Galois theory

Oliver Lorscheid

Lecture notes, IMPA,
August–November 2018

Contents

Preface

These notes are the offspring of an attempt to organize my handwritten notes for the course on Galois theory, as given in the first half of Algebra 2 at IMPA. There are numerous excellent books and lecture notes available on the topic, and these notes do not cover other material than what appears in most of these sources.

The only particularity of this course is that it is taught in the limited time of around two months (it takes me 16 lectures of 90 minutes each), followed by an immediate mid-term exam. Therefore these notes present a fast approach towards the central topics of Galois theory, which are the solution of the classical problems about constructibility and the impossibility to solve the general quintic equation, while leaving some other important topics to the end of the lecture.

I have included all the exercises that I use for the weekly homework at the end of the corresponding chapters. At the very end, there is a list of further exercises that I hand out for the exam preparation.

Acknowledgements: I thank Eduardo Santos Silva and Marcel de Sena Dallagnol for their feedback on previous versions of this text.

Chapter 1

Motivation

1.1 Constructions with ruler and compass

The mathematics of ancient Greece included the knowledge of the (positive) natural numbers, ratios of positive natural numbers, square roots, and certain other numbers. The main approach to numbers was in terms of distances that arise from constructions with ruler and compass, and some famous and long standing problems concern the constructability of certain quantities.

Question: which numbers are constructible with ruler and compass?

Constructibility with ruler and compass are defined by the following rules: given (constructed) points $0, 1, P_1, \dots, P_n$ in the plane $\mathbb{R}^2$, we call a point Q **constructible from** $P_1, \dots, P_n$ if it can be derived using the following operations:

(1) draw a line through two constructed points;

(2) draw a circle around a constructed point whose radius equals the distance between two contructed points;

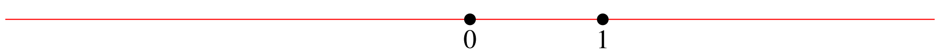
(3) call the intersection points of lines and circles **contructed points**.

A (positive real) number is **constructible** if it occurs as a distance between two points in the plane that are constuctible from 0 and 1.

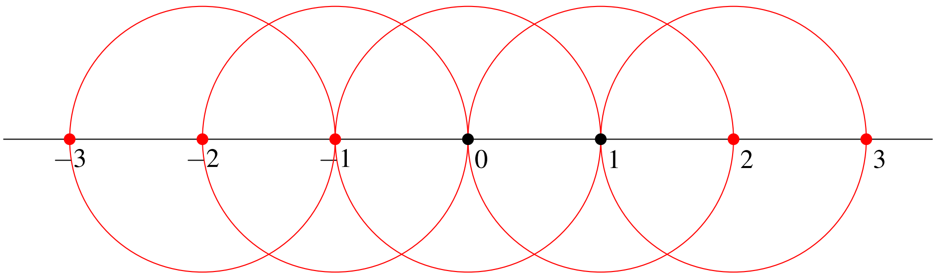
In the following, we will explain certain constructions with ruler and compass.

Coordinates: given 0 and 1

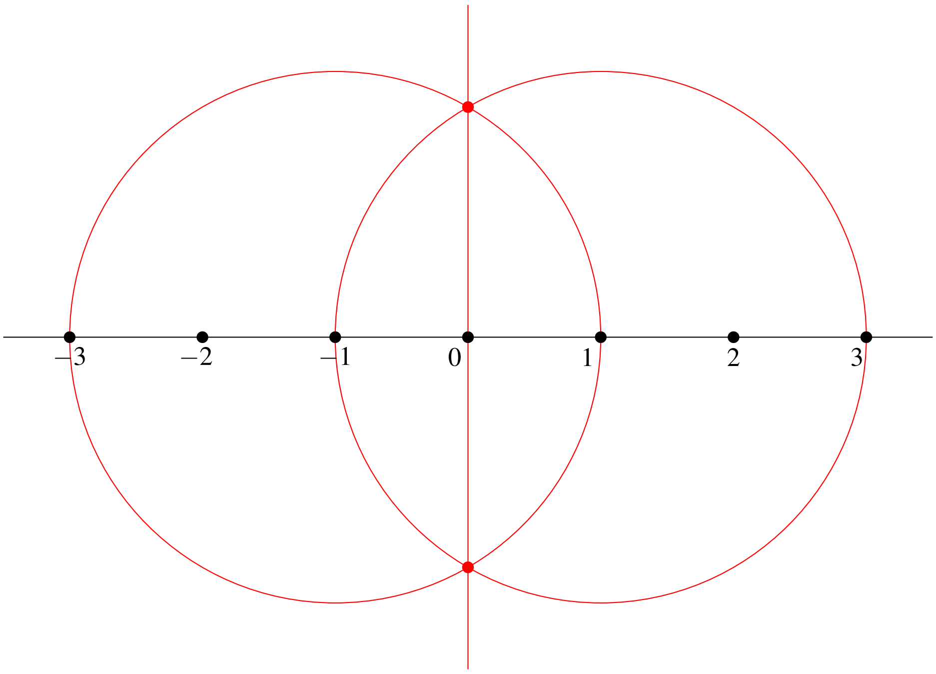
step 1: draw a line



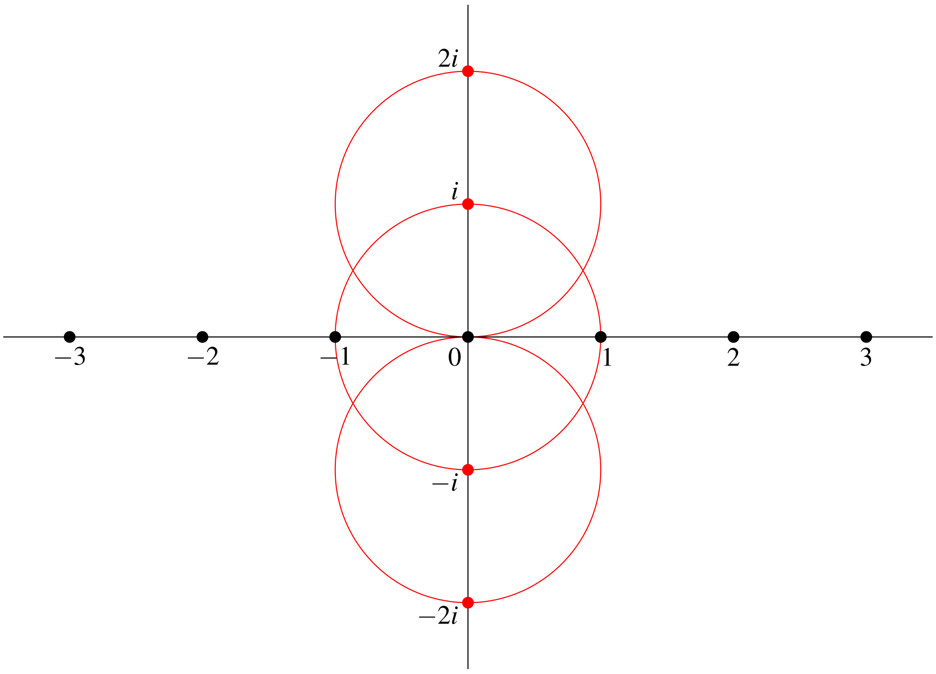
step 2: draw circles of radius 1



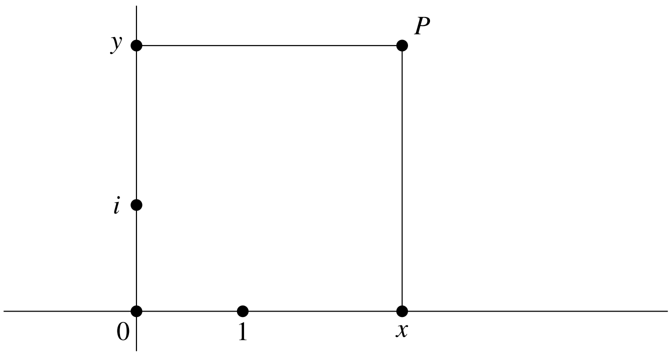
step 3: draw two circles with radius 2 around 1 and -1; connect the intersection points:



step 4: more circles with radius 1:

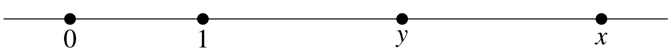


Observation: In particular, this shows how to construct orthogonal lines. It follows that it is equivalent to know a point P in $\mathbb{R}^2$ and its coordinates x and y:



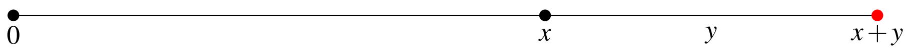
Thus it is equivalent to talk about constructible points P in the plane and constructible (positive) real numbers $x, y \in \mathbb{R}_{\geqslant 0}$. The constructions of x and y from P, and vice versa, are left as an exercise.

Arithmetic operations: given

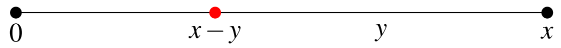


we can construct the following quantities.

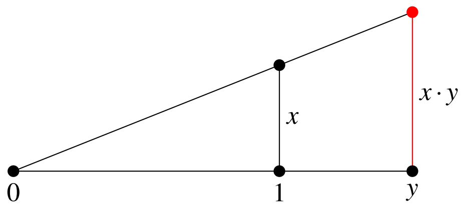
$\underline{x+y}$:



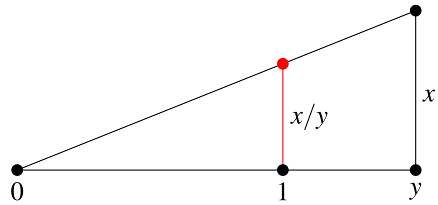
$x - y$:



$x \cdot y$:

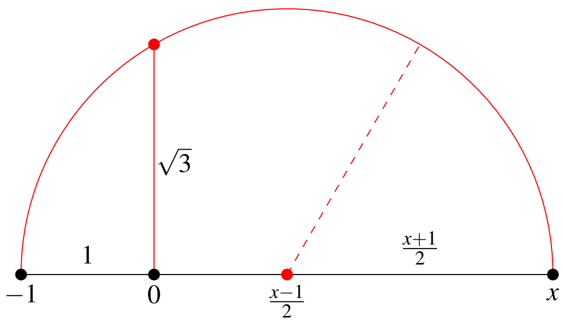


x/y:

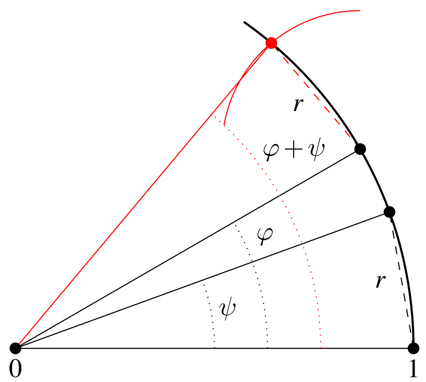


Conclusion: the length of constructible numbers and their additive inverses form a subfield of $\mathbb{R}$. But there are more arithmetic operations that can be performed by constructions.

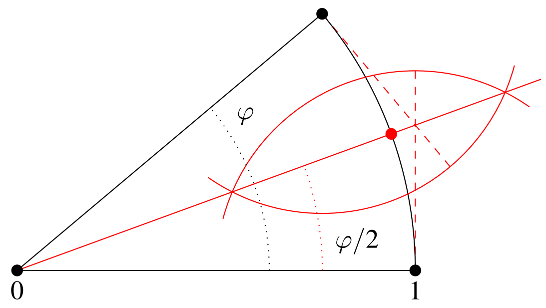
$\sqrt{x}$:



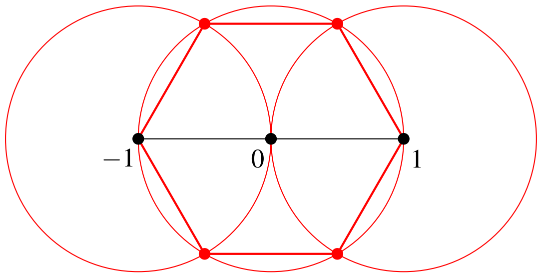
$\varphi + \psi$:



$\underline{\varphi/2:}$



Euclid constructs regular n-gons for all $n \geqslant 3$ of the form $2^r \cdot 3^i \cdot 5^j$ with $r \geqslant 0$ and $i, j \in \{0, 1\}$. For example, the regular hexagon can be constructed as follows:



Problems of the antique:

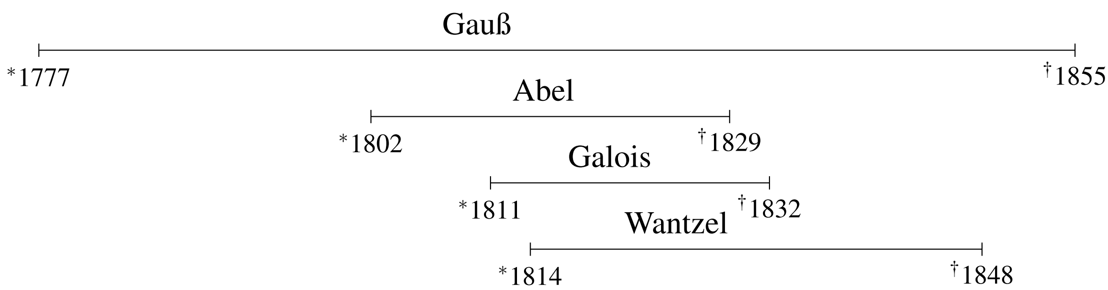
(1) *Double the cube:* given a cube with volume V and side length $a \in \mathbb{R}_{>0}$, can we construct a cube with volume $2V$, i.e. its side length $b = \sqrt[3]{2} \cdot a$?

(2) *Trisect an angle:* given an angle φ (i.e. a point on the unit circle), can we construct the angle $\varphi/3$?

(3) *Square the circle:* given a circle with area A (and radius r), can we construct a square with area A, i.e. its side length $a = \sqrt{\pi} r$?

(4) For which $n \geqslant 3$ is it possible to construct a regular n-gon?

Some answers:



Gauß 1796: Construction of the regular 17-gon.

Wantzel 1837:

- Construction of the regular 257-gon and 65537-gon;
- $\sqrt[3]{2}$ is not contructible;
- trisecting an angle is in general not possible.

Lindemann 1882: π is "transcendental" $\Rightarrow$ not constructible $\Rightarrow$ squaring the circle is impossible.

1.2 Equations of low degrees

Degree 2: The equation $aX^2 + bX + c = 0$ has two solutions

$$X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Degree 3: Ferro and Tartaglia had formulas to solve cubic equations, but kept them secret. Such a formula was first published by Cardano in his Ars Magna in 1545. Gieven a cubic equation

$$aX^3 + bX^2 + cX + d = 0,$$

we can replace X by $Y = X - b/3a$ and obtain

$$Y^3 + pY + q = 0$$

for some p and q. Suppose that $\Delta = q^2/4 + p^3/27 > 0$. Then there exists a real solution

$$Y = \sqrt[3]{-q/2 + \sqrt{\Delta}} + \sqrt[3]{-q/2 - \sqrt{\Delta}}.$$

Degree 4: A formula for solving quartic equations was found by Cardano's student Ferrari, and it was also published in Ars Magna.

Degree 5: Much effort was done to find a Formula for solving quintic equations. Ruffini (1799) gave a first, but incomplete proof of that this was not possible. The first complete proof was given by Abel (1824). Wantzel (1845) clarified this proof, using Galois theory.

1.3 What is Galois theory?

Galois theory is a method to study the roots of polynomials $f = T^n + c_{n-1}T^{n-1} + \cdots + c_0$ with coefficients in a field K.

Fact: There is a smallest field L containing K and all roots of f. This field and the roots of f can be studied with Galois theory. Let

$$\mathrm{Aut}_K(L) = \left\{ \sigma : L \to L \;\middle|\; \begin{array}{c} \sigma \text{ bijective, } \sigma(a) = a \text{ for all } a \in K, \\ \sigma(a+b) = \sigma(a) + \sigma(b),\ \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) \end{array} \right\}$$

and $[L : K] = \dim_K L$.

Definition. Let $[L:k]$ be finite. The field L is **Galois** over K if $\#\mathrm{Aut}_K(L) = [L:K]$. In this case, $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ is called the **Galois group of** L **over** K.

Theorem 1.3.1 (Galois, 1833). *Let L be Galois over K and $G = \mathrm{Aut}_K(L)$. Then the maps*

$$\begin{array}{ccc} \{\, \textit{intermediate fields } K \subset E \subset L \,\} & \stackrel{1:1}{\longleftrightarrow} & \{\, \textit{subgroups } H < G \,\} \\ E & \longmapsto & \mathrm{Aut}_E(L) \\ L^H = \{\, a \in L \,|\, \sigma(a) = a \textit{ for all } \sigma \in H \,\} & \longleftarrow & H \end{array}$$

are mutually inverse bijections. Moreover, E is Galois over K if and only if $\mathrm{Aut}_E(L)$ *is a normal subgroup of G.*

With this theory, we are able to understand the answers from the previous sections.

1.4 Exercises

Exercise 1.1. Let P be a point in $\mathbb{R}^2$ with coordinates x and y. Show that P is constructible from a given set of points $0, 1, P_1, \ldots, P_n$ if and only if x and y are constructible (considered as points $(x,0)$ and $(y,0)$ of the first coordinate axis in $\mathbb{R}^2$). Conclude that the point $P_1 + P_2$ (using vector addition) is constructible from $0, 1, P_1, P_2$.

Exercise 1.2. Let r be a positive real number. Show that $h = \sqrt{r}$ is constructible from 0, 1 and r.

Hint: Use classical geometric theorems like the theorem of Thales or the theorem of Pythagoras.

Exercise 1.3. Construct the following regular n-gons with ruler and compass:

(1) a regular 2^r-gon for $r \geqslant 2$;

(2) a regular 3-gon;

(3) a regular 5-gon.

Exercise 1.4. Prove Cardano's formula: given an equation $x^3 + px + q = 0$ with real coefficients p and q such that $\Delta = q^2/4 + p^3/27 > 0$, then

$$x \quad = \quad \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}$$

is a solution.

Exercise 1.5. Find all solutions for $x^4 - 2x^3 - 2x - 1 = 0$.

Hint: Use Ferrari's formula.

Exercise 1.6 (very difficult)**.** Find solutions to the following classical problems:

(1) Given a positive real number r, is it possible to construct the cube root $\sqrt[3]{r}$?

(2) Given an angle φ, is it possible to construct $\varphi/3$?

(3) Given a circle with area A, is it possible to construct a square with area A?

Chapter 2

Algebraic field extensions

2.1 Algebraic extensions

Definition. (1) A **field extension** is an inclusion $K \hookrightarrow L$ of a field K as a subfield of a field L. We write L/K.

(2) The **degree of** L/K is the dimension

$$[L : K] = \dim_K L$$

of L as a K-vector space.

(3) An element $a \in L$ is **algebraic over** K if it satisfies a nontrivial equation of the form

$$c_n a^n + \cdots + c_1 a + c_0 = 0$$

with $c_0, \dots, c_n \in K$. Otherwise a is called **transcendental over** K.

(4) L/K is **algebraic** if every $a \in L$ is algebraic over K.

Example. (1) K/K is algebraic.

(2) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is algebraic.

(3) $\mathbb{C}/\mathbb{R}$ is algebraic.

(4) $\mathbb{R}/\mathbb{Q}$ is not algebraic.

Definition. Let L/K be a field extension. The unique K-linear ring homomorphism

$$\begin{array}{rccc} \mathrm{ev}_a : & K[T] & \longrightarrow & L \\ & f & \longmapsto & \mathrm{ev}_a(f) = f(a) \end{array}$$

that sends T to $a \in L$ is called the **evaluation map at** a. Since $K[T]$ is a principal ideal domain, $\ker(\mathrm{ev}_a) = (f)$ for some $f \in K[T]$. We call this f the **minimal polynomial of** a if it is **monic**, i.e. if its leading coefficient is 1, and we write $f = \mathrm{Mipo}_a$.

Remark. (1) f is uniquely determined up to a multiple by some $b \in K^\times$. Thus Mipo_a is unique.

(2) Since $K[T]/(f) \subset L$ is an integral domain, (f) is a prime ideal. Thus $f = 0$ or f is prime and thus irreducible ($K[T]$ is a UFD).

(3) The map

$$\begin{array}{rccc} M_a: & L & \longrightarrow & L \\ & b & \longmapsto & ab \end{array}$$

is K-linear. If $[L:K] < \infty$, then the minimal polynomial of M_a equals Mipo_a. (This is an exercise on List 2).

(4) A K-linear ring homomorphism $F: R_1 \to R_2$ between two rings that contain K fixes K, i.e. $f(a) = a$ for every $a \in K$.

Lemma 2.1.1. *Let L/K be a field extension and $a \in L$. Then a is algebraic over K if and only if* $\ker(\text{ev}_a) \neq 0$.

Proof. Assume that $\ker(\text{ev}_a) = (f) \neq 0$, i.e. $f = \sum c_i T^i \neq 0$. Then

$$0 \;=\; \text{ev}_a(f) \;=\; \sum c_i \text{ev}_a(T)^i \;=\; \sum c_i a^i,$$

i.e. a is algebraic over K.

If $\ker(\text{ev}_a) = 0$, then $\text{ev}_a: K[T] \to L$ is injective. This means that $\{1, a, \ldots, a^n, \ldots\} \subset L$ is linearly independent over K. Therefore a does not satisfy any algebraic relation over K, i.e. a is transcendental over K. $\square$

Lemma 2.1.2. *If L/K is of finite degree $n = [L:K]$, then L/K is algebraic.*

Proof. Let $a \in L$. Then $\{1, a, \ldots, a^n\}$ is linearly dependent over K, i.e.

$$c_0 \;+\; c_a a \;+\; \cdots \;+\; c_n a^n \;=\; 0$$

for some nontrivial $c_i \in K$. $\square$

Lemma 2.1.3. *Given finite extensions L/E and E/K. Then $[L:K] = [L:E] \cdot [E:K]$.*

Proof. Choose bases $(x_1, \ldots, x_n)$ of E/K and $(y_1, \ldots, y_m)$ of L/E where $n = [E:K]$ and $m = [L:E]$. Then for $a \in L$, there exist unique $\mu_1, \ldots, \mu_m \in E$ such that

$$a \;=\; \mu_1 y_1 + \cdots + \mu_m y_m$$

and unique $b_{i,j} \in K$ ($i = 1, \ldots, m$, $j = 1, \ldots, n$) s.t.

$$\mu_i \;=\; b_{i,1} x_1 + \cdots + b_{i,n} x_n.$$

Thus

$$a \;=\; \sum_{i,j} b_{i,j} x_j y_i.$$

By the uniqueness of the $b_{i,j}$, $(x_j y_i)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}}$ is a basis for L/K and thus $[L:K] = n \cdot m$. $\square$

Definition. Let L/K be a field extension and $a_1, \ldots, a_n \in L$.

(1) $K[a_1, \dots, a_n]$ is the smallest *subring* of L that contains K and $a_1, \dots, a_n$. It is called the **K-algebra generated by** $a_1, \dots, a_n$.

(2) $K(a_1, \dots, a_n)$ is the smallest *subfield* of L that contains K and $a_1, \dots, a_n$. It is called the **field extension of K generated by** $a_1, \dots, a_n$.

Remark. There is a unique smallest such subring / subfield. We have

$$K[a_1, \dots, a_n] \;=\; \bigcap_{\substack{K \subset E \subset L \\ E \text{ ring, } a_1, \dots, a_n \in E}} E \;=\; \left\{ b \in L \;\middle|\; b = f(a_1, \dots, a_n) \; \begin{array}{c} \text{for some } f \text{ in} \\ K[T_1, \dots, T_n] \end{array} \right\}$$

and

$$K(a_1, \dots, a_n) \;=\; \bigcap_{\substack{K \subset E \subset L \\ E \text{ field, } a_1, \dots, a_n \in E}} E \;=\; \left\{ b \in L \;\middle|\; b = \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} \; \begin{array}{c} \text{for some } f, g \\ \text{in } K[T_1, \dots, T_n] \\ \text{with } g \neq 0 \end{array} \right\}.$$

Theorem 2.1.4. *Let L/K be a field extension and $a \in L$. The following are equivalent:*

(1) a is algebraic over K.

(2) $[K(a) : K]$ is finite.

(3) $K(a)/K$ is algebraic.

(4) $K[a] = K(a)$.

Proof. The theorem is clear for $a = 0$. Assume $a \neq 0$.
(1)⇒(4): If a is algebraic over K , then $(f) = \ker(\mathrm{ev}_a)$ is a maximal ideal. Thus

$$K[a] \;=\; \mathrm{im}(\mathrm{ev}_a) \;\simeq\; K[T]/(f)$$

is a field containing K and a. Therefore $K[a] = K(a)$.
(4)⇒(2): $K[a] = K(a)$ implies that $\mathrm{ev}_a : K[T] \to K(a)$ is surjective. Thus $1, a, \dots, a^{n-1}$ form a finite basis of $K(a) = K[a]$ over K where $n = \deg f = [K(a) : K]$.
(2)⇒(3): This is Lemma 2.1.2.
(3)⇒(4): If $K(a)/K$ is algebraic, then there is an $f = \sum c_i T^i \in K[T]$ for every $b \in K[a] - \{0\}$ such that

$$f(b^{-1}) \;=\; c_n b^{-n} + \dots + c_1 b^{-1} + c_0 \;=\; 0.$$

After multiplying with b^{n-1}/c_n, this yields that

$$b^{-1} \;=\; -c_n^{-1}(c_{n-1} + c_{n-2} b + \dots + c_0 b^{n-1}) \;\in\; K[a].$$

Thus $K[a]$ is a field, i.e. $K[a] = K(a)$.
(4)⇒(1): If $K[a] = K(a)$, then $a^{-1} = \sum_{i=1}^{n} c_i a^{i-1}$ for some $c_i \in K$. Thus $\sum_{i=1}^{n} c_i a^i - 1 = 0$, i.e. a is algebraic over K. □

Corollary 2.1.5. *If a is algebraic over K, then $[K(a) : K] = \deg(\mathrm{Mipo}_a)$.* □

Corollary 2.1.6. *If L/E and E/K are algebraic, then L/K is algebraic.*

Proof. Every $a \in L$ has a minimal polynomial $f = \sum c_i T^i$ with $c_i \in E$ and c_i algebraic over K for $i = 0, \dots, n$. Thus

$$K \subset K(c_0) \subset K(c_0, c_1) \subset \cdots \subset K(c_0, \dots, c_n) \subset K(c_0, \dots, c_n, a)$$

is a series of finite field extensions by Thm. 2.1.4. By Lemma 2.1.3,

$$[K(c_0, \dots, c_n, a) : K] = [K(c_0, \dots, c_n, a) : K(c_0, \dots, c_n)] \cdots [K(c_0) : K],$$

which is finite. Thus $K(a)/K$ is finite and a is algebraic over K by Thm. 2.1.4. $\square$

Remark. Note that there are infinite algebraic field extensions; for example, the extension $L/\mathbb{Q}$ with $L = \mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{2}, \dots, \sqrt[n]{2}, \dots)$ is algebraic but not finite.

2.2 Algebraic closure

Definition. Let L/K be a field extension, $f = \sum c_i T^i \in K[T]$ and $a \in L$. Then a is called a **root of** f if $f(a) = \mathrm{ev}_a(f) = 0$.

Lemma 2.2.1. *Let $f \in K[T]$ be irreducible, $L = K[T]/(f)$ and $a = [T] \in L$. Then a is a root of f.*

Proof. The evaluation map $\mathrm{ev}_a : K[T] \to L$ sends f to 0 by the definition of $a = [T]$ and $L = K[T]/(f)$. $\square$

Corollary 2.2.2. *Every f of degree $\geqslant 1$ has a root in some finite field extension.*

Proof. Since $\deg f \geqslant 1$, f has an irreducible factor g. By Lemma 2.2.1, g has a root $a = [T]$ in $L = K[T]/(f)$. Since $f = gh$ for some $h \in K[T]$,

$$f(a) = \mathrm{ev}_a(f) = \mathrm{ev}_a(g) \cdot \mathrm{ev}_a(h) = 0. \qquad \square$$

Definition. A field K is **algebraically closed** if every polynomial $f \in K[T]$ of degree $\geqslant 1$ has a root in K.

Lemma 2.2.3. *Let K be an algebraically closed field and $f \in K[T]$ of degree n. Then $f = u \prod_{i=1}^{n} (T - a_i)$ for some $u, a_1, \dots, a_n \in K$.*

Proof. Induction on $n = \deg f$.

<u>n=0:</u> $f = u$ for some $u \in K$.

<u>n>0:</u> Since K is algebraically closed, f has a root $a \in K$, i.e. $f \in \ker(\mathrm{ev}_a)$. But also $\mathrm{ev}_a(T - a) = 0$. Since $T - a$ is irreducible, $\ker(\mathrm{ev}_a) = (T - a)$. Thus $f = (T - a)g$ for some $g \in K[T]$, and g must have degree $n - 1$. The claim follows from the inductive hypothesis. $\square$

Corollary 2.2.4. *Let K be an algebraically closed field and L/K algebraic. Then $L = K$.*

Proof. Let $a \in L$. Since L/K is algebraic, a has a minimal polynomial $f \in K[T]$. By Lemma 2.2.3, $f = u\prod(T - a_i)$ for some $u, a_i \in K$. Since f is irreducible, $f = u(T - a_1)$ and $a = a_1 \in K$. □

Corollary 2.2.5. *A field K is algebraically closed if and only if every irreducible polynomial $f \in K[T]$ has degree 1.*

Proof. "$\Rightarrow$": If K is algebraically closed, then $f = u\prod(T - a_i)$ for some $u, a_i \in K$. Thus f irreducible if and only if $\deg f = 1$.
"$\Leftarrow$": Consider $f \in K[T]$ of positive degree and let $f = \prod g_i$ be a factorization into irreducible polynomials g_i. Then $\deg g_i = 1$, i.e. $g_i = u_i(T - a_i)$ for some $u_i, a_i \in K$. Thus a_i is a root of g_i and consequently of f. □

Theorem 2.2.6. *Every field K is contained in an algebraically closed field L.*

Proof. Set $L_0 = K$. We define a series of field extensions L_i of K ($i \geqslant 0$).

Given L_i, we construct L_{i+1} as follows. Define a set of symbols

$$S_i = \{X_f \,|\, f \in L_i[T] \text{ of degree } \geqslant 1\}.$$

Then for $g = \sum c_i T^i \in L_i[T]$,

$$g(X_g) = \sum c_i X_g^i \qquad \in L_i[S_i] = L_i[X_g | g \in L_i[T] \text{ of degree } \geqslant 1].$$

Claim 1: $I = (g(X_g) | \deg g \geqslant 1)$ is a proper ideal of $L_i[S_i]$.

Assume that $I = L_i[S_i]$. Then

$$1 = h_1 g_1(X_{g_1}) + \cdots + h_n g_n(X_{g_n})$$

for some $g_1, \dots, g_n \in L_i[T]$ of degree $\geqslant 1$ and some $h_1, \dots, h_n \in L_i[S_i]$. By Corollary 2.2.2, there is a finite field extension E/L_i such that every g_j has a root a_j in E. Define the L-linear ring homomorphism

$$\begin{array}{rrcll} \chi & L_i[S_i] & \longrightarrow & & E. \\ & X_{g_j} & \longmapsto & & a_j \\ & X_f & \longmapsto & 0 & \text{for } f \notin \{g_1, \dots, g_n\} \end{array}$$

Then

$$1 = \chi(1) = \sum \chi(h) \underbrace{\chi(g_j(X_{g_j}))}_{=g_j(a_j)=0} = 0,$$

which is a contradiction. Thus Claim 1. ♦

Let $\mathfrak{m}$ be a maximal ideal of $L_i[S_i]$ that contains $\mathfrak{m}$. We define $L_{i+1} = L_i[S_i]/\mathfrak{m}$. Note that the map

$$L_i \longrightarrow L_i[S_i] \longrightarrow L_i[S_i]/\mathfrak{m} = L_{i+1}$$

is a field extension, and that every polynomial $g \in L_i[T]$ of positive degree has the root $[X_g]$ in L_{i+1} since $g(X_g) \in I \subset \mathfrak{m}$.

Claim 2: $L = \bigcup_{i \geqslant 0} L_i$ is an algebraically closed field.

It is clear that L is a field since for all $x, y \in L$, there exists an i such that $x, y \in L_i$. Thus also $x+y, x-y, xy, x/y \in L_i \subset L$ (provided $y \neq 0$).

Let $f = \sum c_i T^i \in L[T]$ be of positive degree. Then $c_0, \ldots, c_n \in L_i[T]$ for some i. Thus f has a root $a \in L_{i+1} \subset L$. Thus Claim 2. ♦ □

Lemma 2.2.7. *Let E/K be an algebraic field extension. Every field homomorphism $\sigma : K \to L$ into an algebraically closed field L extends to a field homomorphism $\sigma_E : E \to L$:*

$$\begin{tikzcd} E \arrow[r, dashed, "\sigma_E"] \arrow[d, dash] & L \\ K \arrow[ur, "\sigma"'] & \end{tikzcd}$$

Proof. Consider the set $\mathcal{S}$ of pairs $(F/K, \sigma_F)$ where $K \subset F \subset E$ is an intermediate field and $\sigma_F : F \to L$ extends σ. We define a partial order on $\mathcal{S}$:

$$(F/K, \sigma_F) \leqslant (F'/K, \sigma_{F'}) \quad \text{if} \quad F \subset F' \text{ and } \sigma_{F'}|_F = \sigma_F.$$

Then every chain

$$(F_1/K, \sigma_1) \leqslant (F_2/K, \sigma_2) \leqslant \cdots \leqslant (F_i/K, \sigma_i) \leqslant \cdots$$

has the upper bound $(F/K, \sigma_F)$ where $F = \bigcup F_i$ and $\sigma_F : F \to L$ is defined by $\sigma_F|_{F_i} = \sigma_i$. By Zorn's lemma, $\mathcal{S}$ has a maximal element $(F/K, \sigma_F)$.

Thus we have

$$\begin{tikzcd} E \arrow[r, dashed, "?"] \arrow[d, dash] & L \\ F \arrow[ur, "\sigma_F"] \arrow[d, dash] & \\ K \arrow[uur, "\sigma"'] & \end{tikzcd}$$

Claim: $F = E$.

If $F \neq E$, then there is an $a \in E - F$, which is algebraic over F. Let f be the minimal polynomial of a, i.e. $(f) = \ker(\mathrm{ev}_a)$. Then there exists a root b of $\sigma(f)$ in L, i.e. f is in the kernel of $\mathrm{ev}_b : K[T] \to L$. Thus $(f) \subset \ker(\mathrm{ev}_b)$ and we get

$$\begin{tikzcd} F(a) \arrow[r, dashed, "\sigma_{F(a)}"] & L, \\ F[T] \arrow[u, "\mathrm{ev}_a"] \arrow[ur, "\mathrm{ev}_b"] & \\ F \arrow[u] \arrow[uur, "\sigma_F"'] & \end{tikzcd}$$

which is an extension of σ_F to $\sigma_{F(a)} : F(a) \to L$, which contradicts the maximality of $(F/K, \sigma_F)$. □

Definition. An **algebraic closure of a field** K is an algebraic field extension L/K where L is algebraically closed. We often denote an algebraic closure of K by $\overline{K}$.

Theorem 2.2.8. *Every field K has an algebraic closure $\overline{K}/K$, and any two algebraic closures of K are isomorphic.*

Proof. Existence: By Theorem 2.2.6, there exists a field extension L/K with L algebraically closed. Define

$$\overline{K} = \bigcup_{\substack{K \subset E \subset L \\ E/K \text{ algebraic}}} E,$$

which is an algebraic extension of K. If $f \in \overline{K}[T] \subset L[T]$ is of positive degree, then f has a root $a \in L$. Thus a is algebraic over $\overline{K}$ and by Corollary 2.1.6, a is algebraic over K. Thus $a \in \overline{K}$, which shows that $\overline{K}$ is algebraically closed.

Uniqueness: Let L/K be another algebraic closure of K. By Lemma 2.2.7, there exists a field homomorphism $\sigma : L \to \overline{K}$ that extends the inclusion $K \to \overline{K}$. Thus σ identifies L with an algebraically closed subfield $\sigma(L)$ of $\overline{K}$. By Corollary 2.2.4, $\overline{K}/\sigma(L)$ is trivial, i.e. $\sigma : L \to \overline{K}$ is an isomorphism of fields. □

2.3 Exercises

Exercise 2.1. Let L/K be a field extension and $a \in L$ algebraic over K. Let $f(T) \in K[T]$ be the minimal polynomial of a over K. Show that the minimal polynomial of the K-linear map

$$\begin{array}{rccc} M_a : & L & \longrightarrow & L \\ & b & \longmapsto & a \cdot b \end{array}$$

is equal to f.

Exercise 2.2. Let L/K be a finite field extension. Then there are elements $a_1, \ldots, a_n \in L$ such that $L = K(a_1, \ldots, a_n)$.

Exercise 2.3. Let L/K be a field extension and $a_1, \ldots, a_n \in L$. Show that $K(a_1, \ldots, a_n)/K$ is algebraic if and only if $a_1, \ldots, a_n$ are algebraic over K.

Exercise 2.4. Consider the following elements $\sqrt[3]{2}$ and ζ_3 as elements of an algebraic closure of $\mathbb{Q}$.

(1) Show that $\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$ and find its minimal polynomial. What is the degree $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$?

(2) Let $\zeta_3 = e^{2\pi i/3}$ be a **primitive third root of unity**, i.e. an element $\neq 1$ that satisfies $\zeta_3^3 = 1$. Show that ζ_3 is algebraic over $\mathbb{Q}$ and find its minimal polynomial. What is the degree $[\mathbb{Q}(\zeta_3) : \mathbb{Q}]$?

(3) What is the degree of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ over $\mathbb{Q}$?

Exercise 2.5. Show that every field K contains a unique smallest subfield K_0. Show that if $\operatorname{char} K = 0$, then K_0 is isomorphic to $\mathbb{Q}$, and if $\operatorname{char} K = p > 0$, then K_0 is isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Remark: The subfield K_0 is called the **prime field of** K.

Exercise 2.6. Proof Fermat's little theorem: If K is a field of characteristic p, then $(a+b)^p = a^p + b^p$. Conclude that $\mathrm{Frob}_{p^n} : K \to K$ with $\mathrm{Frob}_{p^n}(a) = a^{p^n}$ is a field automorphism of K.

Remark: Frob_p is called the **Frobenius homomorphism in characteristic** p.

Exercise 2.7. Let $a, b \in \mathbb{R}$. Show that $a \geqslant b$ if and only if $a - b = c^2$ for some $c \in \mathbb{R}$. Conclude that the only field automorphism $\sigma : \mathbb{R} \to \mathbb{R}$ is the identity map.

Exercise 2.8. Recall the proofs of the Eisenstein criterium and Gauss' lemma, i.e. the content of fg equals the product of the contents of f and g for polynomials f, g over a unique factorization domain.

Chapter 3

Galois theory

3.1 Normal extensions

Definition. Let L/K be a field extension and $f \in K[T]$. Then f **splits over** L if $f = u\prod(T - a_i)$ in $L[T]$.

Definition. Let $\{f_i\}_{i \in I}$ be a subset of $K[T]$. A **splitting field of** $\{f_i\}$ **over** K is a field extension L/K such that f_i splits over L for every $i \in I$ and such that L is generated over K by the roots of all the f_i. If $S = \{f\}$, then we say that L is a **splitting field of** f **over** K.

Remark. Given a finite subset $\{f_1, \dots, f_n\}$ of $K[T]$, a field extension L/K is a splitting of $\{f_1, \dots, f_n\}$ over K if and only if it is a splitting field of the product $f_1 \cdots f_n$ over K.

Proposition 3.1.1. *Let $\overline{K}$ be an algebraic closure of K and $\{f_i\} \subset K[T]$. Let*

$$f_i \;=\; u_i \prod_{k=1}^{\deg f_i} (T - a_{i,k})$$

be the factorizations over $\overline{K}$. Then $K(a_{i,k})$ is a splitting field of $\{f_i\}$ over K.

If L/K is any other splitting field and $\sigma : L \to \overline{K}$ a K-linear field homomorphism, then $\sigma(L) = K(a_{i,k})$. In particular any two splitting fields of $\{f_i\}$ over K are isomorphic.

Proof. It is clear that $K(a_{i,k})$ is a splitting field of $\{f_i\}$ over K. Let L/K be another splitting field of $\{f_i\}$ and $f_i = v_i \prod(T - b_{i,k})$ the factorization in $L[T]$. Since

$$v_i \prod_{k=1}^{\deg f_i} (T - a_{i,k}) \;=\; f_i \;=\; \sigma(f_i) \;=\; \sigma(v_i) \prod_{k=1}^{\deg f_i} (T - \sigma(b_{i,k})),$$

and $K(a_{i,k})[T]$ is a UFD, we have $\{\sigma(b_{i,k})\} = \{a_{i,k}\}$. Thus the image of

$$\sigma :\; L \;=\; K(b_{i,k}) \;\longrightarrow\; \overline{K}$$

is $K(a_{i,k})$.

Given any splitting field L of $\{f_i\}$ over K, there exists a K-linear field homomorphism $\sigma : L \to \overline{K}$ by Lemma 2.2.7. Thus the previous claims imply that every splitting field of $\{f_i\}$ over K is isomorphic to $K(a_{i,k})$. □

Definition. A field extension L/K is **normal** if it is algebraic and if every irreducible polynomial $f \in K[T]$ with a root $a \in L$ splits over L.

Theorem 3.1.2. *Let L/K be an algebraic field extension. The following are equivalent:*

(1) L/K is normal.

(2) L is a splitting field of a family $\{f_i\}$ of polynomials $f_i \in K[T]$.

(3) For every field extension E/L, the image of a K-linear field homomorphism $\sigma : L \to E$ is L.

(4) Every K-linear field homomorphism $\sigma : L \to \overline{L}$ has image $\sigma(L) = L$.

Proof. (1)⇒(2): Consider $\{f_a\}_{a \in L}$ where f_a is the minimal polynomial of a over K. Then f_a splits over L by (1) and $L = K[a|a \in L]$. Thus (2).

(2)⇒(3): Let L be the splitting field of $\{f_i\}$ over K. Since L/K is algebraic, the image of a K-linear $\sigma : L \to E$ is contained in $E' = \{a \in E | a \text{ algebraic over } L\}$, which is an algebraic extension of K. Thus there is an embedding $\tau : E' \to \overline{K}$. By Proposition 3.1.1, $\overline{K}$ contains a unique splitting field F of $\{f_i\}$. Thus $\tau(\sigma(L)) = F = \tau(L)$ and $\sigma(L) = L$.

(3)⇒(4): Obvious.

(4)⇒(1): Let $f \in K[T]$ be irreducible and $a \in L$ a root of f. Let $b \in \overline{K}$ be another root of f. Then we have a field isomorphism

$$\begin{array}{cccccc} \sigma: & K(a) & \xrightarrow{\sim} & K[T]/(f) & \xrightarrow{\sim} & K(b), \\ & a & \longmapsto & [T] & \longmapsto & b \end{array}$$

which extends to a homomorphism $\sigma_L : L \to \overline{L}$ by Lemma 2.2.7. By (4), $\sigma_L(L) = L$; thus $b = \sigma(a) \in L$. Therefore L contains all roots of f, i.e. f splits over L. □

Corollary 3.1.3. *Let $K \subset E \subset L$ be a field extensions. If L/K is normal, then L/E is normal.*

Proof. Any E-linear field homomorphism $\sigma : L \to \overline{L}$ is K-linear. Since L/K is normal, Theorem 3.1.2 implies $\sigma(L) = L$. Applying 3.1.2 once again to L/E shows that L/E is normal. □

Definition. Let L/K be an algebraic field extension. A **normal closure of** L/K is a splitting field L^{norm} of $\{f_a\}_{a \in L}$ together with an inclusion $L \to L^{\text{norm}}$ where f_a is the minimal polynomial of a over K.

Corollary 3.1.4. *Let L/K be an algebraic field extension. Then L/K has a normal closure L^{norm} and L^{norm}/K is normal. We have*

$$L^{\text{norm}} = \bigcap_{\substack{L \subset E \subset \overline{L} \\ E/K \text{ normal}}} E.$$

Proof. This follows at once from Theorem 3.1.2. □

Example. (1) K/K is normal.

(2) Let L/K be of degree 2. If $f \in K[T]$ is irreducible with root $a \in L$, then $\deg f \leqslant 2$ since $K[T]/(f) \subset L$, and $T-a$ divides f. Thus $f = u(T-a)$ or $f = u(T-a)(T-b)$, i.e. f splits over L. Thus L/K is normal.

(3) $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not normal because

$$T^3 - 2 \;=\; (T - \sqrt[3]{2})\left(T^2 + \sqrt[3]{2}T + (\sqrt[3]{2})^2\right)$$

does not split over $\mathbb{Q}[\sqrt[3]{2}]$.

(4) Similarly $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ is not normal because

$$T^4 - 2 \;=\; (T - \underbrace{\sqrt[4]{2}}_{\in\mathbb{Q}[\sqrt[4]{2}]})\,(T + \underbrace{\sqrt[4]{2}}_{\in\mathbb{Q}[\sqrt[4]{2}]})\,(T - \underbrace{i\sqrt[4]{2}}_{\notin\mathbb{Q}[\sqrt[4]{2}]})\,(T + \underbrace{i\sqrt[4]{2}}_{\notin\mathbb{Q}[\sqrt[4]{2}]}),$$

does not split over $\mathbb{Q}[\sqrt[4]{2}]$.

Note: $L/\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ are successive extensions of degree 2 and thus normal, but $L/\mathbb{Q}$ is not. Thus the property to be normal is **not** transitive in field extensions.

Remark.

3.2 Separable extensions

Definition. Let K be a field, $f \in K[T]$ with factorization $f = u\prod_{i=1}^n (T - a_i)$ in $\overline{K}[T]$ and L/K a field extension.

(1) The polynomial f is **separable** if $a_1, \ldots, a_n$ are pairwise distinct.

(2) An element $a \in L$ is **separable over** K if it is algebraic over K and if its minimal polynomial over K is separable.

(3) The extension L/K is **separable** if every $a \in L$ is separable.

Definition. Let $f = \sum_{i=0}^n c_i T^i \in K[T]$. The **formal derivative of** f is

$$f' \;=\; \sum_{i=1}^n i \cdot c_i T^{i-1}.$$

Lemma 3.2.1. *If f is irreducible and **not** separable, then* $\operatorname{char} K = p > 0$ *and* $f = c_0 + c_p T^p + c_{2p} T^{2p} + \cdots$.

Proof. Consider the factorization $f = u\prod(T - a_i)$ in $\overline{K}[T]$. By Leibniz' formula (exercise!),

$$f' \;=\; u \cdot \sum_{i=1}^n \;\prod_{j \neq i} (T - a_j)$$

in $\overline{K}[T]$. Since f has a multiple root, say $a = a_1 = a_2$, we have $f'(a) = 0$.

Thus the minimal polynomial g of a over K divides f' and f. Since f is irreducible, $f = ug$. Since $\deg f' < \deg f$ and $f' \in (g) = (f)$, $f' = 0$.

This is only possible if $\operatorname{char} K = p > 0$ and all coefficients of $f' = \sum i \cdot c_i T^{i-1}$ are divisible by p, i.e. $c_i = 0$ if i is not a multiple of p. □

Corollary 3.2.2. *If* $\operatorname{char} K = 0$, *then every irreducible polynomial is separable.* □

Definition. Let L/K be an algebraic extension. The **separable degree of** L/K is the number

$$[L:K]_s \;=\; \#\,\{\,\sigma : L \to \overline{K} \,|\, \sigma(a) = a \text{ for } a \in K\,\}$$

of K-linear embeddings

$$\begin{tikzcd} L \arrow[rr, "\sigma"] & & \overline{K}. \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

Lemma 3.2.3. *Let L/K be an algebraic extension, $a \in L$ and $f = \sum c_i T^i$ the minimal polynomial of a over K. Then $[K(a):K]_s$ is equal to the number of roots of f in $\overline{K}$.*

Proof. A K-linear field homomorphism $\sigma : K(a) \to \overline{K}$ is determined by the image $\sigma(a)$ of a. Since σ leaves K fixed,

$$f(\sigma(a)) \;=\; \sum c_i \sigma(a)^i \;=\; \sigma\left(\sum c_i a^i\right) \;=\; \sigma(f(a)) \;=\; 0,$$

i.e. $\sigma(a)$ is a root of f in $\overline{K}$.

If conversely, b is a root of f in $\overline{K}$, then the minimal polynomial g of b divides f. Since f is irreducible, $f = ug$. Since $\mathrm{ev}_b : K[T] \to \overline{K}$ has kernel $(g) = (f)$, we obtain a K-linear homomorphism

$$\begin{array}{rccccc} \sigma: & K(a) & \xrightarrow{\sim} & K[T]/(f) & \xrightarrow{\mathrm{ev}_b} & \overline{K} \\ & a & \longmapsto & [T] & \longmapsto & b \end{array}$$

that maps a to b. This establishes a bijection

$$\begin{array}{ccc} \left\{ \begin{tikzcd} K(a) \arrow[rr, "\sigma"] & & \overline{K} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \right\} & \xleftrightarrow{1:1} & \{\text{ roots of } f \text{ in } \overline{K}\,\}. \\ \sigma & \longmapsto & \sigma(a) \end{array}$$

□

Corollary 3.2.4. *We have $[K(a):K]_s \leqslant [K(a):K]$, and an equality holds if and only if a is separable over K.*

Proof. Let f be the minimal polynomial of a. Then

$$[K(a):K]_s \;=\; \#\{\text{roots of } f \text{ in } \overline{K}\} \;\leqslant\; \deg f \;=\; [K(a):K].$$

We have an equality if and only if all the roots of f are pairwise distinct. This is the case if and only if f is separable, i.e. if a is separable. □

Lemma 3.2.5. *Let $K \subset E \subset L$ be finite field extensions. Then $[L:K]_s = [L:E]_s \cdot [E:K]_s$.*

Proof. Consider

$$S = \left\{ \begin{tikzcd}[column sep=small] E \arrow[rr, "\sigma_i"] & & \overline{E} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \right\} \qquad \text{and} \qquad T_i = \left\{ \begin{tikzcd}[column sep=small] L \arrow[rr, "\tau_{i,j}"] & & \overline{L} \\ & E \arrow[ul, dash] \arrow[ur, "\sigma_i"'] & \end{tikzcd} \right\}.$$

Thus $\#S = [E:K]_s$ and $\#T_i = [L:E]_s$ for all i. Thus

$$[L:K]_s = \#\left\{ \begin{tikzcd}[column sep=small] L \arrow[rr, "\tau_{i,j}"] & & \overline{L} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \right\} = \sum_i \#T_i = \#T_i \cdot \#S = [L:E]_s \cdot [E:K]_s. \qquad \square$$

Corollary 3.2.6. *Let $L = K(a_1, \dots, a_n)$ be a finite extension of K. Then $[L:K]_s \leqslant [L:K]$, and equality holds if $a_1, \dots, a_n$ are separable over K.*

Proof. Define $K_i = K(a_1, \dots, a_i)$ and consider

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L.$$

Since $K_{i+1} = K_i(a_{i+1})$, Corollary 3.2.4 implies $[K_{i+1}:K_i]_s \leqslant [K_{i+1}:K_i]$, with an equality if a_{i+1} is separable over K_i, which is the case if a_{i+1} is separable over K. By Lemma 3.2.5,

$$[L:K]_s = \prod_{i=0}^{n-1} [K_{i+1}:K_i]_s \leqslant \prod_{i=0}^{n-1} [K_{i+1}:K_i] = [L:K],$$

with equality if $a_1, \dots, a_n$ are separable over K. $\square$

Theorem 3.2.7. *Let $L = K(a_1, \dots, a_n)$ be a finite extension of K. The following are equivalent:*

(1) L/K is separable.

(2) $a_1, \dots, a_n$ are separable over K.

(3) $[L:K]_s = [L:K]$.

Proof. (1)⇒(2): Clear.

(2)⇒(3): This is Corollary 3.2.6

(3)⇒(1): Consider $a \in L$ and $K \subset K(a) \subset L$. Then

$$[L:K(a)]_s \cdot [K(a):K]_s = [L:K]_s = [L:K] = [L:K(a)] \cdot [K(a):K].$$

Since $[-]_s \leqslant [-]$ (Corollary 3.2.6), we have $[K(a):K]_s = [K(a):K]$. Thus a is separable over K by Corollary 3.2.4, and L/K is separable. $\square$

Corollary 3.2.8. *Let $K \subset E \subset L$ be finite field extensions. Then L/K is separable if and only if both L/E and E/K are separable.*

Proof. By Theorem 3.2.7, L/K is separable if and only if

$$[L:E]_s \cdot [E:K]_s \;=\; [L:K]_s \;=\; [L:K] \;=\; [L:E]\cdot[E:K].$$

Since $[-]_s \leqslant [-]$ (Corollary 3.2.6), this is the case if and only if $[L:E]_s = [L:E]$ and $[E:K]_s = [E:K]$. Using Theorem 3.2.7 once again, this is equivalent with both L/E and E/K being separable. □

Definition. L/K field extension. The **separable closure of** K **in** L is

$$E \;=\; \{a \in L \,|\, a \text{ separable over } K\}.$$

The **separable closure of** K is the separable closure of K in $\overline{K}$.

Corollary 3.2.9. *L/K field extension. The separable closure E of K in L is the largest subfield of L that is separable over K.*

Proof. Let $a_1, a_2 \in E$. Thus $K(a_1,a_2)/K$ is separable by Theorem 3.2.7, and

$$a_1 + a_2,\; a_1 - a_2,\; a_1 \cdot a_2,\; a_1/a_2 \;\in\; K(a_1,a_2) \;\subset\; E$$

are separable over K. This shows that E is a subfield of L. By the definition of the separable closure, E is the largest subfield of L that is separable over K. □

Remark. Later we will see that $[L:K]_s = [E:K]$, and thus $[L:K]_s$ is a divisor of $[L:K]$.

Theorem 3.2.10 (Theorem of the primitive element)**.**
Let L/K be finite separable. Then there is an element $a \in L$ such that $L = K(a)$. The element a is called a ***primitive element for*** *L/K.*

Proof. $\underline{K\text{ finite:}}$ later (Theorem 3.5.1) / exercise.

$\underline{K\text{ infinite:}}$ $L = K(a_1,\dots,a_n)$ for some $a_1,\dots,a_n \in L$. Induction on $n \geqslant 1$:

$\underline{n=1:}$ $L = K(a_1)$.

$\underline{n>1:}$ $L = K(a_1,\dots,a_{n-1})(a_n)$. By the inductive hypothesis, $K(a_1,\dots,a_{n-1}) = K(b)$ for some primitive element b for $K(a_1,\dots,a_{n-1})/K$. Thus $L = K(a,b)$ for $a = a_n$.

Let $m = [L:K]$. Then there are m distinct embeddings

$$\begin{tikzcd} L \arrow[rr, "\sigma_i"] \arrow[dr, dash] & & \overline{K}. \\ & K \arrow[ur, dash] & \end{tikzcd}$$

Define

$$P(T) \;=\; \prod_{i\neq j}\Big[\big(\sigma_i(a)T + \sigma_i(b)\big) - \big(\sigma_j(a)T + \sigma_j(b)\big)\Big].$$

Since K is infinite, there is a $c \in K$ such that $P(c) \neq 0$. Thus $\sigma_1(ac+b),\dots,\sigma_m(ac+b)$ are pairwise distinct, i.e. $[K(ac+b):K]_s \geqslant m$. Since $K(ac+b) \subset L$ and $[L:K]_s = m$, we conclude that $L = K(ac+b)$. □

Remark. The proof works also for finite fields if K has more than $\deg P(T) = \frac{m^2-m}{2}$ elements.

3.3 The Galois correspondence

Definition. Let L/K be a field extension. Then we denote by $\mathrm{Aut}_K(L)$ the group of K-linear field automorphisms. The extension L/K is **Galois** if it is normal and separable. In this case, $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ is called the **Galois group of** L/K.

Definition. Let $H \subset \mathrm{Aut}_K(L)$ be a subgroup. Then

$$L^H = \left\{ a \in L \,\middle|\, \sigma(a) = a \text{ for all } \sigma \in H \right\}$$

is called the **fixed field of** H.

Remark. Since $\sigma(a*b) = \sigma(a)*\sigma(b) = a*b$ for all $a, b \in L^H$, $\sigma \in H$ and $* \in \{+, -, \cdot, /\}$, L^H is indeed a field. Clearly, $K \subset L^H \subset L$.

Theorem 3.3.1 (Fundamental theorem of Galois theory)**.** *Let L/K be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then the maps*

$$\begin{array}{ccc} \{K \subset E \subset L\} & \overset{1:1}{\longleftrightarrow} & \{\textit{subgroups } H < G\} \\ E & \overset{\Phi}{\longmapsto} & \mathrm{Gal}(L/E) \\ L^H & \overset{\Psi}{\longleftarrow\!\shortmid} & H \end{array}$$

are mutually inverse bijections.

A subextension E/K is normal if and only if $H = \mathrm{Gal}(L/E)$ is normal in G. In this case, $\sigma \mapsto \sigma|_E$ defines a group isomorphism $G/H \xrightarrow{\sim} \mathrm{Gal}(E/K)$, i.e. we have a short exact sequence

$$0 \longrightarrow \mathrm{Gal}(L/E) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K) \longrightarrow 0$$

of groups.

A part of the theorem can be proven directly with our techniques (Lemma 3.3.2), the rest will be completed at the end of this section, after we have proven a preliminary result by Artin (Thm. 3.3.3).

Lemma 3.3.2. *$L^G = K$ and Φ is injective.*

Proof. Let $a \in L^G$ and $\sigma : K(a) \to \overline{L}$ a K-linear field homomorphism. Let $\sigma_L : L \to \overline{L}$ be an extension of σ to L, which exists by Lemma 2.2.7. Since L/K is normal, $\sigma_L(L) = L$, i.e. $\sigma_L \in G$. Since $\tau(a) = a$ for every $\tau \in G$, $[K(a):K]_s = 1$. Since a is separable over K, $K(a) = K$, i.e. $a \in K$. Thus $L^G = K$.

Let $K \subset E \subset L$ be an intermediate field and $H = \mathrm{Gal}(L/E)$. Then $E = L^H$ by what we have proven. Thus if $H' = \mathrm{Gal}(L/E') = H$, then $E' = L^{H'} = L^H = E$. Thus Φ is injective. $\square$

Theorem 3.3.3 (Artin)**.** *Let L be a field with automorphism group $\mathrm{Aut}(L)$ and $G \subset \mathrm{Aut}(L)$ of finite order n. Let $K = L^G$. Then $[L:K] = n$ and L/K is Galois with Galois group $\mathrm{Gal}(L/K) = G$.*

The proof of this theorem will utilize the following two lemmas.

Lemma 3.3.4. *Let L/K be separable and $a \in L$. Define* $\deg_K(a) = [K(a) : K] = \deg(\mathrm{Mipo}_a)$. *Then*

$$[L:K] \;=\; \sup\left\{ \deg_K(a) \,\middle|\, a \in L \right\}.$$

In particular, $[L:K]$ *is finite if there is an* $n \in \mathbb{N}$ *such that* $\deg_K a \leqslant n$ *for all* $a \in L$.

Proof. Clearly $[L:K] \geqslant \deg_K(a)$ for all $a \in L$ and $[L:K] \geqslant n = \sup\{\deg_K(a) | a \in L\}$. Thus we can assume that n is finite and that there is an $a \in L$ with $\deg_K(a) = n$.

We claim that $L = K(a)$. Consider $b \in L$. Then $K(a,b) = K(c)$ for some $c \in L$ by the theorem of the primitive element (Thm. 3.2.10), i.e.

$$K \;\subset\; K(a) \;\subset\; K(a,b) \;=\; K(c).$$

Since $\deg_K(c) \leqslant n$, we have $[K(c) : K] \leqslant n$. Thus $K(a,b) = K(a)$, i.e. $b \in K(a)$. Therefore $L = K(a)$ as claimed, and $[L:K] = \deg_K(a) = n$, which completes the proof. $\square$

Lemma 3.3.5. *Let L/K be a finite extension. Then* $\#\mathrm{Aut}_K(L) \leqslant [L:K]_s$*, and equality holds if and only if L/K is normal. In particular,* $\#\mathrm{Aut}_K(L) = [L:K]$ *if and only if L/K is Galois.*

Proof.

$$\begin{array}{ccc} \mathrm{Aut}_K(L) & \longrightarrow & \left\{ \begin{tikzcd}[ampersand replacement=\&] L \arrow[rr, "\sigma"] \& \& \overline{L} \\ \& K \arrow[ul, dash] \arrow[ur, dash] \& \end{tikzcd} \right\} \\ L \xrightarrow{\sigma} L & \longmapsto & L \xrightarrow{\sigma} L \to \overline{L} \end{array}$$

is injective. This shows $\#Aut_K(L) \leqslant [L:K]_s$. We have an equality if and only if every $\sigma : L \to \overline{L}$ comes from $\mathrm{Aut}_K(L)$, which is the case if and only if $\sigma(L) = L$ for all σ, i.e. if L/K is normal. Thus the former claim.

The inequalities in

$$\#\mathrm{Aut}_K(L) \;\leqslant\; [L:K]_s \;\leqslant\; [L:K]$$

are equalities if and only if L/K is Galois. Thus the latter claim. $\square$

Proof of Theorem 3.3.3. Let $a \in L$ and $\{\sigma_1, \ldots, \sigma_r\}$ a maximal subset of G such that $\sigma_1(a), \ldots, \sigma_r(a)$ are pairwise distinct. For $\tau \in G$, also $\tau \circ \sigma_1(a), \ldots, \tau \circ \sigma_r(a)$ are pairwise distinct. By the maximality of $\{\sigma_1, \ldots, \sigma_r\}$, this shows that τ permutes the $\sigma_i(a)$, i.e. $\{\tau \circ \sigma_i\} = \{\sigma_i\}$.

Thus

$$f \;=\; \prod_{i=1}^{r} (T - \sigma_i(a))$$

is separable and $\tau(f) = f$ for all $\tau \in G$, i.e. $f \in K[T]$. Since $\mathrm{id}_L(a) = a$, a is a root of f.Thus a is separable over K and $\deg_K(a) \leqslant n$.

By Lemma 3.3.4, $[L:K] \leqslant n = \#G$ and by Lemma 3.3.5, $\#\mathrm{Aut}_K(L) \leqslant [L:K]$. Since $G < \mathrm{Aut}_K(L)$, we have $\#\mathrm{Aut}_K(L) = [L:K]$. Thus Lemma 3.3.5 implies that L/K is Galois with Galois group G. $\square$

Proof of Theorem 3.3.1. By Lemma 3.3.2, Φ is injective. Given $H < G$, then the extension L/L^H is Galois with Galois group H by Theorem 3.3.3. Thus Φ and Ψ are mutually inverse bijections.

If E/K is normal, then $\sigma(E) = E$ for every $\sigma \in G$, which yields a map

$$\begin{array}{cccc} \pi: & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(E/K). \\ & \sigma & \longmapsto & \sigma|_E \end{array}$$

Since every K-linear automorphism $\tau : E \to E$ extends to an automorphism $\tau_L : L \to L$ (Lemma 2.2.7 plus L/K is normal), π is surjective. Clearly, $\mathrm{Gal}(E/K) = \{\sigma : L \to L | \sigma|_E = \mathrm{id}_E\}$ is the kernel of π and therefore a normal subgroup.

Assume conversely that $H \lhd G$ is normal. Let $\sigma : E \to \overline{L}$ be a K-linear embedding with image E'. Then σ extends to an automorphism $\sigma_L : L \to L$ (Lemma 2.2.7 plus L/K is normal) and restricts to an isomorphism $\sigma_E : E \to E'$. Since L/K is normal, L/E' is normal, cf. Corollary 3.1.3. Let $H' = \mathrm{Gal}(L/E')$. Then we obtain an isomorphism

$$\begin{array}{ccc} H & \longrightarrow & H', \\ \big[\tau : E \to E\big] & \longmapsto & \big[\sigma_E \tau \sigma_E^{-1} : E' \to E'\big] \end{array}$$

i.e. $H' = \sigma_E H \sigma_E^{-1}$ is conjugated to H in G. Since $H \lhd G$, $H' = H$ and $E' = E$. This shows that E/K is normal and thus Galois. $\square$

3.4 An example

Consider $L = \mathbb{Q}[i, \sqrt{2}]$. In this section, we show that $L/\mathbb{Q}$ is Galois, determine its Galois group and intermediate fields.

$L/\mathbb{Q}$ is separable since $\mathrm{char}\,\mathbb{Q} = 0$ and normal since L is the splitting field of $\{T^2+1, T^2-2\}$ over $\mathbb{Q}$:

$$T^2+1 \;=\; (T-i)(T+i) \qquad \text{and} \qquad T^2-2 \;=\; (T-\sqrt{2})(T+\sqrt{2}).$$

Thus $L/\mathbb{Q}$ is Galois.

$\mathbb{Q}[i]$ has degree 2 over $\mathbb{Q}$ as splitting field of T^2+1 and L has degree 2 over $\mathbb{Q}[i]$ a splitting field of T^2-2 (note that $\sqrt{2} \notin \mathbb{Q}[i]$). Thus $[L:\mathbb{Q}] = [L:\mathbb{Q}[i]]\cdot[\mathbb{Q}[i]:\mathbb{Q}] = 4$ and

$$L \;=\; \big\{a+bi+c\sqrt{2}+di\sqrt{2}\,\big|\,a,b,c,d \in \mathbb{Q}\big\}.$$

We find the following four automorphisms of L

$$\begin{array}{ccc} L & \xrightarrow{\mathrm{id}_L} & L \\ i & \longmapsto & i \\ \sqrt{2} & \longmapsto & \sqrt{2} \end{array} \qquad \begin{array}{ccc} L & \xrightarrow{\sigma_i} & L \\ i & \longmapsto & -i \\ \sqrt{2} & \longmapsto & \sqrt{2} \end{array} \qquad \begin{array}{ccc} L & \xrightarrow{\sigma_{\sqrt{2}}} & L \\ i & \longmapsto & i \\ \sqrt{2} & \longmapsto & -\sqrt{2} \end{array} \qquad \begin{array}{ccc} L & \xrightarrow{\sigma_{i,\sqrt{2}}} & L \\ i & \longmapsto & -i \\ \sqrt{2} & \longmapsto & -\sqrt{2} \end{array}$$

Since $\#\mathrm{Gal}(L/\mathbb{Q}) = [L:\mathbb{Q}] = 4$ by Lemma 3.3.5, these are all automorphisms of L, i.e. $G = \mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}, \sigma_i, \sigma_{\sqrt{2}}, \sigma_{i,\sqrt{2}}\}$. Since each of these automorphisms has order 2, we see that G is the Klein four group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The diagram of subgroups of G is

$$\begin{tikzcd} & G \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\ \langle \sigma_i \rangle \arrow[dr, dash, "2"'] & \langle \sigma_{\sqrt{2}} \rangle \arrow[d, dash, "2"] & \langle \sigma_{i,\sqrt{2}} \rangle \arrow[dl, dash, "2"] \\ & \{\mathrm{id}_L\} & \end{tikzcd}$$

where the number at an edge indicates the index of the group on the bottom inside the group on the top of the edge. The fixed fields of the subgroups of index 2 are

$$L^{\langle \sigma_i \rangle} = \mathbb{Q}[\sqrt{2}], \qquad L^{\langle \sigma_{\sqrt{2}} \rangle} = \mathbb{Q}[i], \qquad L^{\langle \sigma_{i,\sqrt{2}} \rangle} = \mathbb{Q}[i\sqrt{2}],$$

and we get the following diagram of intermediate fields of L/K:

$$\begin{tikzcd} & L \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\ \mathbb{Q}[\sqrt{2}] \arrow[dr, dash, "2"'] & \mathbb{Q}[i] \arrow[d, dash, "2"] & \mathbb{Q}[i\sqrt{2}] \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$

3.5 Finite fields

Theorem 3.5.1. *Let p be a prime number, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements and $\overline{\mathbb{F}_p}$ its algebraic closure.*

(1) For every $n \geqslant 1$, there is a unique subfield $\mathbb{F}_{p^n}$ of $\overline{\mathbb{F}_p}$ with p^n elements, and all finite subfields of $\overline{\mathbb{F}_p}$ are of this form.

(2) $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ if and only if $n|m$. In this case, $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is Galois and primitive. Its Galois group is cyclic of order m/n, generated by

$$\begin{array}{rccc} \mathrm{Frob}_{p^n} : & \mathbb{F}_{p^m} & \longrightarrow & \mathbb{F}_{p^m}. \\ & a & \longmapsto & a^{(p^n)} \end{array}$$

(3) The unit group $\mathbb{F}_{p^n}^\times$ of $\mathbb{F}_{p^n}$ is cyclic of order $p^n - 1$.

Proof. (1): Every finite subfield $K \subset \overline{\mathbb{F}_p}$ contains $\mathbb{F}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Thus K is a $\mathbb{F}_p$-vector space of positive dimension and thus has p^n elements for some $n \geqslant 1$.

Existence of $\mathbb{F}_{p^n}$: Let $L \subset \overline{\mathbb{F}_p}$ be the splitting field of $f = T^{p^n} - T \in \mathbb{F}_p[T]$. Then $f = \prod (T - a_i)$ for some $a_i \in L[T]$.

Claim: $L = \{a_i\}$.

Note that $f(a) = 0$ if and only if $a^{p^n} = a$ for $a \in \overline{\mathbb{F}_p}$. We have

$$0^{p^n} = 0, \quad 1^{p^n} = 1, \quad (a_i + a_j)^{p^n} = a_i^{p^n} + a_j^{p^n} = a_i + a_j, \quad (a_i \cdot a_j)^{p^n} = a_i^{p^n} \cdot a_j^{p^n} = a_i \cdot a_j,$$

$$(a_i^{-1}) = (a_i^{p^n})^{-1} = a_i^{-1}, \quad (-a_i)^{p^n} = (-1)^{p^n} a_i^{p^n} = \begin{cases} -a_i & \text{if } p \text{ is odd,} \\ a_i = -a_i & \text{if } p = 2. \end{cases}$$

Thus $\{a_i\}$ forms a subfield of $\overline{\mathbb{F}_p}$ and $L = \{a_i\}$. ♦

Since $f' = p^n T^{p^n - 1} - 1 = -1$ has no root in common with f, f has no multiple roots and $\#L = \deg f = p^n$. We define $\mathbb{F}_{p^n} = L$ and note that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is normal and separable.

Uniqueness of $\mathbb{F}_{p^n}$: Consider $L \subset \overline{\mathbb{F}_p}$ with p^n elements. Then $L^\times$ is a group with $p^n - 1$ elements and thus $a^{p^n-1} = 1$ for all $a \in L^\times$ (by Lagrange's theorem). Therefore $f(a) = 0$ for all $a \in L$ where $f = T^{p^n} - T$. This shows that L is the splitting field of f and thus $L = \mathbb{F}_{p^n}$.

(2): If $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, then $\mathbb{F}_{p^m}$ is an $\mathbb{F}_{p^n}$-vector space and $p^m = (p^n)^d$ for some $d \geqslant 1$, i.e. $m = dn$.

If, conversely, $m = dn$, then every $a \in \mathbb{F}_{p^n}$ satisfies

$$a^{p^m} \;=\; (\cdots((a^{p^n})^{p^n})\cdots)^{p^n} \;=\; a.$$

Thus $a \in \mathbb{F}_{p^m}$.

Since $\mathbb{F}_{p^m}/\mathbb{F}_p$ is Galois, $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is so, too. $\mathbb{F}_{p^m}$ has at most one subfield of cardinality p^i for every $i = 1, \ldots, m-1$. Since $p \geqslant 2$, we have

$$\#\Big(\mathbb{F}_{p^m} - \bigcup_{E \subsetneq \mathbb{F}_{p^m}} E \Big) \geqslant p^m - \sum_{i=1}^{m-1} p^i \;>\; 1,$$

i.e. $\mathbb{F}_{p^m}$ contains an element a that is not contained in any proper subfield. Thus a is a primitive element for $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$.

The Galois group $G = \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$ has order $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = m/n = d$, and $\mathrm{Frob}_{p^n} \in G$ (exercise). Let $H = \langle \mathrm{Frob}_{p^n} \rangle < G$ and $e = \#H$ the exponent of Frob_{p^n}. Then $e \leqslant d$ and $\big(\mathrm{Frob}_{p^n}(a)\big)^e = 1$ for all $a \in \mathbb{F}_{p^m}^\times$. This means that a is a root of $f = T^{p^{ne}} - T$, which has p^{ne} different roots in $\overline{\mathbb{F}_p}$. Thus $p^{ne} \geqslant p^m$, i.e. $e \geqslant m/n = d$.

Therefore $\#H = e = d = \#G$, which shows that $G = H$ is cyclic and generated by Frob_{p^n}.

(3): $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$ is of order n. Thus $a^{p^n-1} = 1$ for all $a \in \mathbb{F}_{p^n}^\times$ and for all $k < p^n - 1$, there is an $a \in \mathbb{F}_{p^n}^\times$ such that $a^k \neq 1$.

Since $\mathbb{F}_{p^n}^\times$ is finite abelian,

$$\mathbb{F}_{p^n}^\times \;\simeq\; \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_r\mathbb{Z}$$

for some prime powers $q_1, \ldots, q_r$. Thus $p^n - 1 = q_1 \cdots q_r$ and

$$p^n - 1 \;=\; \min\{ k \in \mathbb{N} \,|\, a^k = 1 \text{ for all } a \in \mathbb{F}_{p^n}^\times \} \;=\; \mathrm{lcm}(q_1, \ldots, q_r),$$

which is only possible if $q_1, \ldots, q_r$ are pairwise coprime. Thus

$$\mathbb{F}_{p^n}^\times \;\simeq\; \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_r\mathbb{Z} \;\simeq\; \mathbb{Z}/(p^n - 1)\mathbb{Z}. \qquad \square$$

3.6 Exercises

Exercise 3.1. Let $f = T^6 + T^3 + 1 \in \mathbb{Q}[T]$ and $L = \mathbb{Q}[T]/(f)$. Show that f is irreducible and find all field homomorphisms $L \to \mathbb{C}$. Is $L/\mathbb{Q}$ normal?

Hint: f divides $T^9 - 1$.

Exercise 3.2. Let $\mathbb{F}_p(x)$ be the quotient field of the polynomial ring $\mathbb{F}_p[x]$ in the indeterminant x, i.e. $\mathbb{F}_p(x) = \{f/g | f, g \in F_p[x] \text{ and } g \neq 0\}$.

(1) Show that $f = T^p - x$ is irreducible over $\mathbb{F}_p(x)$.

Hint: For a direct calculation, use the factorization of f over $\mathbb{F}_p(\sqrt[p]{x})$; or you can apply the Eisenstein criterium to show that f is irreducibel in $\mathbb{F}_p[x,T]$ and conclude with the help of Gauss' lemma that f is irreducible in $\mathbb{F}_p(x)[T]$.

(2) Show that f is not separable over $\mathbb{F}_p(x)$.

Hint: Use Fermat's little theorem.

(3) Conclude that $\mathbb{F}_p(\sqrt[p]{x})/\mathbb{F}_p(x)$ is not separable. Is $\mathbb{F}_p(\sqrt[p]{x})/\mathbb{F}_p(x)$ normal?

Exercise 3.3. Let $\zeta_3 = e^{2\pi/3} \in \mathbb{C}$ be a primitive third root of unity, i.e. $\zeta_3^3 = 1$, but $\zeta_3 \neq 1$. Which of the field extensions $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ of $\mathbb{Q}$ are Galois? What are the respective automorphism groups over $\mathbb{Q}$? Find all intermediate extensions of $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ and draw a diagram.

Exercise 3.4. Let L/K be a finite field extension and E the separable closure of K in L. Show that $[E:K]_s = [E:K]$ and $[L:E]_s = 1$. Conclude that the separable degree $[L:K]_s$ is a divisor of $[L:K]$.

Exercise 3.5. (1) Find a finite separable (but not normal) field extension L/K that does not satisfy the Galois correspondence.

(2) Find a finite normal (but not separable) field extension L/K that does not satisfy the Galois correspondence.

(3) Find a normal and separable (but not finite) field extension L/K that does not satisfy the Galois correspondence.

Exercise 3.6.
Calculate the Galois groups of the splitting fields of the following polynomials over $\mathbb{Q}$.

(1) $f_1 = T^3 - 1$;

(2) $f_2 = T^3 - 2$;

(3) $f_3 = T^3 + T^2 - 2T - 1$.

Hint: $\zeta_7^i + \zeta_7^{7-i}$ is a root of f_3 for $i = 1, 2, 3$.

Chapter 4

Applications of Galois theory

4.1 The central result

The central result of this chapter is a characterization of field extensions that can be generated by associating consecutively n-th roots in terms of Galois groups. Thanks to this characterization, we are able to solve the problems mentioned in Chapter 1. We need two definitions to state the result where we restrict to characteristic 0 for simplicity.

Definition. A finite field extension L/K of characteristic 0 is **a radical extension** if there exists a sequence of subfields

$$K = K_0 \ \subset \ K_1 = K_0(a_1) \ \subset \ K_2 = K_1(a_2) \ \subset \ \cdots \ \subset \ K_r = K_{n-1}(a_n) = L$$

such that $b_i = a_i^{n_i} \in K_{i-1}$ for all $i = 1, \ldots, r$ and some $n_i \geqslant 1$, i.e. $b_i = \sqrt[n_i]{a_i}$.

Definition. A finite group G is **solvable** if there exists a sequence of subgroups

$$\{e\} = G_0 \ \subset \ G_1 \ \subset \ \cdots \ \subset \ G_r = G$$

such that G_{i-1} is normal in G_i with cyclic quotient $G_i/G_{i-1} \simeq \mathbb{Z}/n_i\mathbb{Z}$ for all $i = 1, \ldots, r$.

Theorem. *Let L/K be a finite field extension of characteristic 0 and L^{norm} the normal closure of L/K. Then L is contained in a radical extension L'/K if and only if $\text{Gal}(L^{\text{norm}}/K)$ is solvable.*

4.2 Solvable groups

Definition. A group G is **simple** if $G \neq \{e\}$ and if the only normal subgroups of G are $\{e\}$ and G.

Example. $\mathbb{Z}/n\mathbb{Z}$ is simple if and only if n is prime.

Theorem 4.2.1. *The alternating group A_n is simple for $n \geqslant 5$.*

Proof. **Claim 1:** A_n is generated by 3-cycles.

We have

$$A_n = \left\langle (ij)(kl) \,\middle|\, i,j,k,l \in \{1,d\dots,n\} \text{ with } i \neq j, k \neq l \right\rangle$$

and

$$\begin{aligned}
&(ij)(kl) = (ijk)(jkl) && \text{if } i,j,k,l \text{ are pairwise distinct,}\\
&(ij)(jl) = (ijl) && \text{if } i,j,l \text{ are pairwise distinct,}\\
&(ij)(ij) = e. \quad \blacklozenge
\end{aligned}$$

Claim 2: All 3-cycles are conjugate in A_n.

Consider two 3-cycles (ijk) and $(i'j'k')$. Let $\gamma \in S_n$ such that $\gamma(i) = i'$, $\gamma(j) = j'$ and $\gamma(k) = k'$. Then $\gamma(ijk)\gamma^{-1} = (i'j'k')$, i.e. (ijk) and $i'j'k')$ are conjugate in S_n. If $\gamma \notin A_n$, then there are l,m such that i,j,k,l,m are pairwise distinct ($n \geqslant 5$). Then $\tilde{\gamma} = \gamma(l,m) \in A_n$ and $\tilde{\gamma}(ijk)\tilde{\gamma}^{-1} = (i'j'k')$ in A_n. $\blacklozenge$

Claim 3: Every normal subgroup $N \neq \{e\}$ of A_n contains a 3-cycle.

Let $\sigma \neq e$ be an element of N with maximal number of fixed points, which are $i \in \{1,\dots,n\}$ with $\sigma(i) = i$. Since $\sigma \neq e$, σ has at least one non-trivial cycle $(ij\dots)$.

Case 1: All orbits of σ have length $\leqslant 2$.

Then there are at least two cycles (ij) and (kl) of length 2 since $\operatorname{sign}\sigma = 1$. Let $m \in \{1,\dots,n\} - \{i,j,k,l\}$ and $\tau = (klm)$. Then

$$\sigma' = \underbrace{\tau\sigma\tau^{-1}}_{\in N}\underbrace{\sigma^{-1}}_{\in N} \quad \in N$$

and $\sigma'(i) = i$ $\sigma'(j) = j$ and $\sigma'(p) = p$ for all $p \neq m$ with $\sigma(p) = p$. Thus σ' has more fixed points than σ. Contradiction!

Case 2: σ has a cycle $(ijk\dots)$ and i,j,k are not the only non-fixed points.

Then there are distinct $l,m \in \{1,\dots,n\} - \{i,j,k\}$ such that $\sigma(l) \neq l$ and $\sigma(m) \neq m$ ($n \geqslant 5$). For $\tau = (klm)$, $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$. We have $\sigma'(i) = i$ and all fixed points of σ are fixed points of σ'. thus σ' has more fixed points than σ. Contradiction!

Thus σ must be a 3-cycle, which proves claim 3. $\blacklozenge$

If $N \neq \{e\}$ is a normal subgroup of A_n, then it contains a 3-cycle (claim 3), which is conjugated to all other 3-cycles (claim 2). Since N is normal, $A_n = \langle\text{3-cycles}\rangle = N$ (claim 1). $\square$

Definition. A **normal series (of length r)** of a group G is a sequence

$$\{e\} = G_0 \mathrel{\ntrianglelefteq} G_1 \mathrel{\ntrianglelefteq} \cdots \mathrel{\ntrianglelefteq} G_r = G$$

of normal subgroups $G_i \lhd G_{i+1}$. Its **factors** are the quotient groups $Q_i = G_i/G_{i-1}$ for $i = 1,\dots,r$. Sometimes we write

$$G_0 \underset{Q_1}{\lhd} G_1 \underset{Q_2}{\lhd} \cdots \underset{Q_r}{\lhd} G_r = G$$

A **refinement** of $G_0 \subsetneq\!\!\!\!\lhd \cdots \subsetneq\!\!\!\!\lhd G_r$ is a normal series $H_0 \subsetneq\!\!\!\!\lhd \cdots \subsetneq\!\!\!\!\lhd H_s$ of G such that $\{G_i\} \subset \{H_j\}$. A **composition series of** G is a normal series whose factors are simple groups.

Remark. A normal series is a composition series if and only if it has no proper refinement.

Example (Decomposition series for A_4 and S_4)**.** $\{e\} \lhd A_4 \lhd S_4$ is a normal series for S_4, but not a composition series since $\{e\} \lhd A_4$ has the refinement

$$\{e\} \underset{\mathbb{Z}/2\mathbb{Z}}{\lhd} \{e, (12)(34)\} \underset{\mathbb{Z}/2\mathbb{Z}}{\lhd} \{e, (12)(34), (13)(24), (14)(23)\} \underset{\mathbb{Z}/3\mathbb{Z}}{\lhd} A_4$$

which is a composition series for A_4. In particular, A_4 is not simple.

Remark. Every finite group has a composition series, but there are infinite groups without composition series, e.g. $G = \mathbb{Z}$.

Definition. Two normal series $G_0 \lhd \cdots \lhd G_r$ and $H_0 \lhd \cdots \lhd H_s$ of a group G are **equivalent** if $r = s$ and if their factors agree up to a permutation.

Example.

$$\{\bar{0}\} \underset{\mathbb{Z}/2\mathbb{Z}}{\lhd} \{\bar{0}, \bar{3}\} \underset{\mathbb{Z}/3\mathbb{Z}}{\lhd} \mathbb{Z}/6\mathbb{Z} \qquad \text{and} \qquad \{\bar{0}\} \underset{\mathbb{Z}/3\mathbb{Z}}{\lhd} \{\bar{0}, \bar{2}, \bar{4}\} \underset{\mathbb{Z}/2\mathbb{Z}}{\lhd} \mathbb{Z}/6\mathbb{Z}$$

are equivalent normal series.

Theorem 4.2.2 (Schreier)**.** *Any two normal series*

$$G_0 \subsetneq\!\!\!\!\lhd \cdots \subsetneq\!\!\!\!\lhd G_r \qquad \textit{and} \qquad H_0 \subsetneq\!\!\!\!\lhd \cdots \subsetneq\!\!\!\!\lhd H_s$$

of a group G have equivalent refinements.

Proof. We define

$$\begin{aligned} G_{i,j} &= G_{i-1}(G_i \cap H_j) && \text{for } i = 1, \ldots, r,\ j = 0, \ldots, s \\ H_{i,j} &= (G_i \cap H_j)H_{j-1} && \text{for } i = 0, \ldots, r,\ j = 1, \ldots, s \end{aligned}$$

and get refinements

$$\begin{aligned} G_0 = G_{1,0} \lhd G_{1,1} \lhd \cdots \lhd G_{1,s} = G_1 = G_{2,0} \lhd \ldots \lhd G_{r,s} = G_r, \\ H_0 = H_{0,1} \lhd H_{1,1} \lhd \cdots \lhd H_{r,1} = H_1 = H_{0,2} \lhd \ldots \lhd H_{r,s} = H_s. \end{aligned}$$

where some inclusions might not be proper. Using the third isomorphism theorem "$H/(H \cap N) \simeq HN/N$", we obtain

$$\begin{aligned} G_{i,j}/G_{i,j-1} \quad &= \quad G_{i-1}(G_i \cap H_j) \,/\, G_{i-1}(G_i \cap H_{j-1}) \\ &\underset{H=G_i\cap H_j,\, N=G_{i,j-1}}{\simeq} (G_i \cap H_j) \,/\, (G_{i-1} \cap H_j)(G_i \cap H_{j-1}) \\ &\underset{H=G_i\cap H_j,\, N=H_{i-1,j}}{\simeq} (G_i \cap H_j)H_{j-1} \,/\, (G_{i-1} \cap H_j)H_{j-1} \;=\; H_{i,j}/H_{i-1,j} \end{aligned}$$

Thus $G_{1,0} \lhd \cdots \lhd G_{r,s}$ and $H_{0,1} \lhd \cdots \lhd H_{r,s}$ have the same factors and are equivalent refinements (after removing the non-proper inclusions). $\square$

Two immediate consequences are the following.

Corollary 4.2.3. *If G has a composition series, then any normal series of G has a refinement that is a composition series.* □

Theorem 4.2.4 (Jordan-Hölder theorem)**.** *Any two composition series of G are equivalent.* □

The definition of solvable finite groups from section 4.1 extends to arbitrary groups as follows. We leave it as an exercise to verify that both definitions agree for finite groups.

Definition. A group is **solvable** if it has a normal series whose factors are abelian.

Example. (1) G abelian $\Rightarrow$ G solvable.

(2) G solvable and finite $\Rightarrow$ all factors in a composition series of G are cyclic of prime order p.

(3)
$$\{e\} \underset{\mathbb{Z}/3\mathbb{Z}}{\lhd} \{e, (123), (132)\} \underset{\mathbb{Z}/2\mathbb{Z}}{\lhd} S_3$$
has abelian factors; thus S_3 is solvable.

(4) S_4 is solvable, with composition series
$$\{e\} \underset{\mathbb{Z}/2\mathbb{Z}}{\lhd} \{e, (12)(34)\} \underset{\mathbb{Z}/2\mathbb{Z}}{\lhd} \{e, (12)(34), (13)(24), (14)(23)\} \underset{\mathbb{Z}/3\mathbb{Z}}{\lhd} A_4 \underset{\mathbb{Z}/2\mathbb{Z}}{\lhd} S_4.$$

(5) A_n is **not** solvable for $n \geqslant 5$. Thus S_n is **not** solvable for $n \geqslant 5$.

Remark. A deep theorem of Feit and Thompson states that every finite group G of odd order is solvable.

Lemma 4.2.5. *If $\#G = p^n$ for some prime p, then G is solvable.*

Proof. **Claim:** The center of G is non-trivial.

Consider the action of G on G by conjugation: $g.h = ghg^{-1}$. Then

- $a \in Z(G) \Leftrightarrow G.a = \{a\}$;
- $G.e = \{e\}$;
- $G.h = G/\operatorname{Stab}_G(h) \Rightarrow \#G.h | p^n$;
- $G = \coprod(\text{orbits})$.

Thus
$$\underbrace{\#G}_{\text{divisible by } p} = \#Z(G) + \sum_{G.h \neq \{h\}} \underbrace{\#G.h}_{\text{divisible by } p}$$
and p divides $\#Z(G)$. Thus $Z(G) \neq \{e\}$. ♦

Define $G_1 = G$ and $G_{i+1} = G_i/Z(G_i)$ for $i \geqslant 1$. Then we get

$$G = G_1 \xrightarrow{\pi_2} G_2 \xrightarrow{\pi_3} \cdots \xrightarrow{\pi_r} G_r = \{e\}.$$

Define $H_0 = \{e\}$, $H_1 = Z(G_1)$ and $H_i = (\pi_i \circ \cdots \pi_2)^{-1}\big(Z(G_i)\big)$, and we get a normal series

$$\{e\} = H_0 \underset{Z(G_1)}{\lhd} H_1 \underset{Z(G_2)}{\lhd} \cdots \underset{Z(G_r)}{\lhd} H_r = G$$

with abelian factors. Thus G is solvable. □

4.3 Cyclotomic extensions

Definition. An element $\zeta \in K$ is a **root of unity** (root of 1) if $\zeta^n = 1$ for some $n \geqslant 1$. It is a **primitive n-th root of unity** if $\operatorname{ord}\zeta = n$. In this case, we often write $\zeta_n = \zeta$. We define

$$\mu_n(K) = \{\zeta \in K \,|\, \zeta^n = 1\}, \qquad \mu_n = \mu_n(\overline{K}) = \{\zeta \in \overline{K} \,|\, \zeta^n = 1\}$$

and

$$\mu_\infty = \{\zeta \in \overline{K} \,|\, \zeta^n = 1 \text{ for some } n \geqslant 1\}.$$

Note that since $T^n - 1$ is defined over the prime field of K, μ_n depends only on the characteristic of K.

Lemma 4.3.1.

(1) If $\operatorname{char} K \nmid n$*, then* $f = T^n - 1$ *is separable and* $\#\mu_n = n$*.*

(2) If $\operatorname{char} K = p > 0$*, then* 1 *is the only root of* $T^{p^n} - 1$ *for every* $n \geqslant 1$*.*

Proof. (1): $f' = nT^{n-1} \neq 0$ in K and thus 0 is the only root of f', but $f(0) \neq 0$. Thus f is separable and has n different roots in $\overline{K}$, i.e. $\#\mu_n = n$.

(2): Clear since $T^{p^n} - 1 = (T-1)^{p^n}$. □

Remark. As a finite subgroup of K, $\mu_n(K)$ is cyclic, and $K(\zeta_n, \zeta_m) = K(\zeta_{\operatorname{lcm}(n,m)})$.

Definition. A field extension L/K is a **cyclotomic extension** if it is algebraic and if there is an embedding $L \to K(\mu_\infty)$. L/K is **abelian** if it is Galois with abelian Galois group.

Example. Let ζ_7 be a primitive root of 1 over $\mathbb{Q}$. Then $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ is cyclotomic. Note that it is not generated by roots of unity.

Theorem 4.3.2. *Every finite cyclotomic field extension is abelian.*

Proof. Fix an embedding $L \to K(\mu_\infty)$. Since L/K is finite, $L \subset K(\zeta_n)$ for some primitive n-th root ζ_n of 1. The case $L = K$ is clear. Otherwise, $n \geqslant 2$ and $\operatorname{char} K \nmid n$, i.e. $K(\zeta_n)/K$ is separable. Thus L/K is separable.

Given a K-linear field homomorphism $\sigma : K(\zeta_n) \to \overline{K}$, we have $\sigma(\zeta_n)^n = \sigma(\zeta_n^n) = 1$ and $\sigma(\zeta_n)^k \neq 1$ for $k < n$. Thus $\sigma(\zeta_n)$ is a primitive n-th root of 1, i.e. $\sigma(\zeta_n) = \zeta_n^i$ for some $i \in (\mathbb{Z}/n\mathbb{Z})^\times$. Thus $\operatorname{im}\sigma = K(\zeta_n)$ and $K(\zeta_n)/K$ is normal.

Since $\sigma : K(\zeta_n) \to \overline{K}$ is determined by $i = i(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$, we get an embedding $\sigma : \operatorname{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$. This is a group homomorphism since

$$\zeta_n^{i(\sigma\tau)} \;=\; \sigma\tau(\zeta_n) \;=\; \sigma(\tau(\zeta_n)) \;=\; (\zeta_n^{i(\tau)})^{i(\sigma)} \;=\; \zeta_n^{i(\tau)\cdot i(\sigma)},$$

i.e. $i(\sigma\tau) = i(\sigma)i(\tau)$.

Thus $\operatorname{Gal}(K(\zeta_n)/K) < (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, and every subgroup is normal with abelian quotients. This shows that L/K is normal and

$$\operatorname{Gal}(L/K) \;=\; \operatorname{Gal}(K(\zeta_n)/K) \;/\; \operatorname{Gal}(K(\zeta_n)/L)$$

is abelian. $\square$

Question. What is the image of the embedding $i : \operatorname{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$?

Consider $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ for p prime and $m = kn$. Then $\mathbb{F}_{p^m}$ is generated by a primitive r-th root of of unity ζ_r over $\mathbb{F}_{p^n}$ where $r = p^m - 1$, and the image of $i : \operatorname{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n}) = \langle \operatorname{Frob}_{p^n} \rangle$ is a cyclic subgroup of $(\mathbb{Z}/(p^m-1)\mathbb{Z})^\times$ of order k.

Theorem 4.3.3. *Assume that p is prime,* $\operatorname{char} K \neq p$ *and $\zeta_p \in \overline{K}$ a primitive p-th root of unity. Assume that $f = T^{p-1} + T^{p-2} + \cdots + T + 1$ is irreducible in $K[T]$. Then $[K(\zeta_p) : K] = p - 1$, and f is the minimal polynomial of ζ_p over K and* $\operatorname{Gal}(K(\zeta_p)/K) = (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$*.*

Proof. Since $f \cdot (T-1) = T^p - 1$, ζ_p^i is a root of f for $i = 1, \ldots, p-1$. Since f is irreducible, $\zeta_p^i \notin K$ for all $i = 1, \ldots, p-1$. Thus $K(\zeta_p)$ is the splitting field of f and of degree $p-1$ over K. By Lemma 4.3.1, f is separable and $K(\zeta_p)/K$ Galois. Therefore $i : \operatorname{Gal}(K(\zeta_p)/K) \to (\mathbb{Z}/p\mathbb{Z})^\times$ is an isomorphism, and f is the minimal polynomial of ζ_p. $\square$

Corollary 4.3.4. $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.

Proof. By Theorem 4.3.3, we need to show that $f = T^{p-1} + \ldots + 1$ is irreducible in $\mathbb{Q}[T]$. This is the case if $f(T+1)$ is irreducible. We have

$$\begin{aligned} f(T+1) &= \big[(T+1)^p - 1\big] \,/\, \big[(T+1) - 1\big] \\ &= \big[\big(\textstyle\sum_{i=0}^p \binom{p}{i} T^i\big) - 1\big] \,/\, T \\ &= \big[T^p + \tbinom{p}{p-1} T^{p-1} + \ldots + \tbinom{p}{1} T\big] \,/\, T \\ &= T^{p-1} + \tbinom{p}{p-1} T^{p-2} + \ldots + \tbinom{p}{1}. \end{aligned}$$

Since $\binom{p}{i}$ is divisible by p for all $i = 1, \ldots, p-1$ and $\binom{p}{1} = p$, $f(T+1)$ is irreducible by the Eisenstein criterion. $\square$

Definition. **Euler's φ-function** or **totient function** is $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 4.3.5. *$\zeta_n \in \overline{\mathbb{Q}}$ primitive n-th root of 1. Then the map $i : \mathrm{Gal}(Q(\zeta_n)/Q) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is a group isomorphism. Consequently $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

Proof. Let f be the minimal polynomial of ζ_n. Then $f | T^n - 1$, i.e. $T^n - 1 = f \cdot g$ for some $g \in \mathbb{Q}[T]$. Since the leading coefficient of f and $T^n - 1$ are 1, the leading coefficient of g is also 1, and thus $f, g \in \mathbb{Z}[T]$ by the Gauß lemma.

Claim: If p is prime and $p \nmid n$, then $f(\zeta_n^p) = 0$.

Assume that ζ_n^p is not a root of f. Then it is a root of g. Thus ζ_n is a root of $\tilde{g}(T) = g(T^p)$, and $f | \tilde{g}$, i.e. $\tilde{g} = f \cdot h$ for some $h \in \mathbb{Q}[T]$. Since the leading coefficient of $\tilde{g}$ is 1, also $h \in \mathbb{Z}[T]$.

We have $g(T)^p \equiv f \cdot h \pmod p$, thus the residue classes $\bar{f}$ and $\bar{g}$ in $\mathbb{F}_p[T]$ have a common factor in $\mathbb{F}_p[T]$ and $T^n - \bar{1} = \bar{f} \cdot \bar{g}$ has multiple roots in $\overline{\mathbb{F}}_p$, i.e. $T^n - \bar{1}$ is not separable over $\mathbb{F}_p$. Since $p \nmid n$, this contradicts Lemma 3.2.1. ♦

Since $p \nmid n$, ζ_n^p is a *primitive* n-th root of 1. For all primitive n-th roots $\tilde{\zeta}$ of 1, we have $\tilde{\zeta} = \zeta^i = \zeta_n^{p_1 \cdots p_r}$ for some $i \geqslant 1$ with prime decomposition $i = p_1 \cdots p_r$. Since $\tilde{\zeta}$ is primitive, $\gcd(i, n) = 1$ and thus $p_1, \dots, p_r \nmid n$.

Applying the claim successively to $p_1, \dots, p_r$ shows that $f(\tilde{\zeta}) = 0$. Thus all primitive n-th roots of 1 are roots of f and $\mathrm{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$. □

A deep result from algebraic number theory, which we will not prove here, is the following.

Theorem (Kronecker-Weber theorem)**.** *Every abelian extension of $\mathbb{Q}$ is cyclotomic.*

4.4 Norm and trace

Definition. Let L/K be finite Galois with Galois group $G = \mathrm{Gal}(L/K)$. The **norm of** L/K is the map

$$\mathrm{N}_{L/K} : \begin{array}{ccc} L & \longrightarrow & K, \\ a & \longmapsto & \prod_{\sigma \in G} \sigma(a) \end{array}$$

and the **trace of** L/K is the map

$$\mathrm{Tr}_{L/K} : \begin{array}{ccc} L & \longrightarrow & K. \\ a & \longmapsto & \sum_{\sigma \in G} \sigma(a) \end{array}$$

Remark. Since for all $\tau \in G$,

$$\tau\big(\prod \sigma(a)\big) = \prod \tau \circ \sigma(a) = \prod \sigma(a) \quad \text{and} \quad \tau\big(\sum \sigma(a)\big) = \sum \tau \circ \sigma(a) = \sum \sigma(a),$$

$\mathrm{N}_{L/K}(a)$ and $\mathrm{Tr}_{L/K}(a)$ are indeed elements of $K = L^G$. We have

$$\mathrm{N}_{L/K}(ab) = \mathrm{N}_{L/K}(a)\mathrm{N}_{L/K}(b) \qquad \text{and} \qquad \mathrm{Tr}_{L/K}(a+b) = \mathrm{Tr}_{L/K}(a) + \mathrm{Tr}_{L/K}(b).$$

If $a \in K$, then $\mathrm{N}_{L/K}(a) = a^n$ and $\mathrm{Tr}_{L/K}(a) = na$.

Lemma 4.4.1. *Let $K \subset E \subset L$ be field extensions such that all of L/K, L/E and E/K are Galois. Then* $\mathrm{N}_{L/K} = \mathrm{N}_{E/K} \circ \mathrm{N}_{L/E}$ *and* $\mathrm{Tr}_{L/K} = \mathrm{Tr}_{E/K} \circ \mathrm{Tr}_{L/E}$.

Proof.

$$\mathrm{N}_{L/K}(a) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma(a) = \prod_{\tau\in\mathrm{Gal}(E/K)} \Big(\prod_{\substack{\sigma\in\mathrm{Gal}(L/K)\\ \sigma|_E=\tau}} \sigma(a) \Big) = \prod_{\tau\in\mathrm{Gal}(E/K)} \tau\Big(\prod_{\sigma\in\mathrm{Gal}(L/E)} \sigma(a) \Big),$$

which is $\mathrm{N}_{E/K} \circ \mathrm{N}_{L/E}(a)$, and

$$\mathrm{Tr}_{L/K}(a) = \sum_{\sigma\in\mathrm{Gal}(L/K)} \sigma(a) = \sum_{\tau\in\mathrm{Gal}(E/K)} \Big(\sum_{\substack{\sigma\in\mathrm{Gal}(L/K)\\ \sigma|_E=\tau}} \sigma(a) \Big) = \sum_{\tau\in\mathrm{Gal}(E/K)} \tau\Big(\sum_{\sigma\in\mathrm{Gal}(L/E)} \sigma(a) \Big),$$

which is $\mathrm{Tr}_{E/K} \circ \mathrm{Tr}_{L/E}(a)$. □

Lemma 4.4.2. *Let $L = K(a)/K$ be Galois and $f = T^n + c_{n-1}T^{n-1} + \cdots + c_0$ the minimal polynomial of a over K. Then* $\mathrm{N}_{L/K}(a) = (-1)^n c_0$ *and* $\mathrm{Tr}_{L/K}(a) = -c_{n-1}$.

Proof. Let $G = \mathrm{Gal}(L/K)$. Over L,

$$f = \prod_{\sigma\in G} (T - \sigma(a)) = T^n - \underbrace{\big(\sum_{\sigma\in G} \sigma(a) \big)}_{=\mathrm{Tr}_{L/K}(a)} T^{n-1} + \cdots + (-1)^n \underbrace{\prod_{\sigma\in G} \sigma(a)}_{=\mathrm{N}_{L/K}(a)}. \qquad \square$$

Definition. Let H be a group and K a field. A **character of G in K** is a multiplicative function $\sigma : G \to K$ with image in $K^\times$. A set of functions $f_1, \ldots, f_n : G \to K$ is **linearly independent** if a relation $a_1 f_1 + \cdots + a_n f_n = 0$ with $a_i \in K$ implies $a_1 = \cdots = a_n = 0$.

Theorem 4.4.3. *Let G be a group, K a field and $\chi_1, \ldots, \chi_n : G \to K$ pairwise distinct characters. Then $\chi_1, \ldots, \chi_n$ are linearly independent.*

Proof. Assume there is a nontrivial relation

$$a_1\chi_1 + \ldots + a_n\chi_n = 0$$

and assume that n is minimal such that such a nontrivial relation exists. If $n = 1$, then $a_1\chi_1 = 0$ and thus $a_1 = 0$, which is a contradiction.

If $n \geqslant 2$, then there is a $g \in G$ such that $\chi_1(g) \neq \chi_2(g)$ since $\chi_1 \neq \chi_2$. Since

$$a_1\chi_1(g)\chi_1(h) + \cdots + a_n\chi_n(g)\chi_n(h) = a_1\chi_1(gh) + \cdots + a_n\chi_n(gh) = 0$$

for all $h \in G$, we have

$$a_1\chi_1(g)\chi_1 + \cdots + a_n\chi_n(g)\chi_n = 0.$$

Thus

$$\begin{aligned} 0 &= a_1\chi_1 + \cdots + a_n\chi_n - \chi_1(g)^{-1} \cdot \big[a_1\chi_1(g)\chi_1 + \cdots + a_n\chi_n(g)\chi_n\big] \\ &= \big[\underbrace{a_2 - a_2\chi_2(g)\chi_1(g)^{-1}}_{\neq 0}\big]\chi_2 + a_3'\chi_3 \ldots + a_n'\chi_n \end{aligned}$$

is a nontrivial relation for some $a_3', \ldots, a_n'$ that involves only $n-1$ terms, which is a contradiction. □

Corollary 4.4.4. *Let L/K be finite Galois. Then $\mathrm{Tr}_{L/K} : L \to K$ is not constant 0.*

Proof. If $\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$, then Theorem 4.4.3 implies that $\sigma_1 + \cdots + \sigma_n \neq 0$ as a map $L \to L$, i.e. there is an $a \in L$ such that

$$0 \neq \sigma_1(a) + \cdots + \sigma_n(a) = \mathrm{Tr}_{L/K}(a).$$

□

Definition. A field extension L/K is **cyclic** if it is finite Galois with cyclic Galois group.

Theorem 4.4.5 (Hilbert's theorem 90)**.** *Let L/K be cyclic and σ a generator of $\mathrm{Gal}(L/K)$. Then $\mathrm{N}_{L/K}(a) = 1$ if and only if there is a $b \in L$ such that $a = b/\sigma(b)$.*

Proof. $\underline{\Leftarrow:}$ If $a = b/\sigma(b)$, then

$$\mathrm{N}_{L/K}(a) = \prod_{\tau \in \mathrm{Gal}(L/K)} \frac{\tau(b)}{\tau\sigma(b)} = 1.$$

$\underline{\Rightarrow:}$ If $\mathrm{N}_{L/K}(a) = 1$ and $n = [L:K]$, then by Theorem 4.4.3,

$$\varphi = \mathrm{id}_L + a\sigma + (a \cdot \sigma(a))\sigma^2 + \cdots + \big(a \cdot \sigma(a) \cdots \sigma^{n-2}(a)\big)\sigma^{n-1}$$

is a non-constant map $\varphi : L \to L$, i.e. there is a $c \in L$ such that $b = \varphi(c) \neq 0$. Thus

$$a \cdot \sigma(b) = a\sigma(c) + a^2\sigma^2(c) + \cdots + \big(\underbrace{a \cdot \sigma(a) \cdots \sigma^{n-1}(a)}_{=\mathrm{N}_{L/K}(a)=1}\big)\underbrace{\sigma^n(c)}_{=c} = \varphi(c) = b$$

and $a = b/\sigma(b)$. □

The additive version of Hilbert's theorem 90 is the following.

Theorem 4.4.6. *Let L/K be cyclic and σ a generator of $\mathrm{Gal}(L/K)$. Then $\mathrm{Tr}_{L/K}(a) = 0$ if and only if there is a $b \in L$ such that $a = b - \sigma(b)$.*

Proof. $\underline{\Leftarrow:}$ If $a = b - \sigma(a)$, then

$$\mathrm{Tr}_{L/K}(a) = \sum_{\tau \in \mathrm{Gal}(L/K)} \big(\tau(b) - \tau\sigma(b)\big) = 0.$$

$\underline{\Rightarrow:}$ Assume $\mathrm{Tr}_{L/K}(a) = 0$. By Corollary 4.4.4, there is a $c \in L$ such that $\mathrm{Tr}_{L/K}(c) \neq 0$. Let $n = [L:K]$ and

$$b = \mathrm{Tr}_{L/K}(c)^{-1} \cdot \big[a\sigma(c) + \big(a + \sigma(a)\big)\sigma^2(c) + \cdots + \big(a + \cdots + \sigma^{n-2}(a)\big)\sigma^{n-1}(c)\big].$$

Then

$$\begin{aligned} b - \sigma(b) &= \mathrm{Tr}_{L/K}(c)^{-1} \cdot \Big[a\sigma(c) + \big(a + \sigma(a)\big)\sigma^2(c) + \cdots + \big(a + \cdots + \sigma^{n-2}(a)\big)\sigma^{n-1}(c) \\ &\qquad - \sigma(a)\sigma^2(c) + \cdots + \big(\underbrace{\sigma(a) + \cdots + \sigma^{n-1}(a)}_{=\mathrm{Tr}_{L/K}(a)-a=-a}\big)\underbrace{\sigma^n(c)}_{=c}\Big] \\ &= \mathrm{Tr}_{L/K}(c)^{-1} \cdot \big[a\sigma(c) + \cdots + a\sigma^{n-1}(c) + ac\big] \\ &= a \end{aligned}$$

□

4.5 Kummer and Artin-Schreier extensions

Definition. A field extension L/K is called a **Kummer extension (of degree** n**)** if $\#\mu_n(K) = n$ and if L/K is Galois with $\mathrm{Gal}(L/K)$ cyclic of degree n.

Note that if $\#\mu_n(K) = n$, then $\operatorname{char} K \nmid n$.

Theorem 4.5.1. *Let K be a field with $\#\mu_n(K) = n$.*

(1) If L/K is a Kummer extension of degree n, then there is an $a \in L$ with minimal polynomial $T^n - b$ over K such that $L = K(a)$.

(2) If $a \in \overline{K}$ is a root of $T^n - b$ for $b \in K$, then $K(a)/K$ is a Kummer extension of degree d where d is a divisor of n such that $c = a^d \in K$ and $T^d - c$ is the minimal polynomial of a over K.

Proof. (1): Let $\zeta_n \in K$ be a primitive n-th root of unity. Then $N_{L/K}(\zeta_n^{-1}) = (\zeta_n^{-1})^n = 1$ since $\zeta_n \in K$. By Theorem 4.4.5 ("Hilbert 90"), there is an $a \in L$ such that $\zeta_n^{-1} = a/\sigma(a)$, i.e. $\sigma(a) = \zeta_n a$. Thus

$$\sigma^i(a) \;=\; \zeta_n \sigma^{i-1}(a) \;=\; \cdots \;=\; \zeta_n^i a.$$

Since $a, \zeta_n a, \ldots, \zeta_n^{n-1} a$ are pairwise distinct, $[K(a):K] \geqslant n$ and thus $L = K(a)$. Since

$$\sigma(a^n) \;=\; \sigma(a)^n \;=\; (\zeta_n a)^n \;=\; a^n,$$

$b = a^n \in L^{\langle\sigma\rangle} = K$ and a is a root of $T^n - b$, which is the minimal polynomial of a over K since $\deg(T^n - b) = [K(a):K]$.

(2): If a is a root of $f = T^n - b$, then $\zeta_n^i a$ is a root of f for all $i = 0, \ldots, n-1$. Thus $f = \prod_{i=0}^{n-1}(T - \zeta_n^i a)$ decomposes in $K(a)[T]$, i.e. $K(a)$ is the splitting field of f and normal over K. Since f is separable, $K(a)/K$ is Galois. Let $G = \mathrm{Gal}(K(a)/K)$. Then

$$\begin{array}{rccc} \iota: & G & \longrightarrow & \mu_n(K) \\ & \sigma & \longrightarrow & \zeta_n^i \text{ such that } \sigma(a) = \zeta_n^i a \end{array}$$

is an injective group homomorphism. Thus $G = \langle\sigma\rangle$ is cyclic of order d dividing n.

Therefore $\iota(\sigma) = \zeta_n^i$ is a primitive d-th root of unity and

$$\sigma(a^d) \;=\; \sigma(a)^d \;=\; (\zeta_n^i a)^d \;=\; a^d,$$

which shows that $c = a^d$ is in $K(a)^{\langle\sigma\rangle} = K(a)^G = K$. Thus a is a root of $g = T^d - a$. Since $\deg g = \#G = [K(a):K]$, g is the minimal polynomial of a. □

Definition. A field extension L/K is an **Artin-Schreier extension (of degree** p**)** if $\operatorname{char} K = p$ and if L/K is cyclic of degree p.

Note that if $\operatorname{char} K = p$, then $\#\mu_p(K) = 1$.

Theorem 4.5.2. *Let* $\operatorname{char} K = p$.

(1) Let L/K be an Artin-Schreier extension of degree p. Then there is an $a \in L$ with minimal polynomial $T^p - T - b$ over K such that $L = K(a)$.

(2) Let $f = T^p - T - b \in K[T]$. Then f either is irreducible or decomposes into linear factors in $K[T]$. If f is irreducible and $a \in \overline{K}$ is a root, then $K(a)/K$ is an Artin-Schreier extension.

Proof. (1): Let $G = \mathrm{Gal}(L/K) = \langle \sigma \rangle$. Since

$$\mathrm{Tr}_{L/K}(-1) \;=\; \underbrace{(-1)+\cdots+(-1)}_{p \text{ times}} \;=\; 0,$$

Theorem 4.4.6 ("additive Hilbert 90") shows that there is an $a \in L$ such that $-1 = a - \sigma(a)$, i.e. $\sigma(a) = a+1$. Thus

$$\sigma^i(a) \;=\; \sigma^{i-1}(a)+1 \;=\; \cdots \;= a+i,$$

and $a, a+1, \ldots, a+(p-1)$ are pairwise distinct. Thus $[K(a):K] \geqslant p$, which shows that $L = K(a)$. Since

$$\sigma(a^p - a) \;=\; \sigma(a)^p - \sigma(a) \;=\; (a+1)^p - (a+1) \;=\; a^p + 1^p - a - 1 \;=\; a^p - a,$$

$b = a^p - a$ is an element of $L^{\langle\sigma\rangle} = L^G = K$. Thus a is a root of $T^p - T - b$.

(2): Let a be a root of $f = T^p - T - b$. Then

$$f(a+i) \;=\; (a+i)^p - (a+i) - b \;=\; a^p + i^p - a - i - b \;=\; a^p - a - b \;=\; 0$$

where $i^p = i$ since $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Thus $a, a+1, \ldots, a+(p-1)$ are pairwise distinct roots of f and f splits over $L = K(a)$. If $a \in K$, then f splits over $K = K(a)$.

Claim: If $a \notin K$, then f is irreducible over K.

Let $f = gh$ in $K[T]$. Then $g = \tilde{c}\prod_{i\in I}(T-(a+i))$ in $L[T]$ for some subset I of $\{0,\ldots,p-1\}$ and $g = \sum_{i=0}^d c_i T^i$ in $K[T]$ where $d = \#I$. Then

$$c_{d-1} \;=\; -\sum_{i\in I}(a+i) \;=\; -da - \sum_{i\in I} i,$$

which is in K if and only if $d = 0$ or $d = p$. Thus either g or h is a unit, which shows that f is irreducible. ♦

Assume that f is irreducible over K. Since $L = K(a)$ is the splitting field of f and f is separable, L/K is Galois. The K-linear automorphism

$$\begin{array}{cccccc} \sigma: & K(a) & \xrightarrow{\sim} & K[T]/(f) & \xrightarrow{\sim} & K(a+1) \simeq K(a), \\ & a & \longmapsto & [T] & \longmapsto & a+1 \end{array}$$

is of order $p = [L:K]$ and therefore generates $\mathrm{Gal}(K(a)/K)$. □

4.6 Radical extensions

Definition. Let E and F be two subfields of L. The **compositum EF of E and F in L** is the smallest subfield of L that contains both E and F.

For the next three lemmas, we fix the following situation:

$$\begin{tikzcd}[column sep=small] & EF \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[dr, dash] & & F \arrow[dl, dash] \\ & K & \end{tikzcd}$$

where all fields are assumed to be subfields of a fixed larger field L. Note that if $E = K(a_i)$ and $F = K(b_j)$, then $EF = K(a_i, b_j)$.

Lemma 4.6.1. *If E/K is normal, then EF/F is normal. If E/K is separable, then EF/F is separable.*

Proof. Let E/K be normal and consider an F-linear field homomorphism $\sigma : EF \to \overline{EF}$. Then $\sigma(E) = E$ since E/F is normal and $\sigma(F) = F$. Thus $\sigma(EF) = \sigma(E)\sigma(F) = EF$, i.e. EF/F is normal.

Let E/K be separable. Then every $a \in E$ is separable over E and thus separable over F. Since $EF = F(a|a \in E)$, EF is separable over F. $\square$

Lemma 4.6.2. *If E/K is Galois, then EF/F is Galois and*

$$\begin{array}{rccc} \varphi : & \mathrm{Gal}(EF/F) & \longrightarrow & \mathrm{Gal}(E/K) \\ & \sigma & \longmapsto & \sigma|_E \end{array}$$

is an injective group homomorphism.

Proof. By Lemma 4.6.1, EF/F is Galois. Since E/K is normal, $\sigma(E) = E$ and the restriction $\sigma|_E : E \to E$ is well-defined as an element of $\mathrm{Gal}(E/K)$. Clearly, φ is a group homomorphism. Consider $\sigma \in \ker\varphi$, i.e. $\sigma|_E = \mathrm{id}_E$. Since also $\sigma|_F = \mathrm{id}_F$, we have $\sigma = \mathrm{id}_{EF}$. Thus φ is injective. $\square$

Lemma 4.6.3. *If both E/K and F/K are Galois, then EF/K is Galois.*

Proof. Since both E/K and F/K are normal, every K-linear field homomorphism $\sigma : EF \to \overline{EF}$ satisfies $\sigma(EF) = \sigma(E)\sigma(F) = EF$. Thus EF/K is normal.

Since both E/K and F/K are separable, EF/F is separable by Lemma 4.6.1 and thus EF/K is separable by Corollary 3.2.8. Thus EF/K is Galois. $\square$

Definition. Let L/K be a finite field extension.

(1) L/K is **solvable** if it is Galois with solvable Galois group.

(2) L/K is a **simple radical extension** if it is separable and $L = K(a)$ for some $a \in L$ that is a root of a polynomial $f \in K[T]$ of the form

$$f = T^n - b \qquad \text{with } \operatorname{char} K \nmid n,$$
$$f = T^n - T - b \qquad \text{with } \operatorname{char} K = n.$$

(3) L/K is a **radical extension** if there exists a sequence

$$K = E_0 \subset E_1 \subset \cdots \subset E_l = L$$

of simple radical extensions. We call $E_0 \subset \cdots \subset E_l$ a **radical tower for** L/K.

(4) L/K is **contained in a radical extension** if there is a radical extension E/K such that $L \subset E$.

Example. (1) Every cyclotomic, Kummer and Artin-Schreier extension is solvable (since abelian) and simple radical (by definition).

(2) The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is simple radical since $\sqrt[3]{2}$ is a root of $T^3 - 2$. It is not solvable since it is not normal.

Lemma 4.6.4. *Let $K \subset E \subset L$ be finite Galois extensions such that also L/K is Galois. Then L/K is solvable if and only if both L/E and E/K are solvable.*

Proof. By Theorem 3.3.1 (Galois correspondence), we have a short exact sequence

$$1 \longrightarrow \mathrm{Gal}(L/E) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K) \longrightarrow 1.$$

The Lemma follows from Exercise 4.2. □

Lemma 4.6.5. *Let $K(a)/K$ be a simple radical extension, $\sigma : K(a) \to \overline{F}$ such that $\sigma(K) \subset F$ for some field F. Then $F(\sigma(a))/F$ is simple radical.*

Proof. Since $K(a)/K$ is simple radical, we can assume that a is a root of a polynomial of the form $f = T^n - b$ or $T^n - T - b$ with $b \in K$. Then $\sigma(a)$ is a root of $\sigma(f) \in F[T]$. Thus $F(\sigma(a))/F$ is simple radical, as claimed. □

Lemma 4.6.6. *Let $K \subset E \subset L$ be finite field extensions. Then L/E is contained in a radical extension if and only if both L/E and E/K are contained in radical extensions.*

Proof. $\underline{\Rightarrow:}$ Assume that L/K is contained in a radical extension F/K, i.e. there is a radical tower $K = F_0 \subset \cdots F_l = F$ with $L \subset F$. Then clearly E/K is contained in F/K as well. Define $F_i' = EF_i$ as the composition of E and F_i in F. By Lemma 4.6.5, F_{i+1}'/F_i' is simple radical. Thus the sequence $E = F_0' \subset \cdots \subset F_l' = F$ is a radical tower that contains L/E.

$\underline{\Leftarrow:}$ Assume that E/K is contained in a radical extension with tower $K = F_0 \subset \cdots \subset F_l$ and L/E is contained in a radical extension with tower $E = E_0 \subset \cdots \subset E_k$. Define $E_i' = E_i F_l$ (inside some fixed algebraic closure of both E_k and F_l). By Lemma 4.6.5, E_{i+1}'/E_i' is simple radical. Thus

$$K = F_0 \subset \cdots \subset F_k = E_0' \subset \ldots \subset E_k'$$

is a radical tower and $L \subset E_k'$, i.e. L/K is contained in the radical extension E_k'/K. □

Theorem 4.6.7. *Let L/K be separable. Then L/K is contained in a radical extension if and only if its normal closure L^{norm}/L in $\overline{L}$ is solvable.*

Proof. $\underline{\Leftarrow:}$ Assume that L^{norm}/K is solvable, i.e. $G = \mathrm{Gal}(L^{\mathrm{norm}}/K)$ is solvable. Define

$$n = \prod_{\substack{q \mid \#G \text{ prime} \\ q \neq \mathrm{char}\, K}} q.$$

In the following, we consider all fields as subfields of $\overline{K}$. Let $\zeta_n \in \overline{K}$ be a primitive n-th root of unity and define $F = K(\zeta_n)$. By Theorem 4.3.2, F/K is abelian and thus F/K is solvable. Since ζ_n is a root of $T^n - 1$ and $\mathrm{char}\, K \nmid n$ by the definition of n, F/K is simple radical.

Let $E = L^{\mathrm{norm}}$ and consider

$$\begin{tikzcd}
& EF \arrow[dl, dash] \arrow[dr, dash, "G'"] & \\
L^{\mathrm{norm}} = E \arrow[dr, dash, "G"'] & & F = K(\zeta_n) \\
& K \arrow[ur, dash, "\text{solvable \& radical}"'] &
\end{tikzcd}$$

where $G' = \mathrm{Gal}(EF/F)$ is a subgroup of $G = \mathrm{Gal}(E/K)$ by Lemma 4.6.2. By Lemma 4.6.3, EF/K is Galois.

By Exercise 4.2, the subgroup G' is solvable, i.e. there exists a normal series

$$\{e\} = G_0 \lhd \cdots \lhd G_r = G'$$

with factors $G_{i+1}/G_i \simeq \mathbb{Z}/p_i\mathbb{Z}$ for prime numbers p_i. Define $E_i = (EF)^{G_i}$. Then

$$F = E_r \subset \cdots \subset E_0 = EF$$

is a tower of cyclic extensions with Galois groups $\mathrm{Gal}(E_i/E_{i+1}) = G_{i+1}/G_i \simeq \mathbb{Z}/p_i\mathbb{Z}$.

If $p_i \neq \mathrm{char}\, K$, then $p_i | n$ and $\#\mu_{p_i}(F) = p_i$. Thus E_i/E_{i+1} is a Kummer extension and by Theorem 4.5.1, there is an $a_i \in E_i$ with minimal polynomial $T^{p_i} - b$ over E_{i+1} such that $E_i = E_{i+1}(a_i)$. Thus E_i/E_{i+1} is simple radical.

If $p_i = \mathrm{char}\, K$, then E_i/E_{i+1} is an Artin Schreier extension and by Theorem 4.5.2, there is an $a_i \in E_i$ with minimal polynomial $T^{p_i} - T - b$ over E_{i+1} such that $E_i = E_{i+1}(a_i)$. Thus E_i/E_{i+1} is simple radical.

This shows that $E_r \subset \cdots \subset E_0$ is a radical tower for EF/F. Since also F/K is radical, Lemma 4.6.6 implies that EF/K is radical. Thus L/K is contained in a radical extension.

$\underline{\Rightarrow:}$ Assume that L/K is contained in a radical extension with tower $K = F_0 \subset \cdots \subset F_s$ where $F_{i+1} = F_i(a_{i+1})$ is simple radical over F_i. We consider F_s as a subfield of $\overline{K}$. Let $\sigma_1 = \mathrm{id}_{F_s}, \ldots, \sigma_r : F_s \to \overline{K}$ be all K-linear embeddings. By Lemma 4.6.5, the successive adjunction of the elements $\sigma_1(a_1), \ldots, \sigma_r(a_s)$ yields a radical tower

$$K = F_0 \subset \cdots \subset F_s \subset F_{s+1} = F_s(\sigma_2(a_1)) \subset \ldots \subset F_t = K\big(\sigma_j(a_i)\big)_{\text{all } i,j}.$$

By definition F_t/K is the normal closure of F_s/K. Since $a_1,\dots,a_s$ are separable over K, as well as their Galois conjugates, F_t/K is Galois. Since $L \subset F_s$, we conclude that $L^{\text{norm}} \subset F_t$.

Define n as the largest divisor of $[F_t : K]$ that is not divisible by $\operatorname{char} K$ and consider

$$E_0 = F_0(\zeta_n) \subset \dots \subset E_t = F_t(\zeta_n)$$

By Lemma 4.6.5, E_{i+1}/E_i is simple radical for all $i = 0,\dots,t-1$, i.e. $E_{i+1} = E_i(a'_{i+1})$ for some $a'_{i+1} \in E_{i+1}$ that is a root of a polynomial of the form $f_i = T^{n_i} - b_i$ or $f = T^{n_i} - T - b_i$ over E_i. In the first case, $[E_{i+1} : E_i]$ is not divisible by $\operatorname{char} K$ and divides $[F_t : K]$. Thus $[E_{i+1} : E_i]$ divides n and $\zeta_n \in E_i$, thus Theorem 4.5.1 yields that E_{i+1}/E_i is a Kummer extension. In the second case, Theorem 4.5.2 yields that E_{i+1}/E_i is an Artin-Schreier extension. In both cases, E_{i+1}/E_i is Galois with cyclic Galois group. This yields a normal series

$$\{e\} = \mathrm{Gal}(E_t/E_t) \lhd \mathrm{Gal}(E_t/E_{t-1}) \lhd \cdots \lhd \mathrm{Gal}(E_t/E_0)$$

with cyclic factors, which shows that E_t/E_0 is solvable.

By Theorem 4.3.2, the cyclotomic extension $E_0 = K(\zeta_n)/K$ is abelian and thus solvable. By Lemma 4.6.4, E_t/K is solvable and thus L/K is solvable. □

Theorem 4.6.8 (Galois' solvability theorem). *Let K be a field of characteristic 0 and $f = \sum c_i T^i$ a polynomial in $K[T]$ with splitting field L and roots $a_1,\dots,a_n \in L$. If L/K is not solvable, then there is no formula for the a_j in the c_i in terms of $+$, $-$, $\cdot$, $/$ and $\sqrt[n]{\ }$.*

Proof. If there was such a formula, then the adjoining of n-th roots $\sqrt[n]{b}$ would yield a radical tower

$$K = E_0 \subset \cdots \subset E_r$$

such that $L \subset E_r$ and by Theorem 4.6.7, L/K would be solvable, which is not the case. □

Definition. Let L/K be a field extension and $a_1,\dots,a_n \in L$. Then L is a **rational function field in $a_1,\dots,a_n$ over K** if the K-linear ring homomorphism

$$\begin{array}{ccc} K[T_1,\dots,T_n] & \longrightarrow & L \\ T_i & \longmapsto & a_i \end{array}$$

is injective and the induced map $\operatorname{Frac}\big(K[T_1,\dots,T_n]\big) \to L$ is an isomorphism.

Theorem 4.6.9 (Abel). *Let $K = K_0(c_0,\dots,c_{n-1})$ be a rational function field in $c_0,\dots,c_{n-1}$ over K_0 and $f = T^n + c_{n-1}T^{n-1} + \cdots + c_0 \in K[T]$. Let L be the splitting of f over K and $a_1,\dots,a_n \in L$ its roots. Assume that $K_0[a_1,\dots,a_n]$ is a rational function field in $a_1,\dots,a_n$ over K_0. Then $\mathrm{Gal}(L/K) \simeq S_n$. In particular, if $\operatorname{char} K = 0$ and $n \geqslant 5$, then L is not contained in a radical extension of K.*

Remark. As we will see in the following proof, $K \subset L = K_0[a_1, \dots, a_n]$. As a consequence of Theorems 5.2.2 and 5.2.4, the transcendence degree of L over K_0 must be at greater or equal to the transcendence degree of K, which is n. Thus the elements $a_1, \dots, a_n$ form a transcendence basis for $K_0[a_1, \dots, a_n]$ over K_0, and it follows that $L = K_0[a_1, \dots, a_n]$ is a rational function field in $a_1, \dots, a_n$ over K_0. This means that this assumption can be removed in Theorem 4.6.9.

Proof. We have

$$f \;=\; T^n + c_{n-1}T^{n-1} + \cdots + c_0 \;=\; \prod_{i=1}^{n}(T - a_i)$$

$$c_i \;=\; (-1)^i s_i(a_1, \dots, a_n) \;=\; (-1)^i \sum_{e_1 < \cdots < e_i} a_{e_1} \cdots a_{e_i}$$

where s_i is the i-th elementary symmetric polynomial in n arguments. This shows that $c_0, \dots, c_{n-1} \in L$ and thus $L = K_0[a_1, \dots, a_n]$. Since $L \simeq \mathrm{Frac}\big(K_0[T_1, \dots, T_n]\big)$, every permutation of $\{a_1, \dots, a_n\}$ induces a unique K-linear field automorphism of L. This realizes S_n as a subgroup of $\mathrm{Aut}_{K_0}(L)$. Since $c_0, \dots, c_{n-1}$ are fixed under this action, we have $K \subset L^{S_n}$.

Claim: $[L : K] \leqslant n!$.

Consider the sequence

$$K \;\subset\; K(a_1) \;\subset\; \cdots \;\subset\; K(a_1, \dots, a_n) = L.$$

Then a_1 is a root of $f_1 = f$ and for $i \geqslant 2$, a_i is a root of

$$f_i \;=\; \frac{f}{(T - a_1)\cdots(T - a_{i-1})} \;=\; \frac{f_{i-1}}{T - a_{i-1}},$$

which is a polynomial in $K(a_1, \dots, a_{i-1})$ since $(T - a_{i-1}) | f_{i-1}$ in $K(a_1, \dots, a_{i-1})[T]$. Since $\deg f_i = n - (i-1)$,

$$[L : K] \;=\; \prod_{i=1}^{n} \big[K(a_1, \dots, a_i) : K(a_1, \dots, a_{i-1})\big] \;\leqslant\; \prod_{i=1}^{n} \deg f_i \;=\; n!. \blacklozenge$$

By Theorem 3.3.3 (Artin's theorem), we know that L/L^{S_n} is Galois with Galois group S_n. Thus

$$n! \;=\; \#S_n \;=\; [L : L^{S_n}] \;\leqslant\; [L : K] \;\leqslant\; n!,$$

which implies that $K = L^{S_n}$ and that L/K is Galois with $\mathrm{Gal}(L/K) = S_n$, as claimed.

Note that the last claim follows immediately from $\mathrm{Gal}(L/K) = S_n$, Theorem 4.6.7 and the fact that S_n is not solvable for $n \geqslant 5$ (Theorem 4.2.1). $\square$

Example. Consider $f = T^5 - 4T + 2 \in \mathbb{Q}[T]$. Let L be the splitting field of f over $\mathbb{Q}$. We claim that $G = \mathrm{Gal}(L/\mathbb{Q}) \simeq S_5$.

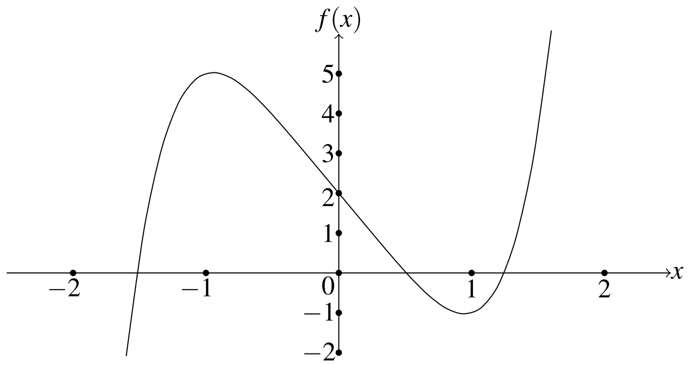
Let $a_1, \dots, a_5 \in L$ be the roots of f. Then G acts on $\{a_1, \dots, a_5\}$, i.e. $G < S_5$.

By the Eisenstein criterion, F is irreducible in $\mathbb{Z}[T]$. Since $\operatorname{cont}(f) = 1$, the Gauß lemma implies that f is irreducible in $\mathbb{Q}[T]$. Thus

$$\mathbb{Q} \underset{\deg 5}{\subset} \mathbb{Q}[T]/(f) \simeq \mathbb{Q}(a_1) \subset L,$$

which shows that 5 divides $\#G = [L : \mathbb{Q}]$, but 5^2 does not. By Sylow's theorem, G has a 5-Sylow subgroup, which shows that G must contain an element σ of order 5. As an element of S_5, σ is a 5-cycle.

Consider the graph of f as a function $f : \mathbb{R} \to \mathbb{R}$.



Note that $f' = 5T^4 - 4$ has the two real zeros $\pm\sqrt[4]{4/5}$, the two local extrema in the illustration are all local extrema of f.

By the intermediate value theorem, the function $f : \mathbb{R} \to \mathbb{R}$ has 3 zeros, and thus 2 complex roots. If we embed L into $\mathbb{C}$, then complex conjugation $\mathbb{C} \to \mathbb{C}$ restricts to an automorphism $\tau : L \to L$ that switches the two complex roots of f. Thus τ is an element of order 2 in G. As an element of S_5, τ is a transposition.

Since S_5 is generated by a 5-cycle and a transposition, we have $G = S_5$, as claimed.

4.7 Constructions with ruler and compass

In the following, we redefine the concept of constructible points in the Euclidean plane, using the identification of the Euclidean plane with $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$. We leave it as an exercise to verify that this coincides with the notion of constructibility from the first chapter.

Definition. Let K be a subfield of $\mathbb{C}$. An element $a \in \mathbb{C}$ is **constructible over** K if there exists a tower

$$K = E_0 \subset E_1 \subset \cdots \subset E_k$$

such that $a \in E_k$ and such that $E_{i+1} = E_i(a_{i+1})$ where a_{i+1} is the intersection point

- of two lines with end points in E_i,
- of two circles with center in E_i and radius in $E_i \cap \mathbb{R}$, or
- of a line and a circle with the previous properties.

Note that lines are defined by linear equations and circles by quadratic equations. Thus $[E_{i+1} : E_i]$ is 1 or 2.

Theorem 4.7.1. *Let $K \subset \mathbb{C}$ and $a \in \mathbb{C}$ be algebraic over K. Let $L = K(a)^{\mathrm{norm}}$ be the normal closure of $K(a)/K$. Then a is constructible if and only if $[L : K]$ is a power of 2.*

Proof. If a is constructible, then there is a tower $K = E_0 \subset \cdots \subset E_k$ of quadratic extensions $E_{i+1} = E_i(a_{i+1})/E_i$ such that $a \in E_k$. The normal closure E_k^{norm} of E_k in $\overline{E_k}$ is generated by the elements $\sigma(a_i)$ where $i = 1, \dots, k$ and where σ ranges through all K-linear embeddings $\sigma : E_k \to \overline{E_k}$. Adjoining successively the elements $\sigma(a_i)$ yields a tower

$$K = E_0 \subset \cdots \subset E_k \subset E_k(\sigma(a_1)) \subset \cdots \subset E_k^{\mathrm{norm}}$$

of degree 2 and possibly degree 1 extensions. Thus $[E_k^{\mathrm{norm}} : K]$ is a power of 2. Since L is a subfield of E_k^{norm}, $[L : K]$ is a divisor of $[E_k^{\mathrm{norm}} : K]$ and therefore also a power of 2.

Conversely, if $[L : K]$ is a power of 2, then $G = \mathrm{Gal}(L/K)$ is a 2-group and solvable by Lemma 4.2.5. Thus G has a composition series

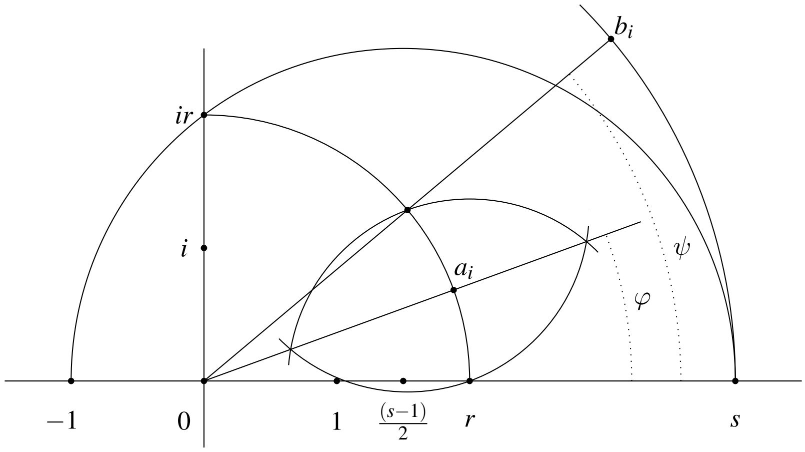
$$\{e\} = G_0 \lhd \cdots \lhd G_l = G$$

with factors $\mathbb{Z}/2\mathbb{Z}$. If we define $E_i = L^{G_i}$, then

$$K = E_l \subset \cdots \subset E_0 = L$$

is a tower of quadratic field extensions. Thus E_i/E_{i+1} is Galois with Galois group $\mathbb{Z}/2\mathbb{Z}$. Since $\zeta_2 = -1 \in E_{i+1}$, the extension E_i/E_{i+1} is a Kummer extension. By Theorem 4.5.1, $E_i = E_{i+1}(a_i)$ with $b_i = a_i^2 \in E_{i+1}$.

The element a_i can be constructed from b_i (and 0 and 1) as follows. Let $r = |a_i|$, $\varphi = \arg a_i$, $s = |b_i|$ and $\psi = \arg b_i$. Then $b_i = a_i^2$ means that $r = \sqrt{s}$ and $\varphi = \psi/2$, which can both be constructed from r and ψ. More precisely, the construction of a_i is summarized in the following picture:



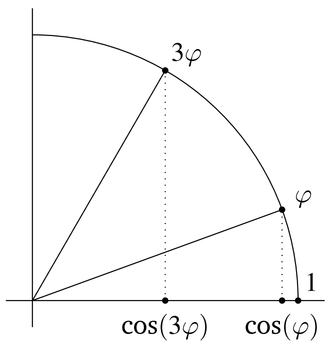
This shows that a_i is constructible over E_{i+1}. An easy induction shows that a is constructible over K. $\square$

Corollary 4.7.2. *The cube cannot be doubled.*

Proof. Given a cube with side length a, then the cube with twice the volume has side length $a\sqrt[3]{2}$. This must be true for $a = 1$ in particular. But $\sqrt[3]{2}$ generates the cubic extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Thus $[\mathbb{Q}(\sqrt[3]{2})^{\mathrm{norm}} : \mathbb{Q}]$ cannot be a power of 2. $\square$

Corollary 4.7.3. *Not every angle can be trisected.*

Proof. An angle φ corresponds to a point a on the unit circle. It is equivalent to know this point or its projection on the real axis, which is $\cos(\varphi)$. Therefore, the problem is equivalent with constructing $\cos(\varphi)$ from $\cos(3\varphi)$ for an arbitrary given angle $\psi = 3\varphi$.



Since $\cos(3\varphi) = 4\cos^3(\varphi) - 3\cos(\varphi)$, we are adjoining a root $a = \cos(\varphi)$ of $f = 4T^3 - 3T - b$ where $b = \cos(3\varphi)$. If, for instance, $b = 3/4$, then $4f = 16T^3 - 12T - 3$ is irreducible over $\mathbb{Q}$ (use the Eisenstein criterion and the Gauß lemma). Thus f is irreducible over $\mathbb{Q}$ and $\mathbb{Q}(a)/\mathbb{Q}$ is of degree 3. Thus $[\mathbb{Q}(a)^{\mathrm{norm}} : \mathbb{Q}]$ cannot be a power of 2. $\square$

Corollary 4.7.4. *The circle is cannot be squared.*

Proof. Given a circle with radius r, its area is $A = \pi r^2$. Thus a square with area A must have side length $\sqrt{\pi}r$. But π is transcendental over $\mathbb{Q}$ (by Lindemann, 1882), thus also $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$ and in particular not constructible. $\square$

Lemma 4.7.5. *Let $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ the Euler φ-function. If $n = \prod p_i^{e_i}$ is the prime decomposition of n with $p_i \neq p_j$ for $i \neq j$, then $\varphi(n) = \prod \big(p_i^{e_i-1}(p_i-1)\big)$.*

Proof. By the Chinese remainder theorem, we have

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod \big(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\big) \qquad \text{and thus} \qquad (\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod \big(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\big)^\times.$$

For each i, we have

$$\#(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times = \#(\mathbb{Z}/p_i^{e_i}\mathbb{Z}) - \#\big\{\overline{kp}\big\}_{k\geqslant 0} = p_i^{e_i} - p_i^{e_i-1} = p_i^{e_i-1}(p_i-1). \qquad \square$$

Corollary 4.7.6. *The regular n-gon is constructible over $\mathbb{Q}$ if and only if there is a finite subset $I \subset \mathbb{N}$ such that*

$$n = 2^r \cdot \prod_{i\in I} \big(2^{2^i}+1\big)$$

and such that $2^{2^i}+1$ is prime for every $i \in I$.

Proof. The regular n-gon is constructible over $\mathbb{Q}$ if and only if ζ_n is constructible over $\mathbb{Q}$. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, this is the case if and only if $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ is a power of 2. By Theorem 4.3.5, $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$.

If $n = \prod p_i^{e_i}$ is the prime decomposition of n, then $\varphi(n) = \prod \big(p_i^{e_i-1}(p_i-1)\big)$ by Lemma 4.7.5. The factor $p_i^{e_i-1}(p_i-1)$ is a power of 2 if and only if

(1) $p_i = 2$ and e_i arbitrary, or

(2) $p_i - 1 = 2^j$ and $e_i = 1$.

Thus the regular n-gon is constructible if and only if

$$n = 2^r \cdot \prod_{j\in J} \big(2^j+1\big)$$

for some finite subset $J \subset \mathbb{N}$.

Note that if $j = k\cdot l$ with l odd, then

$$2^j + 1 = (2^k+1)\,\big(2^{(l-1)k} - 2^{(l-2)k} + \ldots + 2^{2k} - 2^k + 1\big).$$

Thus if 2^j+1 is prime, then $l = 1$. This shows that $j = 2^i$ for some i. Thus indeed $n = 2^r \cdot \prod_{i\in I}\big(2^{2^i}+1\big)$, as claimed. $\square$

Definition. The ***i*-th Fermat number** is $F_i = 2^{2^i}+1$ for $i \geqslant 0$. If F_i is prime, then it is called a **Fermat prime**.

Fermat number	value	prime?
F_0	$2^{2^0}+1=3$	yes
F_1	$2^{2^1}+1=5$	yes
F_2	$2^{2^2}+1=17$	yes
F_3	$2^{2^3}+1=257$	yes
F_4	$2^{2^4}+1=65537$	yes
F_5	10 digits	no
$\vdots$	$\vdots$	$\vdots$
F_{32}	$\sim 10^9$ digits	no
F_{33}	$\sim 10^{10}$ digits	first unknown
$\vdots$	$\vdots$	$\vdots$
$F_{3.329.780}$	$\sim 10^{1.000.000}$ digits	no (largest known)

The information of this table is taken from http://www.prothsearch.com/fermat.html and reflects the knowledge from July 2018.

Conjecture. F_i is not prime for $i \geqslant 5$.

4.8 Normal bases

Definition. Let L/K be a finite Galois extension with $\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$. A **normal basis for** L **over** K is a basis of the form $\big(\sigma_1(a), \dots, \sigma_n(a)\big)$ where $a \in L$.

Theorem 4.8.1. *Every finite Galois extension of infinite fields has a normal basis.*

Remark. This theorem holds also for finite fields, and we will see a proof of this more general result in the second part of the course.

Proof. Let L/K be a finite Galois extension with Galois group $\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$ where we assume that K is infinite and $\sigma_1 = \mathrm{id}_L$. By Theorem 3.2.10 (theorem of the primitive element), $L = K(a)$ for some $a \in L$. Let f be the minimal polynomial of a over K and $a_i = \sigma_i(a)$ for $i = 1, \dots, n$ the roots of f. Define

$$g_i \;=\; \frac{f}{(T-a_i)f'(a_i)} \;=\; \frac{1}{\prod_{j\neq i}(a_i - a_j)} \prod_{j\neq i}(T - a_j),$$

which are polynomials in $L[T]$. Then

$$g_i(a_j) \;=\; \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

which means that $g_1 + \cdots + g_n - 1 \in L[T]$ has n different roots $a_1, \dots, a_n$. Since $\deg g_i = \deg f - 1 = n - 1$, this means that $g_1 + \cdots + g_n = 1$.

Since $(T-a_k)$ divides $g_i g_j$ for all $i \neq j$ and all k in $\{1,\dots,n\}$, we have $g_i g_j \equiv 0 \pmod f$. Thus

$$g_i \;=\; g_i \cdot \big(g_1+\cdots+g_n\big) \;=\; g_i g_1 + \ldots + g_i g_n \;\equiv\; g_i^2 \pmod f.$$

Define the $(n\times n)$-matrix $D = (\sigma_k \sigma_i(g_1))_{i,k=1,\dots,n}$ over $L[T]$. Since $a_i = \sigma_i(a)$ and $\sigma_1 = \mathrm{id}_L$, we have $a = a_1$ and $\sigma_i(g_1) = g_i$. Thus the previous relations for the g_i show that

$$D^2 \;\equiv\; \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \pmod f.$$

In turn, we have $\det D^2 \equiv 1 \pmod f$, which shows that the polynomial $\det D$ in $L[T]$ is not trivial. Since K is infinite, there is a $b \in K$ such that $(\det D)(b) \neq 0$, i.e. if $c = g(b)$, then $\det(\sigma_k\sigma_i(c))_{i,k} \neq 0$.

Consider relation

$$\lambda_1 \sigma_1(c) + \cdots + \lambda_n \sigma_n(c) \;=\; 0$$

with $\lambda_1,\dots,\lambda_n \in K$. Applying $\sigma_1,\dots,\sigma_n$ to this equation yields

$$\begin{array}{ccc} \lambda_1\sigma_1\sigma_1(c) + \cdots + \lambda_n\sigma_1\sigma_n(c) & = & 0 \\ \vdots \qquad\qquad \vdots & & \vdots \\ \lambda_1\sigma_n\sigma_1(c) + \cdots + \lambda_n\sigma_n\sigma_n(c) & = & 0 \end{array}$$

Since $\det(\sigma_k\sigma_i(c))_{i,k} \neq 0$, this can only be satisfied for $\lambda_1 = \cdots = \lambda_n = 0$. This shows that $\sigma_1(c),\dots,\sigma_n(c)$ are linearly independent over K. Thus $\big(\sigma_1(c),\dots,\sigma_n(c)\big)$ is a normal basis for L/K. $\square$

Lemma 4.8.2. *Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and $a \in L$ such that $\big(\sigma(a)\big)_{\sigma\in G}$ is a normal basis for L/K.*

(1) Let H be a subgroup of G. Then

$$L^H \;=\; \Big\{ \sum_{\sigma\in G} c_\sigma \sigma(a) \,\Big|\, c_\sigma \in K \text{ such that } c_\sigma = c_{\tau\sigma} \text{ for all } \sigma\in G,\, \tau\in H \Big\}.$$

(2) Let H be a normal subgroup of G and $I \subset G$ a set of representatives for G/H. Define $b = \sum_{\tau\in H}\tau(a)$. Then $\big(\sigma(b)\big)_{\sigma\in I}$ is a normal basis for L^H over K.

Proof. (1): Consider an element $\sum c_\sigma\sigma(a)$ be an element of L. For $\tau \in H$, we have

$$\tau\Big(\sum_{\sigma\in G} c_\sigma\sigma(a)\Big) \;=\; \sum_{\sigma\in G} c_\sigma \tau\sigma(a) \;=\; \sum_{\sigma\in G} c_{\tau^{-1}\sigma}\sigma(a).$$

Thus $\tau\big(\sum c_\sigma\sigma(a)\big) = \sum c_\sigma\sigma(a)$ if and only if $c_\sigma = c_{\tau\sigma}$ for all $\sigma\in G$ and $\tau \in H$.

(2): Let $\sigma \in G$. Since $\sigma H = H\sigma$,

$$\sigma(b) \;=\; \sum_{\tau\in H} \sigma\tau(a) \;=\; \sum_{\tau\in H}\tau\sigma(a)$$

is invariant under H, i.e. $\sigma(b) \in L^H$. By (1), $\big(\sigma(b)\big)_{\sigma\in I}$ spans L^H over K. Since $\#G/H = [L^H : K]$, it is a basis of L^H/K and since $\big(\sigma(b)\big)_{\sigma\in I} = \big(\sigma(b)\big)_{\sigma\in\mathrm{Gal}(L^H/K)}$, it is a normal basis. $\square$

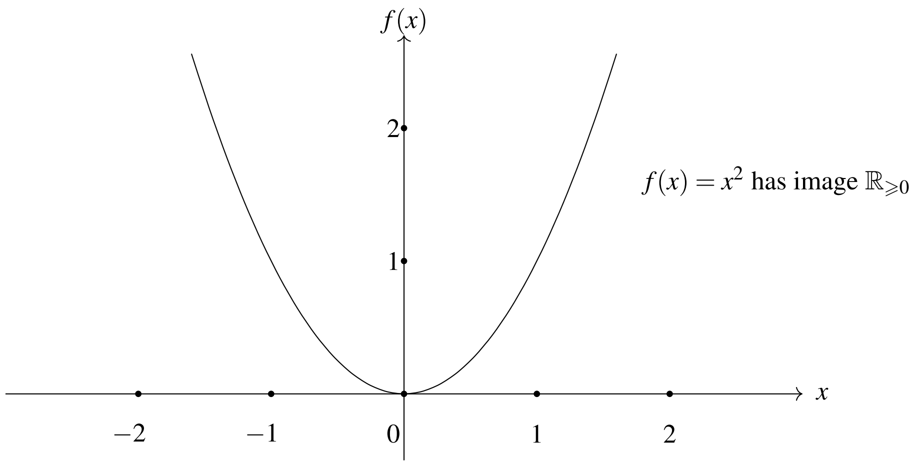
4.9 The fundamental theorem of algebra

Theorem 4.9.1. *$\mathbb{C}$ is algebraically closed.*

Proof. We use the following facts from real analysis, which both follow from the intermediate value theorem.

Fact 1: Let $a \in \mathbb{R}$. Then $a \geqslant 0$ if and only if there is a $b \in \mathbb{R}$ such that $a = b^2$.

Indeed, "$\Leftarrow$ " follows from the fact that the image of $f : x \mapsto x^2$ is contained in $\mathbb{R}_{\geqslant 0}$; and "$\Rightarrow$ " follows since every given $a \geqslant 0$ lies between $f(0) = 0^2$ and $f(c) = c^2$ for a sufficiently large $c \in \mathbb{R}$ and thus equals $f(b) = b^2$ for some $b \in \mathbb{R}$ by the intermediate value theorem. ♦



Fact 2: Every polynomial $f \in \mathbb{R}[T]$ of odd degree and with leading coefficient 1 has a real root $a \in \mathbb{R}$.

Indeed, for small $b \in \mathbb{R}$, we have $f(b) < 0$ and for large $c \in \mathbb{R}$ we $f(c) > 0$. By the intermediate value theorem, there is an $a \in \mathbb{R}$ such that $f(a) = 0$. ♦

Claim 1: Every $z \in \mathbb{C}$ has a square root.

Write $z = a + bi$ with $a, b \in \mathbb{R}$. By Fact 1, there are $c, d \in \mathbb{R}$ with

$$c^2 = \frac{1}{2}\big(\underbrace{a + \sqrt{a^2 + b^2}}_{\geqslant 0}\big) \qquad \text{and} \qquad d^2 = \frac{1}{2}\big(\underbrace{-a + \sqrt{a^2 + b^2}}_{\geqslant 0}\big).$$

Thus we obtain $(c + di)^2 = a + bi$. ♦

Let $L/\mathbb{C}$ be a finite field extension. After enlarging L, we can assume that both $L/\mathbb{C}$ and $L/\mathbb{R}$ are Galois.

Claim 2: $L = \mathbb{C}$.

Let $G = \mathrm{Gal}(L/\mathbb{R})$, $H < G$ a 2-Sylow subgroup and $E = L^H$. Then $E/\mathbb{R}$ is of odd degree $\#(G/H)$. By Theorem 3.2.10 (theorem of the primitive element), $E = \mathbb{R}(a)$ for some $a \in E$. Let f be the minimal polynomial of a over $\mathbb{R}$. Then f has odd degree and thus a root in $\mathbb{R}$ by Fact 2. Since f is irreducible, we have $f = T - a$ and $E = \mathbb{R}$, which shows that $G = H$ is a 2-group.

Therefore $G' = \mathrm{Gal}(L/\mathbb{C}) < G$ is also a 2-group. Either $G' = \{e\}$ and $L = \mathbb{C}$ (as claimed), or G' has a subgroup H' of index 2 since G' has a composition series and every composition series of G' has factors $\mathbb{Z}/2\mathbb{Z}$ by Lemma 4.2.5. If $F = L^{H'}$, then $F/\mathbb{C}$ is cyclic of degree 2. Since $\zeta_2 = -1 \in \mathbb{C}$, Theorem 4.5.1 shows that $F = \mathbb{C}(a)$ for a root a of a polynomial $T^2 - b \in \mathbb{C}[T]$. But by Claim 1, $a = \sqrt{b} \in \mathbb{C}$, which is a contradiction. □

4.10 Exercises

Exercise 4.1. Let

$$0 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 0$$

be a short exact sequence of groups. Show that N and Q are solvable if and only if G is solvable.

Exercise 4.2. Find all composition series and their factors for the dihedral group

$$D_6 \;=\; \langle r, s \,|\, r^6 = s^2 = e,\, srs = r^{-1} \rangle.$$

Exercise 4.3. Let K be a field and G a finite subgroup of the multiplicative group $K^\times$. Show that G is cyclic, which can be done along the following lines.

(1) Let $\varphi(d)$ be the number of generators of a cyclic group of order d. Show for $n \geqslant 1$ that

$$\sum_{d|n} \varphi(d) \;=\; n.$$

Remark: The function $\varphi(d)$ is called **Euler's φ-function**.

(2) Let $G_d \subset G$ be the subset of elements of order d. Show that G_d is empty if d is not a divisor of n and that G_d has exactly $\varphi(d)$ elements if it is not empty.

Hint: Use that $T^d - 1$ has at most d roots in a field.

(3) Let n be the cardinality of G. Conclude that G must have an element of order n and that G is cyclic.

Exercise 4.4 (Cyclotomic polynomials)**.** Let $\mu_\infty = \{\zeta \in \overline{\mathbb{Q}} | \zeta^n = 1 \text{ for some } n \geqslant 1\}$. Define

$$\Phi_d \;=\; \prod_{\substack{\zeta\in\mu_\infty \\ \text{of order } d}} (T - \zeta).$$

(1) Show that $\prod_{d|n} \Phi_d = T^n - 1$ for $n \geqslant 1$.

(2) Show that Φ_d has integral coefficients, i.e. $\Phi_d \in \mathbb{Z}[T]$.

(3) Let $\zeta \in \mu_\infty$ be of order d. Show that Φ_d is the minimal polynomial of ζ over $\mathbb{Q}$.

(4) Conclude that $\deg \Phi_d = \varphi(d)$ and that Φ_d is irreducible in $\mathbb{Z}[T]$.

(5) Show that $\Phi_d = T^{d-1} + \cdots + T + 1$ if d is prime.

(6) Calculate Φ_d for $d = 1, \ldots, 12$.

The polynomial Φ_d is called the **d-th cyclotomic polynomial**.

Exercise 4.5. Show that there is an n_i for $i = 1,2,3$ such that the following fields E_i are contained in $\mathbb{Q}(\zeta_{n_i})$. What are the smallest values for n_i?

(1) $E_1 = \mathbb{Q}(\sqrt{2})$;

(2) $E_2 = \mathbb{Q}(\sqrt{3})$;

(3) $E_3 = \mathbb{Q}(\sqrt{-3})$;

Hint: Try to realize $\sqrt{2}$ and $\sqrt{3}$ as the side length of certain rectangular triangles. Which angles do occur?

Exercise 4.6. Let ζ_{12} be a primitive 12-th root of unity. What is $\mathrm{Gal}(\mathbb{Q}(\zeta_{12}/\mathbb{Q}))$? Find primitive elements for all subfields E of $\mathbb{Q}(\zeta_{12})$.

Exercise 4.7. Let L be the splitting field of $T^3 - 2$ over $\mathbb{Q}$. Show that $\sqrt[3]{2}$, $\sqrt{-3}$ and ζ_3 are elements of L. Calculate $\mathrm{N}_{L/\mathbb{Q}}(a)$ and $\mathrm{Tr}_{L/\mathbb{Q}}(a)$ for $a = \sqrt[3]{2}$, $a = \sqrt{-3}$ and $a = \zeta_3$. Calculate $\mathrm{N}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\zeta_3)$ and $\mathrm{Tr}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\zeta_3)$.

Exercise 4.8. Let L be the splitting field of $f = T^4 - 3$ over $\mathbb{Q}$. What is the Galois group of $L/\mathbb{Q}$? Make a diagram of all subgroups of $\mathrm{Gal}(L/K)$ that illustrates which subgroups are contained in others. Which of the subextensions of $L/\mathbb{Q}$ are elementary radical? Is $L/\mathbb{Q}$ radical?

Hint: Find the four complex roots $a_1, \ldots, a_4$ of f. Which permutations of $a_1, \ldots, a_4$ extend to field automorphisms of L?

Exercise 4.9. Let L/K be a Galois extension and let

$$\begin{array}{rccc} M_a : & L & \longrightarrow & L \\ & b & \longmapsto & a \cdot b \end{array}$$

be the K-linear map associated with an element $a \in L$. Show that the trace of M_a equals $\mathrm{Tr}_{L/K}(a)$ and that the determinant of M_a equals $\mathrm{N}_{L/K}(a)$.

Hint: Use Exercise 2.1.

Exercise 4.10. Let p be a prime number and $n \geqslant 1$ and $\zeta \in \mathbb{F}_{p^n}$ a generator of $\mathbb{F}_{p^n}^\times$. Exhibit an embedding $i : \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \to (\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ and conclude that n divides $\varphi(p^n - 1)$. Can you find a proof for $n | \varphi(p^n - 1)$ that does not use Galois theory?

Exercise 4.11. Let K be a field and L the splitting field of a cubic polynomial f over K. Assume that $\zeta_3 \in L$ and that L/K is separable. Show that there is a subfield E of L such that $K \subset E \subset L$ is a tower of elementary radical extensions (with possibly $L = E$ or $E = K$). In which situations are E/K and L/E cyclotomic, Kummer and Artin-Schreier? What are E and L if $K = \mathbb{Q}$ and $f = T^3 - b \in \mathbb{Q}[T]$?

Exercise 4.12. Let $L/\mathbb{Q}$ be a cubic solvable extension. Show that $L/\mathbb{Q}$ is not radical. Show that such an extension exists.

Hint: Show that if $L/\mathbb{Q}$ was radical, it must contain ζ_3. Lead this to a contradiction.

Exercise 4.13. Which roots of the following polynomials are constructible over $\mathbb{Q}$?

(1) $f_1 = T^4 - 2$

(2) $f_2 = T^4 - T$

(3) $f_3 = T^4 - 2T$

Exercise 4.14. Let K be a subfield of $\mathbb{C}$ and a a root of $T^2 - b \in K[T]$. Show that every element of $K(a)$ is constructible over K. Use this to explain the relationship between the two definitions of constructible numbers from sections 1.1 and 4.6 of the lecture.

Exercise 4.15. Let K be a field and L the splitting field of a polynomial f over K of degree 4 or less. Show that L/K is solvable if it is separable.

Chapter 5

Non-Galois extensions

5.1 Inseparable extensions

In this section, we study field extensions that are not separable. The reader might keep the extension $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$ as a guiding example in mind.

Proposition 5.1.1. *Let K be a field of characteristic $p > 0$ and $\overline{K}$ an algebraic closure of K. Consider $a \in \overline{K}$ with minimal polynomial f over K. Then there is an $n \geqslant 0$ such that the following holds:*

(1) Every root of f has multiplicity p^n.

(2) a^{p^n} is separable over K.

(3) $[K(a):K] = p^n \cdot [K(a):K]_s$

Proof. (1): Let $a = a_1, \dots, a_r \in \overline{K}$ be the distinct roots of f and $e_1, \dots, e_r$ their respective multiplicities, i.e. $f = c \cdot \prod (T - a_i)^{e_i}$ in $\overline{K}[T]$.

Since f is irreducible in $K[T]$, f is the minimal polynomial of each a_i. Thus we have isomorphisms

$$\begin{array}{rcccccc} \sigma_i: & K(a) & \xrightarrow{\sim} & K[T]/(f) & \xrightarrow{\sim} & K(a_i) \\ & a & \longmapsto & [T] & \longmapsto & a_i \end{array}$$

for every i, which extend to automorphisms $\overline{\sigma}_i : \overline{K} \to \overline{K}$ by Lemma 2.2.7.

Since f has coefficients in K and $\sigma_j(f) = f$, we have

$$\prod_{i=1}^{r} (T - a_i)^{e_i} \;=\; f \;=\; \sigma_j(f) \;=\; \prod_{i=1}^{r} (T - \overline{\sigma}_j(a_i))^{e_i},$$

which implies that $e_j = e_1$ for all $j = 1, \dots, r$. Thus all roots have the same multiplicity $e = e_1 = \dots = e_r$.

By Lemma 3.2.1, $f = \sum c_{ip} T^{ip}$ if it is not separable. Thus $f = g(T^p)$ for $g = \sum c_{ip} T^i$ with $\deg f = p \cdot \deg g$, and a^p is a root of g. Repeating this argument if necessary, we find an $n \geqslant 0$ and a separable polynomial h in $K[T]$ such that $f = h(T^{p^n})$ and $\deg f = p^n \deg h$. We will show that this n satisfies (1)–(3).

The polynomial h is irreducible since a decomposition $h = h_1 \cdot h_2$ yields a decomposition $f = f_1 \cdot f_2$ with $f_i = h_i(T^{p^n})$. Since f is irreducible, one of f_1 or f_2 is a unit, which means that one of h_1 and h_2 is a unit.

Since a^{p^n} is a root of h, we have $K[T]/(h) \simeq K(a^{p^n})$. Since $\deg f = p^n \cdot \deg h$, we have $[K(a):K] = p^n \cdot [K(a^{p^n}):K]$ and $[K(a):K(a^{p^n})] = p^n$.

Since a is a root of multiplicity p^n of $T^{p^n} - a^{p^n}$, which is a polynomial over $K(a^{p^n})$, and since $(T-a)^{p^n} = T^{p^n} - a^{p^n}$ divides f, we have $e \geqslant p^n$. Since h is separable, it has $s = \deg h$ pairwise distinct roots. Thus f has $r \geqslant s$ distinct roots.

Since $p^n \cdot s = p^n \cdot \deg g = \deg f = e \cdot r$, we conclude that $e = p^n$ and $r = s$, which verifies (1) and (2). By Lemma 3.2.3, we have $[K(a):K]_s = \#\{\text{roots of } f\} = r$ and thus $[K(a):K] = p^n \cdot r = p^n \cdot [K(a):K]_s$, which shows (3). □

Definition. Let L/K be a finite extension. The **inseparable degree of L over K** is $[L:K]_i = [L:K]/[L:K]_s$.

The following is an immediate consequence of Proposition 5.1.1.

Corollary 5.1.2. *Let L/K be a finite extension. If $\operatorname{char} K = p > 0$, then $[L:K]_i = p^n$ for some $n \geqslant 0$.* □

Corollary 5.1.3. *Let $K \subset E \subset L$ be finite extensions. Then $[L:K]_i = [L:E]_i \cdot [E:K]_i$.*

Proof. This follows immediately from the multiplicativity of the degree of L/K (Lemma 2.1.3) and the separable degree of L/K (Lemma 3.2.5). □

Definition. Let L/K be an algebraic extension of fields of characteristic $p > 0$. An element $a \in L$ is **purely inseparable over** K if there is an $n \geqslant 0$ such that $a^{p^n} \in K$. The extension L/K is **purely inseparable** if every $a \in L$ is purely inseparable over K.

Theorem 5.1.4. *Let L/K be a finite extension and $a_1, \dots, a_r \in L$ such that $L = K(a_1, \dots, a_r)$. Then the following are equivalent.*

(1) L/K is purely inseparable.

(2) $a_1, \dots, a_r$ are purely inseparable over K.

(3) $[L:K]_s = 1$.

(4) The minimal polynomial of every $a \in L$ over K is of the form $T^{p^n} - a^{p^n}$ for some $n \geqslant 0$.

Proof. (1)⇒ (2): This follows directly from the definition.

(2)⇒ (3): Let $a_1, \dots, a_r$ are purely inseparable over K. Then the minimal polynomial f_i of a_i over K is a divisor of $T^{p^{n_i}} - a_i^{p^{n_i}}$ for some $n_i \geqslant 0$. This means that a_i is the only root of f_i. Thus every K-linear field homomorphism $\sigma : L \to \overline{L}$ sends a_i to a_i, which means that there is only one such homomorphism. Thus $[L:K]_s = 1$.

(3)⇒ (4): Let $a \in L$. Then $[K(a):K]_s \leqslant [L:K]_s = 1$ and thus a is the only root of its minimal polynomial f over K. By Proposition 5.1.1,

$$\deg f \;=\; [K(a):K] \;=\; p^n \cdot [K(a):K]_s \;=\; p^n.$$

Thus $f = (T-a)^{p^n} = T^{p^n} - a^{p^n}$.

(4)$\Rightarrow$ (1): This follows directly from the definition of a purely inseparable extension. $\square$

Corollary 5.1.5. *Let L/K be algebraic and E the separable closure of K in L. Then E/K is separable of degree $[E:K] = [L:K]_s$ and L/E is purely inseparable of degree $[L:E] = [L:K]_i$.*

Proof. The extension E/K is separable by its definition. By Proposition 5.1.1, there is for every $a \in L$ an $n \geqslant 0$ such that a^{p^n} is separable over K. Thus $a^{p^n} \in E$, i.e. a is purely inseparable over E. Thus L/E is purely inseparable.

Since E/K is separable, $[E:K]_s = [E:K]$. By Theorem 5.1.4, $[L:E]_s = 1$. Thus $[L:K]_s = [L:E]_s \cdot [E:K]_s = [E:K]$ and $[L:K]_i = [L:K]/[L:K]_s = [L:E]$. $\square$

Definition. A field K is **perfect** is every algebraic field extension L/K is separable.

Example.

- Every field of characteristic 0 is perfect.
- Every algebraically closed field is perfect.
- Every finite field is perfect.
- If K is perfect and L/K is algebraic, then L is perfect.
- If char $K = p > 0$, then $K(T)$ is **not** perfect.

5.2 Transcendental extensions

Definition. Let L/K be a field extension and S be a subset of L. Then S is **algebraically independent over** K if the K-linear homomorphism

$$\begin{array}{rccc} \mathrm{ev}_S: & K[T_a | a \in S] & \longrightarrow & L \\ & T_a & \longmapsto & a \end{array}$$

is injective. Otherwise, S is called **algebraically dependent over** K. The subset S is called a **transcendence basis for** L/K if it is a maximal algebraically independent subset over K.

Remark. Let L/K be a field extension and $S \subset L$ algebraically independent over K. Then

$$K(S) = \bigcap_{\substack{K \subset E \subset L \\ \text{s.t. } S \subset E}} E \simeq \mathrm{Frac}\big(K[T_a | a \in S]\big)$$

is the smallest subfield of L that contains S.

Lemma 5.2.1. *Let L/K be a field extension and $S \subset L$ algebraically independent over K. Then S is a transcendence basis for L/K if and only if L is algebraic over $K(S)$.*

Proof. $\underline{\Rightarrow:}$ Assume that S is a transcendence basis for L/K. Then there is for every $t \in L$ a nonzero polynomial $f \in K[X_s | s \in S][T]$ such that $f((s)_{s\in s}, t) = 0$ since $S \cup \{t\}$ is not algebraically independent. We can write

$$f = \sum_{i=0}^{n} f_i((X_s)_{s\in S}) T^i.$$

Since S is algebraically independent, $f_i((s)_{s\in S}) \neq 0$ if $f_i((X_s)_{s\in S} \neq 0$. Thus $f((s)_{s\in S}, T)$ is a nonzero element of $K(S)[T]$, which shows that t is algebraic over $K(S)$. Thus $L/K(S)$ is algebraic.

$\underline{\Leftarrow:}$ Assume that $L/K(S)$ is algebraic. Then there is for every $t \in L$ a nonzero polynomial $f \in K(S)[T]$ such that $f(t) = 0$. Since $K(S) \simeq \mathrm{Frac}(K[X_s | s \in S])$, f is of the form

$$f = \sum_{i=0}^{n} \frac{g_i((s))}{h_i((s))} T^i$$

for some polynomials $g_i((X_s)), h_i((X_s)) \in K[X_s | s \in S]$ with $h_i \neq 0$. Multiplying f with $h = \prod h_i$ yields

$$\tilde{f} = h \cdot f = \sum_{i=0}^{n} \big[\prod_{j\neq i} h_j((X_s))\big] \cdot g_i((X_s)) T^i,$$

which is nonzero a polynomial in $K[X_s | s \in S][T]$ that vanishes in $((s), t)$. Thus $S \cup \{t\}$ is algebraically dependent over $K(S)$ for every $t \in L$, i.e. S is a maximal algebraically independent set. $\square$

Theorem 5.2.2. *Let L/K be a field extension and $T_0 \subset T_1 \subset L$ subsets such that T_0 is algebraically independent over K and such that $L/K(T_1)$ is algebraic. Then there exists a transcendence basis S of L/K with $T_0 \subset S \subset T_1$.*

Proof. Let $\mathcal{S}$ be the poset of algebraically independent sets $T \subset T_1$ with $T_0 \subset T$, ordered by inclusion. Since every chain

$$T_0' \subset T_1' \subset \cdots$$

of elements in $\mathcal{S}$ has $T' = \bigcup_{i\geqslant 0} T_i'$ as an upper bound, Zorn's Lemma implies that $\mathcal{S}$ contains a maximal element S.

Claim: $L/K(S)$ is algebraic.

We know that $L/K(T_1)$ is algebraic and by the maximality of S, every $t \in T_1 - S$ is algebraic over $K(S)$.

Let $\mathcal{S}'$ be the poset of all $T \subset T_1 - S$ such that $K(S)(T)$ is algebraic over $K(S)$ Since every chain

$$T_0' \subset T_1' \subset \cdots$$

of elements in $\mathcal{S}'$ has $T' = \bigcup_{i\geqslant 0} T_i'$ as an upper bound, Zorn's Lemma implies that there is a maximal $T \in T_1 - S$ such that $K(S)(T)$ is algebraic over $K(S)$.

If T is not equal to all of $T_1 - S$, then there exists an $t \in T_1 - (S \cup T)$ such that $K(S \cup T \cup \{t\})$ is algebraic over $K(S \cup T)$. By the transitivity of algebraic extensions, $K(S \cup T \cup \{t\})$ is algebraic over $K(S)$, which is a contradiction to the maximality of T.

Thus $T = T_1 - S$, i.e. $K(T_1)$ is algebraic over $K(S)$. By transitivity, L is algebraic over $K(S)$. ♦

By Lemma 5.2.1, S is a transcendental basis for L/K. □

Lemma 5.2.3. *Let L/K be a field extension with transcendence basis S. Let $t \in L$ be transcendental over K. Then there is an $s \in S$ such that $(S - \{s\}) \cup \{t\}$ is a transcendence basis for L/K.*

Proof. Since t is algebraic over $K(S)$, there is a nonzero polynomial $f \in K(S)[T]$ such that $f(t) = 0$. After clearing denominators, we can assume that $f \in K[S][T]$. Moreover, we can assume that f is irreducible in $K[S][T]$.

Since t is transcendental, $\deg_{X_s} f((X_s), T) \geqslant 1$ for some $s \in S$, i.e.

$$f((X_s),T) \;=\; \tilde{f}((X_{\tilde{s}})_{\tilde{s}\neq s}, T, X_s) = \sum \tilde{g}_j((X_{\tilde{s}})_{\tilde{s}\neq s}, T) X_s^i$$

has positive degree in X_s and $\tilde{g}_j((X_{\tilde{s}}),T) \neq 0$ for some $j \geqslant 1$. Since $f = f((s),T)$ cannot be a divisor of $\tilde{g}_j((\tilde{s}),T)$ in $K(S)[T]$ and f is the minimal polynomial of t over $K(S)$, up to a scalar multiple, we have $\tilde{g}_j((\tilde{s}),t) \neq 0$.

Thus $\tilde{f}((\tilde{s}),t,X_s)$ is not zero in $K(S')[X_s]$ where $S' = (S - \{s\}) \cup \{t\}$, and s is a root of $\tilde{f}$. This shows that s is algebraic over $K(S')$. Thus L is algebraic over $K(S')$.

Since $S - \{s\} \subsetneq S'$ is not a maximal algebraic independent subset of L, Theorem 5.2.2 implies that S' is a transcendence basis for L/K. □

Theorem 5.2.4. *Let L/K be a field extension. Then any two transcendence bases for L/K have the same cardinality.*

Proof. Let S and T be two transcendence bases for L/K. Let $\mathcal{S}$ be the set of all bijections $\alpha : S' \to T'$ between subsets $S' \subset S$ and $T' \subset T$ such that $S^{S'}_{T'} = (S - S') \cup T'$ is a transcendence basis for L/K. These partially order $\mathcal{S}$ by the rule that $\alpha_1 \leqslant \alpha_2$ for bijections $\alpha_i : S'_i \to T'_i$ if $S'_1 \subset S'_2$ and $T'_1 \subset T'_2$, and if α_1 is the restriction of α_2 to S'_1, i.e.

$$\begin{array}{ccc} S'_1 & \xrightarrow{\alpha_1} & T'_1 \\ \downarrow & & \downarrow \\ S'_2 & \xrightarrow{\alpha_2} & T'_2 \end{array}$$

commutes. Then every chain $\alpha_1 \leqslant \alpha_2 \leqslant \cdots$ is bounded by $\alpha : \bigcup_{i\geqslant} S'_i \to \bigcup_{i\geqslant 0} T'_i$ where $\alpha|_{S'_i} = \alpha_i$. By Zorn's lemma $\mathcal{S}$ has a maximal element $\alpha : S' \to T'$.

Claim: $T' = T$.

If this is not the case, then there is a $t \in T - T'$. By Lemma 5.2.3, there is an $s \in S^{S'}_{T'}$ such that $S^{S' \cup \{s\}}_{T' \cup \{t\}} = (S^{S'}_{T'} - \{s\}) \cup \{t\}$ is a transcendence basis of L/K. Note that since $T' \cup \{t\}$ is algebraically independent over K, $s \notin T' \subset S^{S'}_{T'}$, but $s \in S - S'$.

Thus we extend $\alpha : S' \to T'$ to a bijection $\alpha' : S' \cup \{s\} \to T' \cup \{t\}$ with $\alpha'(s) = t$ that is an element of $\mathcal{S}$. But this contradicts the maximality of α. ♦

To conclude the proof, note that if $T' = T$, then $S_T^{S'} = (S - S') \cup T$ is a transcendence basis for L/K that contains T, which is only possible if $S' = S$. Thus the bijection $\alpha : S \to T$ verifies that S and T have the same cardinality. □

Definition. Let L/K be a field extension. The **transcendence degree of** L/K is the cardinality of a transcendence basis of L/K. The extension L/K is **purely transcendental** if $L = K(S)$ for some transcendence basis S for L/K.

Note that L is a rational function field over K if and only if $L = K(S)$ for a finite transcendence basis S for L/K.

Example. (1) The rational function field

$$K(T) \ = \ \left\{ \tfrac{f}{g} \,\middle|\, f, g \in K[T],\, g \neq 0 \right\}$$

is of transcendence degree 1 over K.

(2) The field extension

$$L \ = \ \operatorname{Frac}\bigl(K[x,y]/(y^2 - x^3 - x)\bigr)$$

is not a rational function field if $\operatorname{char} K \neq 2$ (note that this is not an elementary fact). But $L/K(x)$ is an algebraic extension of degree 2. Thus the transcendence degree of L/K is equal to that of $K(x)/K$, which is 1.

5.3 Exercises

Exercise 5.1. Consider the purely transcendental extension $K = \mathbb{F}_3(x)/\mathbb{F}_3$ of transcendence degree 1, and let $\overline{K}$ be an algebraic closure of K. Let $a \in \overline{K}$ be a root of $f = T^3 - x$ and $b \in \overline{K}$ a root of $g = T^2 - 2$. Find the separable closure E of K in $K(a,b)$. What are the degrees $[K(a,b) : E]$ and $[E : K]$? What are the corresponding separable degrees and inseparable degrees?

Exercise 5.2. Let $\mathbb{F}_p[x,y]$ be the polynomial ring in two variables x and y and $\mathbb{F}_p(x,y)$ its fraction field. Let $\sqrt[p]{x}$ be a root of $T^p - x$ and $\sqrt[p]{y}$ be a root of $T^p - y$.

(1) Show that $\mathbb{F}_p(\sqrt[p]{x}, \sqrt[p]{y})$ is a field extension of $\mathbb{F}_p(x,y)$ of degree p^2.

(2) Show that $a^p \in \mathbb{F}_p(x,y)$ for every $a \in \mathbb{F}_p(\sqrt[p]{x}, \sqrt[p]{y})$.

(3) Conclude that the field extension $\mathbb{F}_p(\sqrt[p]{x}, \sqrt[p]{y}) / \mathbb{F}_p(x,y)$ has no primitive element and that it has infinitely many intermediate extensions.

Exercise 5.3. Let $K \subset E \subset L$ be a tower of field extensions. Show that if the transcendence degree of L/K is finite, then it is the sum of the transcendence degrees of L/E and E/K.

5.4 Additional exercises for the exam preparation

Exercise 5.4. Let ζ_n be a primitive n-th root of unity.

(1) Determine its minimal polynomial over $\mathbb{Q}$ and the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ for $n = 1, \dots, 20$.

(2) Calculate $\mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n)$ and $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n)$.

(3) Find all $n \geqslant 0$ such that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is quadratic.

(4) Determine all subfields of $\mathbb{Q}(\zeta_n)$ for your 5 favorite values of n.

Exercise 5.5. Let K be $\mathbb{Q}$, $\mathbb{F}_3$ or $\mathbb{F}_5$, $n = 3$ or 4 and $a = 1$, 2 or 3. Consider the polynomial $f = T^n - a$ in $K[T]$ and its splitting field L over K.

(1) Is L/K separable? If so, calculate $\mathrm{Gal}(L/K)$.

(*Remark:* Notice the different outcomes for $\mathrm{Gal}(L/K)$ if K or a varies.)

(2) Determine all intermediate fields E of L/K and find primitive elements for E/K.

(3) Which of the subextensions F/E (with $K \subset E \subset F \subset L$) are separable, normal, cyclic, cyclotomic, abelian, solvable, Kummer, Artin-Schreier or radical?

Exercise 5.6. Which of the following elements are constructible over $\mathbb{Q}$?

(1) $\sqrt{3}$, $\sqrt{-3}$, $\sqrt{6}$, $\sqrt{2}+\sqrt{3}$, $\sqrt[3]{3}$, $\sqrt[4]{3}$.

(2) ζ_n for $n = 1, \dots, 20$.

(3) $1+\zeta_4$, $\zeta_3+\zeta_6$, $\zeta_3+\zeta_9$, $\zeta_6+\zeta_6^{-1}$, $\zeta_9+\zeta_9^{-1}$, $\zeta_9+\zeta_9^4+\zeta_9^7$, $\zeta_7+\zeta_7^{-1}$, $\zeta_7+\zeta_7^2+\zeta_7^4$.

Let a be any of the above elements and L the normal closure of $\mathbb{Q}(a)/\mathbb{Q}$. Calculate $N_{L/\mathbb{Q}}(a)$ and $\mathrm{Tr}_{L/\mathbb{Q}}(a)$.

Exercise 5.7. Give three examples and three non-examples for the following types of extensions: algebraic, transzendental, separable, purely inseparable, normal, Galois, cyclic, cyclotomic, abelian, solvable, Kummer, Artin-Schreier, simple radical and radical.

Exercise 5.8. Find normal bases for the following extensions: $\mathbb{Q}(\zeta_3)/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{F}_4/\mathbb{F}_2$ and $\mathbb{F}_8/\mathbb{F}_2$.

Exercise 5.9. Solve all exercises of Chapters V and VI of Lang's "Algebra".