on U.

Proof. (a). Suppose that $g \in G$ is such that $s(g) = 1$. Then g preserves U pointwise. Therefore g preserves any element in the ring $K[U]$ by proposition 62b and indeed any element in the field $K(U) = L$. This shows that $g = 1$ and that s is injective.

(b). Proof that U is G-invariant. Let $u \in U$, $s \in G$. Then $f(s(u)) = s(f(u)) = s(0) = 0$ where the first equality is by lemma 62b. This shows $s(u) \in U$ as required.

Proof that the G-action on U is faithful. Note that this means by definition that the corresponding homomorphism $G \to \mathrm{Sym}(U)$ is injective. It is true by part (a) and the fact that $L = K(U)$. □

6.3 *Examples*

Example 102. Let $n \geq 1$ and let $\varepsilon \in \mathbb{C}$ be a primitive n-th root of unity. Prove that $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois.

Solution. Let $f = X^n - 1$. By (2) $\Rightarrow$ (1) in theorem 100 it suffices to prove that $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is separable and a splitting field of f.

We have the factorisation

$$f = \prod_{i=0}^{n-1} (X - \varepsilon^i).$$

To prove this, observe that $X - \varepsilon^i$ divides f in $\mathbb{C}[X]$. Therefore the least common multiple $\prod_{i=0}^{n-1}(X - \varepsilon^i)$ divides f. The argument is finished by looking at the leading terms.

But each root ε^i is in $\mathbb{Q}(\varepsilon)$. It follows that f factors completely over $\mathbb{Q}(\varepsilon)$. Also, $\mathbb{Q}(\varepsilon)$ is generated by $\mathbb{Q}$ and the roots $1, \varepsilon, \ldots, \varepsilon^{n-1}$ of f, thus proving that $\mathbb{Q}(\varepsilon)$ is a splitting field for f over $\mathbb{Q}$.

Moreover, $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is separable because the characteristic is 0. By (2) $\Rightarrow$ (1) in theorem 100, $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois.

Alternatively, one can avoid the characteristic 0 argument because we have even proved that f splits into *distinct* linear factors over $\mathbb{Q}(\varepsilon)$ which again implies that $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois by (3) $\Rightarrow$ (1) in theorem 100. □

The surprise in the above example is that all roots of $X^n - 1$ can be expressed in terms of just one of them.

Example 103. Put $L = \mathbb{Q}(\sqrt{2}, \sqrt{5}) \subset \mathbb{C}$.

(a) Prove that $L/\mathbb{Q}$ is Galois.

(b) Which standard group is isomorphic to the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$?

(c) List all subgroups of G (by generators) and the corresponding intermediate fields (also by generators).

Solution. (a). It is clear that L is a splitting field over $\mathbb{Q}$ of $(X^2 - 2)(X^2 - 5)$. Also, L is separable over $\mathbb{Q}$ because the characteristic is 0. By theorem 100, $L/\mathbb{Q}$ is Galois.

(b). Let $G, \mathcal{F}, \mathcal{G}, \dagger, *$ be as usual. Every element of G takes $\sqrt{2}$ into $\{-\sqrt{2}, \sqrt{2}\}$ and $\sqrt{5}$ into $\{-\sqrt{5}, \sqrt{5}\}$. Moreover, an element of G is determined by where it takes $\sqrt{2}$ and $\sqrt{5}$. Therefore, there are at most 4 elements of G, which we can already identify as follows, although we don't know yet whether they exist.

$s \in G$	$s(\sqrt{2})$	$s(\sqrt{5})$
1	$\sqrt{2}$	$\sqrt{5}$
a	$\sqrt{2}$	$-\sqrt{5}$
b	$-\sqrt{2}$	$\sqrt{5}$
c	$-\sqrt{2}$	$-\sqrt{5}$

In example 67 we already showed that $[L : \mathbb{Q}] = 4$. By (a), $L/\mathbb{Q}$ is Galois, so by theorem 81 G has precisely 4 elements. Therefore, the elements in the table exist. From the table it is clear that $G \cong (\mathbb{Z}_2)^2$.

(c). Prove yourself that the answer is as follows.

subgroup	1	$\langle a \rangle$	$\langle b \rangle$	$\langle c \rangle$	G
field	L	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{10})$	$\mathbb{Q}$

□

Example 104: Subgroups of D_8. Let $n \geq 1$. The *dihedral group* D_{2n} of order $2n$ is the group of permutations of $\mathbb{Z}/n$ of the form $x \mapsto a + x$ or $x \mapsto a - x$ (with $a \in \mathbb{Z}/n$). We will freely use the following properties of D_8. It is generated by s, t defined by $s(x) = x + 1$, $t(x) = -x$. The subgroups of D_8

are the following.

$$\begin{tikzcd}
 & & 1 \arrow[dll, no head, bend right] \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] \arrow[drr, no head, bend left] & & \\
\langle t\rangle \arrow[dr, no head] & \langle s^2t\rangle \arrow[d, no head] & \langle s^2\rangle \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \langle st\rangle \arrow[d, no head] & \langle s^3t\rangle \arrow[dl, no head] \\
 & \langle s^2,t\rangle \arrow[dr, no head] & \langle s\rangle \arrow[d, no head] & \langle s^2,st\rangle \arrow[dl, no head] & \\
 & & G & &
\end{tikzcd} \tag{105}$$

Example 106: Biquadratic equation. Let L/K be a splitting field of

$$f = (X^2 - p)^2 - q.$$

Let $G = \mathrm{Gal}(L/K)$ and suppose $\#G \geq 8$. Let $\beta \in L$ be such that $\beta^2 = q$. Let $\alpha_1, \alpha_2 \in L$ be such that $\alpha_1^2 = p + \beta$, $\alpha_2^2 = p - \beta$.

(a) Prove that $f = (X - \alpha_1)(X + \alpha_1)(X - \alpha_2)(X + \alpha_2)$ and that f has 4 distinct roots.

(b) Let Γ be the graph whose vertices are the roots of f in L and such that θ_1, θ_2 are adjacent whenever $\theta_1 + \theta_2 \neq 0$.

Prove that G acts faithfully on Γ. Draw Γ. You may now assume that the automorphism group of Γ is isomorphic D_8. Prove that $G = \mathrm{Aut}(\Gamma)$.

(c) Prove that there are unique $s, t \in G$ such that

$$s(\alpha_1) = \alpha_2, \qquad s(\alpha_2) = -\alpha_1, \qquad t(\alpha_1) = \alpha_1, \qquad t(\alpha_2) = -\alpha_2.$$

(d) Define $\gamma = \alpha_1\alpha_2$, $\delta_1 = \alpha_1 + \alpha_2$, $\delta_2 = \alpha_1 - \alpha_2$. For each $H \in \mathcal{G}$ define $H^0 \in \mathcal{F}$ to be the field in the corresponding slot in figure 2. Prove that $H^\dagger \supset H^0$ for all $H \in \mathcal{G}$.

(e) Prove that if $H_1 \subset H_2 \subset G$ are groups and $[H_2 : H_1] = 2$ then $[H_1^0 : H_2^0] \leq 2$.

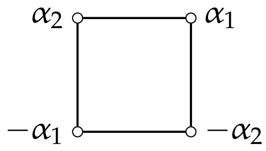
(f) Prove that $H^\dagger = H^0$ for all $H \in \mathcal{G}$.

Solution. (a). The factorisation of f follows from

$$\begin{aligned}
&(X - \alpha_1)(X + \alpha_1)(X - \alpha_2)(X + \alpha_2) = (X^2 - \alpha_1^2)(X^2 - \alpha_2^2) \\
&= (X^2 - (p + \beta))(X^2 - (p - \beta)) = (X^2 - p)^2 - \beta^2 \\
&= (X^2 - p)^2 - q = f.
\end{aligned}$$

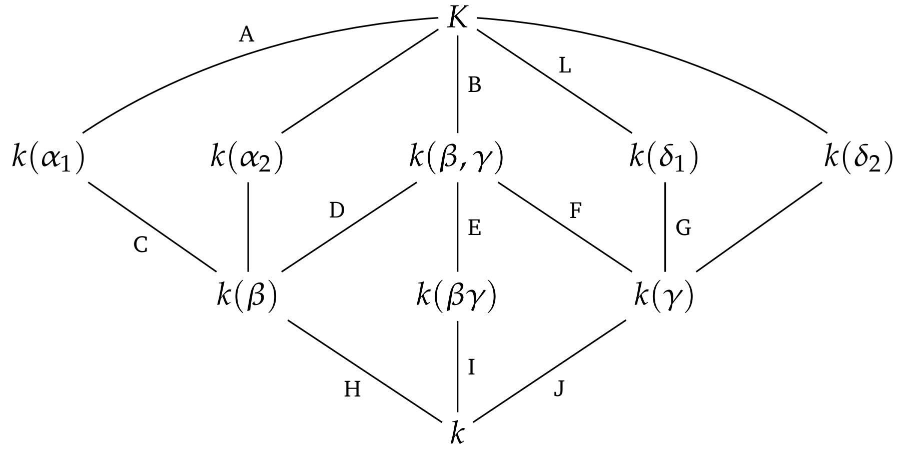
Suppose that f has precisely r distinct roots. So $r \leq 4$. As G consists of K-automorphisms and $f \in K[X]$ we have that G acts on the set of roots of f. This action is faithful because L is generated by the roots of f. Thus we have an injective homomorphism $G \to S_4$. So $8 = \#G \leq \#S_r = r!$ so $r \geq 4$.

(b).



The graph Γ.

Figure 2.



(107)

Let $g \in G$. We have seen in (a) that g permutes the roots in L of f, that is, the vertices of Γ. In order to prove that it takes edges to edges, let θ_1, θ_2 be vertices of Γ, that is, roots of f. Then

$$\begin{aligned} g(\theta_1), g(\theta_2) \text{ are adjacent} &\iff g(\theta_1) + g(\theta_2) = 0 \\ &\iff g(\theta_1 + \theta_2) = 0 \\ &\iff \theta_1 + \theta_2 = 0 \\ &\iff \theta_1, \theta_2 \text{ are adjacent.} \end{aligned}$$

This proves that G acts on Γ. The action is faithful by the same argument as in (a).

In other words, we have an injective homomorphism $G \to \mathrm{Aut}(\Gamma)$. We may assume that $\mathrm{Aut}(\Gamma)$ is isomorphic to D_8, in particular, has 8 elements. We know that G has at least 8 elements. Therefore G has precisely 8 elements and $G = \mathrm{Aut}(\Gamma)$.

(c). In (b), we already identified G with D_8. One easily checks that the elements of G corresponding to what we called s and t in example 104 act precisely on the roots of f the way specified.

(d). Note that $s(p+\beta) = s(\alpha_1^2) = \alpha_2^2 = p - \beta$ so $s(\beta) = -\beta$. Similarly, we have $t(p+\beta) = t(\alpha_1^2) = \alpha_1^2 = p + \beta$ so $t(\beta) = \beta$. So

$$s(\beta) = -\beta, \qquad s(\gamma) = -\gamma, \qquad t(\beta) = \beta, \qquad t(\gamma) = -\gamma.$$

The required inclusion $H^\dagger \supset H^0$ follows easily except for $K(\delta_i)$ which we handle as follows: $st(\delta_1) = st(\alpha_1 + \alpha_2) = s(\alpha_1 - \alpha_2) = \alpha_2 - (-\alpha_1) = \alpha_2 + \alpha_1 = \delta_1$ and similarly for $K(\delta_2)$.

(e). We do this case by case. In general, one proves that $[L(\theta) : L] \leq 2$ by writing down a quadratic equation over L satisfied by θ.

In case B we have $[K(\alpha_1) : K(\beta)] \leq 2$ by the equation $\alpha_1^2 = p + \beta$ (the cases are indicated next to the edges in figure 2). The same equation handles the cases A, B, C.

The equation $\beta^2 = q$ settles cases E, F, H. We have $\gamma^2 = \alpha_1^2\alpha_2^2 = (p+\beta)(p-\beta) = p^2 - q$ which handles J, D. We get $(\beta\gamma)^2 = q(p^2 - q)$ which settles case I.

Consider next case G. We have $\delta_1^2 = (\alpha_1+\alpha_2)^2 = \alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2 = (p+\beta) + 2\gamma + (p-\beta) = 2(p+\gamma)$. The equation

$$\delta_1^2 = 2(p+\gamma) \tag{108}$$

shows that δ_1 is of degree at most 2 over $K(\gamma)$.

Finally, we consider case L of $L/K(\delta_1)$. The characteristic is not 2 by part (a). So (108) implies that $\gamma \in K(\delta_1)$. Therefore $(X-\alpha_1)(X-\alpha_2) = X^2 - (\alpha_1+\alpha_2)X + \alpha_1\alpha_2 = X^2 - \delta_1 X + \gamma \in K(\delta_1)[X]$. This handles the case L.

The remaining cases are similar to the ones we have done.

(f). Let $H \in \mathcal{G}$. Then there is a chain of groups $1 = H_0 \subset H_1 \subset H_2 \subset H_3 = G$ such that $\#H_k = 2^k$ for all k and such that H is one of the H_i. By (e) we have $[H_i^0 : H_{i+1}^0] \le 2$. Multiplying over all $i \in \{0,1,2\}$ and the tower law yields

$$8 = [L:K] = [H_0^0 : H_3^0] = \prod_{i=0}^{2} [H_i^0 : H_{i+1}^0] \le 2^3 = 8.$$

So equality holds throughout. The same is true for $H_i^\dagger$ so $H_i^\dagger = H_i^0$ for all i. In particular, $H^\dagger = H^0$. □

Example 109. Let ε be a complex primitive fifth root of unity. Put $L = \mathbb{Q}(\varepsilon)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$.

(a) Prove that there exists a unique $s \in G$ such that $s(\varepsilon) = \varepsilon^2$.

(b) Prove that G is generated by s, and write down all subgroups of G by generators.

(c) Prove that $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\alpha)$ where $\alpha = \varepsilon + \varepsilon^2$.

Solution. (a). Uniqueness. The extension $L/\mathbb{Q}$ is generated by ε so any element of G is determined by what it does with ε. This proves uniqueness of σ.

Existence. Both ε and ε^2 are roots of the irreducible polynomial $\phi_5 \in \mathbb{Q}[X]$. By uniqueness of primitive extensions (proposition 63b) there exists a $\mathbb{Q}$-isomorphism $s\colon \mathbb{Q}(\varepsilon) \to \mathbb{Q}(\varepsilon^2)$ taking ε to ε^2. Then $s^2(\varepsilon) = s(\varepsilon^2) = \varepsilon^4$ and $s^4(\varepsilon) = (\varepsilon^4)^4 = \varepsilon^{16} = \varepsilon$. Therefore s is bijective and $s \in G$.

(b). In part (a) we already saw that $s^4 = 1$ and $s^2 \neq 1$, so s is of order 4. In example 102 we proved that $L/\mathbb{Q}$ is Galois. By theorem 81, the main theorem of Galois theory, it follows that $\#G = [L:\mathbb{Q}] = 4$. Therefore $G = \langle s \rangle$. The subgroups are 1, G and $\langle s^2 \rangle$.

(c). We know that $L/\mathbb{Q}$ is Galois. In particular, $\mathbb{Q}(\alpha) = \mathbb{Q}(\varepsilon)$ would be equivalent to $\mathbb{Q}(\alpha)^* = \mathbb{Q}(\varepsilon)^*$, that is, to $H = 1$ where we define $H = \mathbb{Q}(\alpha)^*$. Suppose that to the contrary $H \neq 1$. Then $s^2 \in H$ so $\varepsilon + \varepsilon^2 = \alpha = s^2(\alpha) = s^2(\varepsilon+\varepsilon^2) = \varepsilon^4 + \varepsilon^8 = \varepsilon^4 + \varepsilon^3$ whence $\varepsilon + \varepsilon^2 - \varepsilon^3 - \varepsilon^4 = 0$, a contradiction as the minimum polynomial of ε is $X^4 + X^3 + \cdots + 1$. This proves $H = 1$ as required.

Another solution to (c) would be to express ε explicitly in terms of α but that is likely to be more work. □

Example 110. Let $K \subset \mathbb{C}$ be the complex splitting field for $f = X^3 - 2$ over $\mathbb{Q}$ and put $G = \mathrm{Gal}(K/\mathbb{Q})$.

(a) Prove that $K/\mathbb{Q}$ is Galois.

(b) Prove that f is irreducible over $\mathbb{Q}$.

(c) Prove $[K : \mathbb{Q}] = 6$.

(d) Prove that $\#G = 6$.

(e) Prove $G \cong S^3$.

(f) List the subgroups of G and the intermediate fields.

Solution. (a). By assumption $K/\mathbb{Q}$ is a splitting field. It is also separable because the characteristic is 0. Now apply (2) $\Rightarrow$ (1) in theorem 100.

(b). The polynomial $f \in \mathbb{Z}[X]$ is Eisenstein at 2. Apply proposition 49.

(c). Put $\alpha = \sqrt[3]{2}$, $\omega = \exp(2\pi i/3)$. Then $K = \mathbb{Q}(\alpha, \omega)$. Also $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ because f is irreducible of degree 3 by (b) and α is a root of f. Moreover $[K : \mathbb{Q}(\alpha)] = 2$ because ω is a root of $X^2 + X + 1$ but is not in $\mathbb{R}$ while $\mathbb{Q}(\alpha) \subset \mathbb{R}$. Using the tower law we find $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 3 = 6$.

(d). Immediate from (a), (c) and the main theorem of Galois theory, theorem 81.

(e). The Galois group G acts faithfully on the set of roots of f, which is a set of three elements. That gives us an injective homomorphism $\phi\colon G \to S_3$. But G has 6 elements by (d), and S_3 has 6 elements too. So ϕ is bijective.

(f). Inspection of the isomorphism from (e) suggests that we define $s, t \in G$ by $s(\omega) = t(\omega) = \omega^2$, $s(\alpha) = \alpha$, $t(\alpha) = \alpha\omega^2$. We find the following intermediate fields.

subgroup	1	$\langle s\rangle$	$\langle t\rangle$	$\langle sts\rangle$	$\langle st\rangle$	G
field	K	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\alpha\omega)$	$\mathbb{Q}(\alpha\omega^2)$	$\mathbb{Q}(\omega)$	$\mathbb{Q}$

As an example we prove that $K^{\langle s\rangle} = \mathbb{Q}(\alpha)$. We have $s(\alpha) = \alpha$ so $K^{\langle s\rangle} \supset \mathbb{Q}(\alpha)$. Also

$$[K^{\langle s\rangle} : \mathbb{Q}] = [G : \langle s\rangle] = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

which proves $K^{\langle s\rangle} = \mathbb{Q}(\alpha)$. □

6.4 *Exercises*

(6.3) Give another solution to exercise 85 by using the results of this section. Namely, if K is a field of characteristic $\neq 2$ and L/K is an extension of degree 2 then L is Galois over K.

(6.4) Let $K(\alpha) = L$ be an algebraic extension of a field K and suppose that $\mathrm{mp}_K(\alpha)$ splits over L into distinct linear factors (that is, is a product of linear polynomials over L and has no multiple roots in L). Prove that $\#\,\mathrm{Gal}(L/K) = [L : K]$ two ways: (1) using no more than the results up to and including chapter 3; (2) using at least one theorem in the present chapter.

(6.5) Let $K \subset L \subset M$ be fields with L/K normal (possibly of infinite degree) and M/L a splitting field of a polynomial with coefficients in K whose irreducible factors over L are separable. Prove that M is Galois over K. [Hint: use exercise 4.17 and proposition 94b].

(6.6) Let K be a field and $f \in K[X]$ (not necessarily irreducible). Prove that f has a multiple root in some larger field if and only if f and f' have a common factor (of degree > 1).

(6.7) If $\alpha_1, \dots, \alpha_r$ are separable over K, prove that $K(\alpha_1, \dots, \alpha_r)$ is separable over K.

(6.8) Let $K = \mathbb{R}(T)$, the field of rational functions in one variable. Let $P \subset \mathbb{R}[T]$ be the ideal generated by t.

(a) Prove that P is a prime ideal.

(b) Prove that $f = X^4 - T \in \mathbb{R}[T][X]$ is Eisenstein at P.

(c) Let L be a splitting field for f over K. Prove that L contains a square root i of -1. Prove $[L : K] = 8$.

(d) Let $\alpha \in L$ be a root of f. Prove that every $g \in G := \mathrm{Gal}(L/K)$ preserves $A = \{\alpha, \alpha i, \alpha i^2, \alpha i^3\}$. Prove that every $g \in G$ preserves the graph with vertex set A and (unoriented) edges $\{\alpha\, i^k, \alpha\, i^{k+1}\}$ where $k \in \{0, 1, 2, 3\}$. Deduce that $G \cong D_8$.

[Hint: you may assume that D_8 is the automorphism group of the above graph, and has 8 elements.]

(e) Give two generators of G and their values at i, α. List all subgroups of G (by group generators), and the corresponding intermediate fields (by field generators). Show either in inclusion diagrams as on page 73 of the printed notes. Give a full proof for just one of the most difficult subgroups (choose yourself) and no proofs for the others.

(6.9) Let $L \subset \mathbb{C}$ be the splitting field of $X^4 - 2$. Prove that $L = \mathbb{Q}(i + \sqrt[4]{2})$. [Hint: Find at least five elements of the $\mathrm{Gal}(L/\mathbb{Q})$-orbit of $i + \sqrt[4]{2}$.]

(6.10) Let M/K be a splitting field of a polynomial $f \in K[X]$ of degree n. Prove that $[M : K]$ divides $n!$.

(6.11) (a) Let $K \subset L \subset M$ be fields with L a splitting field over K. Prove that L is stable.

(b) Let M be a splitting field over K and L an intermediate field. Prove that L is a splitting field over K if and only if L is stable. Show also that $G/L^* \cong \mathrm{Gal}(L/K)$.

(6.12) Suppose that $f = X^4 - 2cX^2 + d^2 \in k[x]$ is irreducible with $c, d \in k$. Show that if $\alpha \in L$ is a root of f in some extension field L, then so is d/α, and deduce that $K = k(\alpha)$ is already a splitting field of f.

(6.13) Let K be a field. Suppose that $f = x^4 - a \in K[x]$ has no root in K but is reducible. Prove that there exists $r \in K$ such that $a = r^2$ or $a = -4\,r^4$.

(6.14) Suppose that $f = X^4 - 2aX^2 + b \in k[X]$ is irreducible, and let K be a splitting field for f over k; prove that $[K:k] = 4$ or 8.

(6.15) Let K be the splitting field of $X^{12} - 1$ over $\mathbb{Q}$. Calculate $[K:\mathbb{Q}]$ and find an explicit $\mathbb{Q}$-basis for K. Prove that K is also the splitting field of $(X^4 - 1)(X^3 - 1)$ over $\mathbb{Q}$.

(6.16) Let $f = X^6 + 3$, $\alpha \in \mathbb{C}$, $f(\alpha) = 0$, $K = \mathbb{Q}(\alpha)$, $g = X^6 + 2$, $M \subset \mathbb{C}$ a splitting field of g over $\mathbb{Q}$, $L = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}) \subset \mathbb{C}$. Clearly, f and g are irreducible over $\mathbb{Q}$ by Eisenstein.

(a) Prove that K contains all 6-th roots of unity.

(b) Prove that K is a splitting field over $\mathbb{Q}$.

(c) Prove $L \subset M$.

(d) Prove $[L:\mathbb{Q}] = 4$.

(e) Prove $[M:\mathbb{Q}] = 12$.

(6.17) (a) Let $f = X^3 - 3X - 1$. Prove that f is irreducible in $\mathbb{Q}[x]$.

(b) Prove directly that if $\alpha \in \mathbb{C}$ is a root of f then so is $2 - \alpha^2$.

(c) Let $\alpha \in \mathbb{C}$ be a root of f and put $K = \mathbb{Q}(\alpha)$. Prove that $K/\mathbb{Q}$ is a Galois extension. [Hint: use theorem 100].

(d) Choose yourself a nontrivial element of $G = \mathrm{Gal}(K/\mathbb{Q})$ and write down its matrix with respect to the $\mathbb{Q}$-basis $(1, \alpha, \alpha^2)$ of K.

(6.18) Let $\varepsilon = \exp(2\pi i/7) \in \mathbb{C}$. You may use the fact that ε has degree 6 over $\mathbb{Q}$. We put

$$\alpha = \varepsilon + \varepsilon^6, \quad \beta = \varepsilon^2 + \varepsilon^5, \quad \gamma = \varepsilon^3 + \varepsilon^4.$$

(a) Prove $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\varepsilon)$ and $[\mathbb{Q}(\varepsilon) : \mathbb{Q}(\alpha)] \in \{1, 2\}$ and use the Tower Law to deduce that α is of degree 3 or 6 over $\mathbb{Q}$.

(b) Compute the polynomial $f = (X - \alpha)(X - \beta)(X - \gamma)$ explicitly and hence prove that it is in $\mathbb{Z}[X]$.

(c) Prove that α is of degree 3 over $\mathbb{Q}$.

(d) Find explicitly an $r \in \mathbb{Z}[X]$ such that $r(\alpha) = \beta$.

(e) Prove that $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$.

(6.19) In this exercise, you prove that $\mathbb{C}$ is algebraically closed (and more).

Let K be a field of characteristic 0 such that every polynomial in $K[X]$ of odd degree has a root in K. Let L/K be a finite Galois extension such that every polynomial in $L[X]$ of degree 2 has a root in L.

For a polynomial f, let $r(f)$ denote the greatest $n \geq 0$ such that 2^n divides the degree of f.

Let $f \in K[X]$ be monic. Let M be a splitting field for f over K. Write $f = \prod_{i=1}^{n}(X - a_i)$ with $a_i \in L$. For $c \in K$, define

$$g_c(X) = \prod_{1 \leq i < j \leq n} (X - a_i - a_j - c a_i a_j).$$

(a) Prove that if the degree of f is even then $r(g) < r(f)$.

(b) Prove that $g_c \in K[X]$.

(c) Prove that if f is not constant then it has a root in L. [Hint: induction on $r(f)$].

(d) Prove that L is algebraically closed.

(e) Deduce that $\mathbb{C}$ is algebraically closed.

(6.20) Let L/K be a finite field extension. Let $f \in K[x]$ be irreducible of degree p, a prime number. Suppose that f is reducible in $L[x]$. Prove that p divides $[L : K]$.

(6.21) Let K be a field and $f = X^4 + p\,X^2 + q \in K[X]$ a polynomial. Let $\alpha \in K$ be such that $X - \alpha \mid f$.

(a) Suppose that the characteristic of K is not 2. Prove that there exists $\beta \in K$ such that $(X - \alpha)(X - \beta) \mid f$.

(b) Suppose that the characteristic of K is 2. Prove again that there exists $\beta \in K$ such that $(X - \alpha)(X - \beta) \mid f$.

(6.22) For each of the following polynomials f, determine the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ where K is a splitting field of f over $\mathbb{Q}$, and all intermediate fields.

(a) $X^4 - 8X^2 + 8$.

(b) $X^4 - 8X^2 + 4$.

(c) $X^4 - 22\,X^2 + 25$.

(d) $X^6 + X^3 + 1$.

(6.23) In this exercise you generalise the results of this section to infinite families of polynomials, with an application to algebraic closures.

We say that L/K is a **splitting field** for an infinite set of polynomials $\{f_i \mid i \in I\} \subset K[X]$ if every f_i factors completely over L, and L is generated over K by the set of those $\alpha \in L$ for which $f_i(\alpha) = 0$ for some $i \in I$.

(a) Analogous to proposition 94, prove that a splitting field for $\{f_i \mid i \in I\}$ exists and is unique. (This involves a set theoretic difficulty; use Zorn's lemma. If you don't like set theory, simply assume that I is countable, say, $I = \mathbb{N}$. For uncountable I the Galois theoretic part of the proof is the same.)

(b) Let L/K be an algebraic extension. Analogous to theorem 100, prove that L/K is Galois if and only if L/K is a splitting field for a family of separable irreducible polynomials over K.

(c) We say that L is an **algebraic closure** of K if L/K is algebraic and L is algebraically closed. Prove that if L/K is a splitting field of all polynomials in $K[X]$, then L is algebraically closed. [Hint: use the result of exercise 5.5]. Deduce that every field has an algebraic closure and that it is unique (in what sense?).

(6.24) Let ε be a complex primitive 7th root of unity. Put $L = \mathbb{Q}(\varepsilon)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$.

(a) Say why we already know that $L/\mathbb{Q}$ is Galois of degree 6.

(b) Prove that there exists a unique element $s \in G$ such that $s(\varepsilon) = \varepsilon^3$.

(c) Prove that s has order 6.

(d) Prove that $G = \langle s \rangle$.

(e) Give a generator for the group $\mathbb{Q}(\alpha)^* \subset G$ where $\alpha = \varepsilon + \varepsilon^{-1}$. Deduce that the degree of α over $\mathbb{Q}$ is 3.

(f) Compute the minimum polynomial over $\mathbb{Q}$ of α.

(g) Give all subgroups of G and the corresponding fields, both by generators. (You should prove your results but you don't have to say how you found them). Hint: if H is a subgroup of G, use the algorithm of example 81 to find elements of $H^\dagger$.

(h) Prove that $X^2 + 7$ factors completely over L.

7 Finite fields

7.1 Finite subgroups of $K^\times$

Proposition 111. Let K be a field. Let $G \subset K^\times$ be a finite subgroup of the multiplicative group of K. Then G is cyclic.

In particular, if K is a finite field then $K^\times$ is a finite group and therefore cyclic by proposition 111.

We shall give two proofs of proposition 111. The first proof relies on a little theory of finite abelian groups and is as follows.

First proof of proposition 111. Suppose that G is not cyclic. The theory of finite abelian groups tells us that then G contains a subgroup H isomorphic to $C_p \times C_p$ with $p > 1$ and C_p a cyclic group of order p. Then all elements of H are roots of $X^p - 1$, so H has at most p elements, a contradiction. □

We now prepare for the second proof of proposition 111, not relying on any results about finite abelian groups. Let G be a finite group. The **order** of an element $a \in G$ is $\#\langle a \rangle$. The **exponent** $e(G)$ is the least common multiple of the orders of the elements of G. Equivalently, it is the least $d > 0$ such that $a^d = 1$ for all $a \in G$.

Lemma 112. Let G be a finite abelian group.

(a) Then G has an element of order $e(G)$.

(b) If $\#G = e(G)$ then G is cyclic.

Proof. Proof of (a). Write

$$e = e(G) = p_1^{k_1} \cdots p_k^{k_\ell}$$

where the p_i are distinct prime numbers. By the definition of exponent, there exists $a_i \in G$ whose order is divisible by $p_i^{k_i}$. On replacing a_i by a power if necessary, we may assume that the order of a_i is $p_i^{k_i}$. Put $b = a_1 \cdots a_k$. We claim that b has order e. We clearly have $b^e = 1$. Conversely, suppose that $b^m = 1$ for some $m \geq 1$. Let $1 \leq i \leq \ell$ and write $q = e \cdot p_i^{-k_i}$. Then

$$1 = b^{mq} = (a_1 \cdots a_\ell)^{mq} = \left(\prod_{j \neq i} a_j^{mq}\right) \cdot a_i^{mq} = a_i^{mq}$$

so the order of a_i is a divisor of mq, that is, $p_i^{k_i}$ divides m. As this is true for all i, we find $e \mid m$ thus proving that the order of b is e.

Proof of (b). Let $b \in G$ be an element of order $e(G)$, which exists by (a). Then G is generated by b. □

Second proof of proposition 111. Let e be the exponent of G. Then $a^e = 1$ for all $a \in G$ by Lagrange's theorem. Therefore every element of G is a root of $X^e - 1$. This polynomial has at most e roots and therefore $\#G \leq e$. By lemma 112b G is cyclic. □

7.2 Finite fields

If p is a prime number, we write $\mathbb{F}_p := \mathbb{Z}/(p)$. Warning: later we shall define $\mathbb{F}_q$ for more values of q, but in these cases it is not $\mathbb{Z}/(q)$.

Let K be a finite field. Then its characteristic is a prime number p because otherwise K would contain a copy of $\mathbb{Q}$. So the prime subfield of K is isomorphic to $\mathbb{F}_p$. Let us assume it *is* $\mathbb{F}_p$.

Write $[K : \mathbb{F}_p] = n$. Then K has precisely p^n elements because, as we learned in linear algebra, there exists an isomorphism of vector spaces over $\mathbb{F}_p$ between K and $(\mathbb{F}_p)^n$. The latter has p^n elements.

Example 113. Let $f \in \mathbb{F}_p[X]$ be monic and irreducible. By proposition 63 there exists a field extension $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ such that f is the minimum polynomial of α. Then $\mathbb{F}_p(\alpha)$ is a field of p^n elements where $n = \deg(f)$.

As an example of this, let us take $p = 2$ and $f = X^2 + X + 1$. By proposition 58, $\{1, \alpha\}$ is an $\mathbb{F}_2$-basis of $\mathbb{F}_2(\alpha)$. Thus $\mathbb{F}_2(\alpha)$ has four elements $0, 1, \alpha, 1 + \alpha$. The multiplication table is as follows.

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Proposition 114. Let $K \subset L$ be finite fields. Then there exists $\alpha \in L$ such that $L = K(\alpha)$.

Proof. By proposition 111 we know that the multiplicative group $L^\times$ of L is cyclic. Say it is generated by α. Then $L = K(\alpha)$. □

We shall prove that for every power q of a prime number there exists a field of q elements and, conversely, any two such fields are isomorphic. The main step is in the following.

Proposition 115. Let p be a prime number and $K/\mathbb{F}_p$ an extension. Let $n \geq 1$ and write $q = p^n$. Then $\#K = q$ if and only if $K/\mathbb{F}_p$ is a splitting field of the polynomial $g = X^q - X$.

Proof. Proof of $\Leftarrow$. Recall from exercise 2.6 the Frobenius endomorphism $F\colon K \to K$ defined by $F(a) = a^p$. Let $A = \{a \in K \mid F^n(a) = a\}$. Then A is a subfield of K because if $a, b \in A$ then $F^n(a + b) = F^n(a) + F^n(b) = a + b$ and likewise for multiplication of a, b or inverting a. Also, A contains the roots of g. Therefore, A contains the subfield of K generated by the roots of g. Since K is a splitting field of g, we find $K \subset A$. It follows that $K = A$, and that every element of K is a root of g. But g has no multiple roots in K by proposition 96 and the observation that $g' = -1$. Therefore $\#K = \deg g = q$.

Proof of $\Rightarrow$. Let $\#K = q$. Then the multiplicative group $K^\times$ has order $q - 1$. Therefore $u^{q-1} = 1$ for all $u \in K^\times$. Therefore $u^q = u$ for all $u \in K$. Every element of K is a root of g. But $\deg g = \#K$ so we must have $g =$

$\prod(X-a)$, the product being over the elements a of K. This shows that $K/\mathbb{F}_p$ is a splitting field of g as required. □

We know that splitting fields exist and are unique up to isomorphism. This proves the following.

Theorem 116. Let $q > 1$ be a power of a prime number. Then there exists a field of q elements. Any two such are isomorphic. □

A field of q elements is usually written $\mathbb{F}_q$. This is justified by the fact that such a field depends only on q up to isomorphism; but no particular field in its isomorphism class is meant specifically. If you would like a model for $\mathbb{F}_q$ ($q = p^n$ and p a prime number) to do calculations, you look for an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n (exercise: prove that such f exists). Then $\mathbb{F}_q \cong \mathbb{F}_p[X]/(f)$.

Next we consider what Galois theory says about a finite extension of a finite field.

Theorem 117. Let $K \subset L$ be finite fields. Then L/K is Galois and its Galois group is cyclic.

Proof. We may assume $\mathbb{F}_p \subset K \subset L$. Let $F\colon L \to L$ be Frobenius, $F(a) = a^p$. You proved in exercise 2.6 that F is an injective ring endomorphism. As L is finite, F is surjective as well. Therefore F is an element of the Galois group $G = \mathrm{Gal}(L/\mathbb{F}_p)$.

Write $p^n = \#L = q$ and $g = X^q - X$. By proposition 115, $L/\mathbb{F}_p$ is a splitting field of g. This proves that $F^n = 1$. No lower power of F is the identity because if $F^k = 1$, $k \geq 1$ then L is contained in the splitting field of $X^{p^k} - X$ and $k \geq n$.

In exercise 4.10 you proved that $[L : \mathbb{F}_p] \geq \#G$ and that equality implies that $L/\mathbb{F}_p$ is Galois. But we have just seen that $\#G \geq \#\langle F\rangle = [L : \mathbb{F}_p]$. This proves that $L/\mathbb{F}_p$ is Galois and that its Galois group is the cyclic group $\langle F\rangle$.

Now K is an intermediate field for $L/\mathbb{F}_p$ hence closed by the main theorem of Galois theory. Thus L/K is also Galois. Its Galois group is a subgroup of the cyclic group $\mathrm{Gal}(L/\mathbb{F}_p)$ and is therefore itself cyclic. □

Exercises

(7.1) Let $K \subset L$ be finite fields. Prove that L is separable over K.

(7.2) Let p be a prime number and $a, b \geq 1$. Prove that $\mathbb{F}_{p^a}$ can be embedded into $\mathbb{F}_{p^b}$ (that is, is isomorphic to a subfield of $\mathbb{F}_{p^b}$) if and only if $a \mid b$. [Hint: For $\Leftarrow$ use theorem 117. Before you find the intermediate field isomorphic to $\mathbb{F}_{p^a}$ you find the corresponding subgroup].

(7.3) Find a generator of the multiplicative group $\mathbb{F}_{31}^{\times}$.

(7.4) For each d in $\{3, 5, 7, 9\}$, find at least one irreducible $f \in \mathbb{F}_2[X]$ such that if α is a root of f in an extension of $\mathbb{F}_2$, then $\#\langle\alpha\rangle = d$, where $\langle\alpha\rangle$ is the multiplicative group generated by α.

(7.5) Let p be a prime number and $a \geq 1$. Prove that there exists an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree a. [Hint: The degree of an algebraic extension of the form $K(\alpha)/K$ equals the degree of the minimum polynomial of α over K].

(7.6) Let $\mathbb{F}_q$ be a finite field of q elements and let $a \geq 1$. Write $g = X^{q^a} - X$.

(a) Prove that there exists an irreducible polynomial in $\mathbb{F}_q[X]$ of degree a.

(b) Prove that g has no multiple roots in any field extension.

(c) Let $a \geq 1$. Prove that g is the product of all irreducible monic polynomials in $\mathbb{F}_q[X]$ whose degree divides a.

(d) Let $h_d(q)$ be the number of monic irreducible $f \in \mathbb{F}_q[X]$ of degree d. Prove

$$\sum_{d|a} d\, h_d(q) = q^a. \tag{118}$$

(e) Prove that there exists a polynomial $H_a \in \mathbb{Q}[Y]$ such that $h_a(r) = H_a(r)$ for all prime powers r.

(f) Let $f \in \mathbb{F}_q[X]$ be of degree d. Prove that f is irreducible if and only if f is coprime to $X^{q^a} - X$ whenever $a < d$. (This gives a fast algorithm to check irreducibility.)

(7.7) Let K be a field of characteristic $p > 0$. Let $f = X^p - X - a \in K[X]$.

(a) Prove $f(X) = f(X+1)$.

(b) Prove: f has no multiple roots in any field extension.

(c) Suppose f has no root in K. Then f is irreducible.

8 Radical extensions

Keywords: Normal closure, solvable group, commutator, radical extension, solvable extension.

8.1 Normal closures

Definition 119. Let $K \subset L \subset M$ be fields with L/K finite. We say that M is a **normal closure** of L/K if:

- The field M is a splitting field over K.
- No field other than M between L and M is a splitting field over K.

Proposition 120. Let L/K be a finite extension. Then there exists a normal closure M of L/K. If L/K is separable then M/K is Galois. Any two normal closures of L/K are L-isomorphic.

Proof. Let $v_1, \ldots, v_r$ be a K-basis of L. Let $f_i = \mathrm{mp}_K(v_i)$ and $f = f_1 \cdots f_r$.

Existence. Let M be a splitting field for f over L. Then M is also a splitting field for f over K (exercise). If L/K is separable then f_i is separable over K whence M/K is Galois by theorem 100. Any splitting field M' of L/K in between L and M must split each f_i for they each acquire a root in L. This shows that $M = M'$ and thus that M is a normal closure of L/K.

Uniqueness. Let M_i be a normal closure of L/K for all $i \in \{1, 2\}$. Then M_i is a splitting field over L of f. By uniqueness of splitting fields (proposition 94) M_1 and M_2 are L-isomorphic. □

8.2 Solvable groups

Definition 121. Let G be a group. We say that G is **solvable** if there are subgroups $G = A_0 \supset A_1 \supset \cdots \supset A_r = 1$ such that for all i, A_{i+1} is normal in A_i and A_i/A_{i+1} is abelian.

If G is solvable and finite, then by inserting more A_i we can arrange for A_i/A_{i+1} to be cyclic and such that its order is a prime number.

Proposition 122. Let G be a group and $H \subset G$ a subgroup.

(a) If G is solvable then so is H.

(b) If G is solvable and H is a normal subgroup of G then G/H is solvable.

(c) If H is normal in G and H and G/H are solvable then G is solvable.

(d) Every abelian group is solvable.

Proof. Proof of (a). Let $G = A_0 \supset A_1 \supset \cdots \supset A_r = 1$ be such that for all i, A_{i+1} is normal in A_i and A_i/A_{i+1} is abelian. Set $B_i = H \cap A_i$. Then $H = B_0 \supset B_1 \supset \cdots \supset B_r = 1$ and B_{i+1} is normal in B_i and B_i/B_{i+1} is a subgroup of an abelian group A_i/A_{i+1} and thereby abelian itself. This shows that H is solvable.

Part (b) is similar. Parts (c) and (d) are easy. □

For elements a, b of a group we write $[a, b] = aba^{-1}b^{-1}$. Such elements are called **commutators**.

Lemma 123. Every element of the alternating group A_5 is a commutator.

Proof. Every element of A_5 is of the form (ijk), $(ij)(k\ell)$ or $(ijk\ell m)$ where $i, j, k, \ell, m \in \{1, 2, 3, 4, 5\}$ are distinct. The following calculations finish the proof:

$$\begin{aligned}
[(ij\ell), (ikm)] &= (ij\ell)(ikm)(i\ell j)(imk) = (ijk),\\
[(ijk), (ij\ell)] &= (ijk)(ij\ell)(ikj)(i\ell j) = (ij)(k\ell),\\
[(ij)(km), (im\ell)] &= (ij)(km)(im\ell)(ij)km(i\ell m) = (ijk\ell m).
\end{aligned}$$ □

Proposition 124. The symmetric group S_5 and the alternating group A_5 are not solvable.

Proof. By proposition 122 it is enough to prove that A_5 is not solvable. Suppose that it is: $A_5 = B_0 \supset B_1 \supset \cdots \supset B_r = 1$ with B_{i+1} normal in B_i and B_i/B_{i+1} abelian. Let $f \colon B_0 \to B_0/B_1$ denote the natural homomorphism. As B_0/B_1 is abelian we have for all $a, b \in B_0$

$$1 = f(a)f(b)f(a)^{-1}f(b)^{-1} = f(aba^{-1}b^{-1}) = f([a, b])$$

so $[a, b] \in B_1$. But all elements of A_5 are commutators by lemma 123 so $B_1 = B_0$. Continuing this way we find $A_5 = B_i$ for all i, a contradiction. □

Lemma 125. Let p be a prime number. Let $H \subset S_p$ be a subgroup containing a p-cycle and at least one transposition (ij). Then $H = S_p$.

Proof. Exercise. □

8.3 Radical extensions

Definition 126. An extension L/K is a **radical extension** if L has the form $K(u_1, \ldots, u_m)$ where for all i there exists $\ell_i > 0$ such that

$$u_i^{\ell_i} \in K(u_1, \ldots, u_{i-1}).$$

It is clear that a radical extension is of finite degree. By inserting further u's if necessary we can arrange that the ℓ_i are prime numbers.

Definition 127. An extension L/K is a **solvable extension** if there exists a radical extension M/K with $L \subset M$.

The main result on solvable extensions is the following.

Theorem 128. Let L/K be a solvable extension of characteristic 0. Then $\mathrm{Gal}(L/K)$ is a solvable group.

Our proof of theorem 128 depends on three lemmas which don't assume the characteristic to be 0.

Lemma 129. Let $K \subset L \subset M$ be fields. Suppose that L/K is a radical extension and M is the normal closure of L/K. Then M/K is a radical extension.

Proof. This is easy using exercise 6.5. □

Lemma 130. Let p be a prime number and L a splitting field of $X^p - 1$ over K. Then $\mathrm{Gal}(L/K)$ is abelian.

Proof. If the characteristic is p then $X^p - 1 = (X-1)^p$ and $L = K$. Suppose now that the characteristic is not p. Let ε be a root of $X^p - 1$ different from 1. Then $X^p - 1$ has p distinct roots $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$. Therefore $L = K(\varepsilon)$. An automorphism of L/K is determined by what it does to ε. Say $s, t \in \mathrm{Gal}(L/K)$ take ε to ε^i, respectively, ε^j. Then st and ts both take ε to ε^{ij}. Thus $st = ts$ and $\mathrm{Gal}(L/K)$ is abelian. □

Lemma 131. Let K be a field in which $X^n - 1$ factors completely. Let $a \in K$ and let L be a splitting field for $X^n - 1$ over K. Then $\mathrm{Gal}(L/K)$ is abelian.

Proof. Let u be a root in L of $X^n - a$. Then $L = K(u)$ because the other roots of $X^n - a$ are of the form $u\alpha$ where α is a root of $X^n - 1$ and is hence in K. Thus, an element of $\mathrm{Gal}(L/K)$ is determined by what it does to u. Let $s, t \in \mathrm{Gal}(L/K)$ and write $s(u) = \alpha u$, $t(u) = \beta u$ where α, β are roots in K of $X^p - 1$. Then st and ts both take u to $\alpha \beta u$. Thus $\mathrm{Gal}(L/K)$ is abelian. □

Proof of theorem 128. Let M/K be a radical extension such that $L \subset M$.

If K_0 denotes the closure $K^{*\dagger}$ with respect to L/K nothing in the problem is changed if we replace K by K_0. Hence we may assume that $K = K_0$, that is, L is Galois over K.

If N denotes a normal closure of M/K then N is a radical extension of K by lemma 129. Thus, changing notation again, we may assume that M is Galois over K (by theorem 100 and because the characteristic is 0).

Since $\mathrm{Gal}(L/K)$ is a quotient of $\mathrm{Gal}(M/K)$ and quotients of solvable groups are solvable by proposition 122, we have only to show that $\mathrm{Gal}(M/K)$ is solvable. Thus we may henceforth forget about L.

As M/K is radical, we may suppose that $M = K(u_1, \dots, u_n)$ where for all i there exists a prime number p_i such that $u_i^{p_i} \in K(u_1, \dots, u_{i-1})$. We argue by induction on n. Write $p = p_1$, $u = u_1$; then $u^p \in K$. Let M_0 be a splitting field for $X^p - 1$ over M. Let M_1 be the subfield of M_0 generated by K and the roots of $X^p - 1$.

$$\begin{tikzcd}
 & M_0 \arrow[dl, dash] \arrow[dr, dash] & \\
M \arrow[dr, dash] & & M_1 \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

If we show that $\mathrm{Gal}(M_0/K)$ is solvable, it will follow that $\mathrm{Gal}(M/K)$ is, again because a quotient of a solvable group is solvable. Now M_1 is a Galois extension of K with an abelian Galois group by lemma 130. Hence it will sufice to show that $\mathrm{Gal}(M_0/M_1)$ is solvable, for a group is solvable if a normal subgroup and its quotient group are solvable (proposition 122c). Now $M_0 = M_1(u_1, \ldots, u_n)$ for M_0 is generated over K by the u's and the roots of $X^p - 1$ and the latter are already in M_1. Write $G = \mathrm{Gal}(M_0/M_1)$ and let $H = M_1(u)^* \subset G$ be the subgroup corresponding to $M_1(u)$. Since $X^p - 1$ factors completely in M_1, $M_1(u)$ is a splitting field for $X^p - u_1^p$ over M_1 and hence is Galois with abelian Galois group by lemma 131. Thus G/H is abelian. To prove that G is solvable it remains finally to show that H is solvable. This follows from our inductive assumption, for M_0 is a radical extension of M_1 generated by a chain $u_2, \ldots, u_n$ as before with $n-1$ elements. This completes the proof of theorem 128. □

Using theorem 128 we can easily construct an unsolvable field extension L/K. Let S_5 act on $L = \mathbb{Q}(X_1, \ldots, X_5)$ by permuting the variables and put $K = L^{S_5}$. Then $\mathrm{Gal}(L/K) \cong S_5$ hence is an unsolvable group; therefore L/K is an unsolvable extension.

We shall give a more satisfying example with $K = \mathbb{Q}$ with the help of the following lemma.

Lemma 132. Let p be a prime number and let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of degree p and with precisely two nonreal complex roots. Let $L/\mathbb{Q}$ be the complex splitting field of f. Then $\mathrm{Gal}(L/K) \cong S_p$.

Proof. Let $H = \mathrm{Gal}(L/K)$. Then H acts faithfully on the set of complex roots of f. Thus $H \subset S_p$. Also $[L : K]$ is divisible by p because if $\alpha \in L$ is a root of f then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$. But $\#H = [L : K]$ so H contains a p-cycle. Complex conjugation restricts to an element of $\mathrm{Gal}(L/K) = H \subset S_p$ which is a transposition. Lemma 125 now implies that $H = S_p$. □

We claim that $f = x^5 - 6x + 3$ is not solvable. It is irreducible over $\mathbb{Q}$ by Eisenstein's criterion and a crude inspection of its graph reveals that it has exactly two nonreal roots. Hence its splitting field over $\mathbb{Q}$ has Galois group S_5 by lemma 132. Therefore f is not solvable by theorem 128.

9 Index

In figure 3 you can find a list of differences in notation and terminology between Irvin Kaplansky's *Fields and rings*, our notes and those of Miles Reid which were used in recent years.

Figure 3. Comparison of terminology.

Kaplansky	We	Reid
finite normal extension	finite Galois extension	Galois extension
split closure	normal closure	normal closure
none	none	normal extension
set of closed intermediate fields	$\mathcal{F}$ = set of closed intermediate fields	none
set of closed subgroups	$\mathcal{G}$ = set of closed subgroups	none
set of intermediate fields	set of intermediate fields	$\mathcal{F}$
set of subgroups	set of subgroups	$\mathcal{G}$
stable intermediate field	stable intermediate field	none