GALOIS THEORY

MARIUS VAN DER PUT & JAAP TOP

Contents

1. Basic definitions

We recall some basic definitions and properties of fields. A field K has a smallest subfield, called the prime field of K. This prime field is either $\mathbb{Q}$, in which case the characteristic of K is 0, or $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for some prime number p, in which case the characteristic of K is p.

Let $K \subset L$ be an extension of fields. Then L can be seen as a vector space over K. The dimension of this vector space is denoted by $[L : K]$. In general $[L : K]$ is infinite. If $[L : K]$ is finite then L is called a finite extension of K of degree $[L : K]$.

Let A be a subset of L, then $K(A)$ denotes the smallest subfield of L containing both A and K. Similarly, $K[A]$ denotes the smallest subring of L containing A and K. For $A = \{a_1, \ldots, a_s\}$ one writes $K(A) = K(a_1, \ldots, a_s)$ and $K[A] = K[a_1, \ldots, a_s]$. An element $a \in L$ is called *algebraic over* K if there is a non-zero polynomial $f \in K[x]$ with $f(a) = 0$. For algebraic a there is a polynomial $F \neq 0$ of minimal degree such that $F(a) = 0$. If F is normalized to be monic, then F is unique and is called the minimal polynomial of a over K. Let F have degree n, then $K(a) = K[a] \cong K[x]/(F)$ is a vector space over K with dimension n and with basis $1, a, \ldots, a^{n-1}$.

An element $a \in L$ which is not algebraic over K is called *transcendental* over K. The obvious ring homomorphism $K[x] \to K[a]$ (i.e.,

Date: August 2001 (some corrections November 2016).

$\sum c_i x^i \mapsto \sum c_i a^i$) is an isomorphism. Thus $K[a]$ is not a field. The field of fractions $K(a)$ of $K[a]$ is in this case isomorphic to $K(x)$, i.e., to the field of rational functions over K.

The field extension $K \subset L$ is called finitely generated if there are elements $a_1, \ldots, a_s \in L$ such that $L = K(a_1, \ldots, a_s)$. The elements $a_1, \ldots, a_s$ are called *algebraically dependent over* K if there is a non-zero polynomial $f \in K[x_1, \ldots, x_s]$ with $f(a_1, \ldots, a_s) = 0$. If such a polynomial f does not exists, then $a_1, \ldots, a_s$ are called *algebraically independent over* K. In the latter case, the obvious homomorphism $K[x_1, \ldots, x_s] \to K[a_1, \ldots, a_s]$ is an isomorphism.Then $K \subset L$ is called a *purely transcendental extension of* K *of transcendence degree* s and L is isomorphic to the field of fractions of the polynomial ring $K[x_1, \ldots, x_s]$. This field of fractions is denoted by $K(x_1, \ldots, x_s)$. It is an exercise (see Exercise 3 below) to show that a finitely generated extension L of K has an intermediate field M (i.e., $K \subset M \subset L$) such that $K \subset M$ is purely transcendental and $M \subset L$ is a finite extension. The *transcendence degree of* L *over* K is defined as the transcendence degree of M over K. It is not at all clear that this definition is a valid one. One has to show that it does not depend on the choice of the intermediate purely transcendental extension. This is, for instance, Theorem 25 in Chapter II of the book *Commutative Algebra* (Vol. 1) by O. Zariski and P. Samuel. A different proof which uses theory of "derivations" and which is valid only in characteristic zero, is to compute the dimension of the M-vector space consisting of all K-linear maps $D : M \to M$ which satisfy $D(m_1 m_2) = m_1 D(m_2) + m_2 D(m_1)$.

1.1. **Exercises.**

(1) Let $K \subset L$ be fields and $a \in L$. Show that $K[a]$ is a field if and only if a is algebraic over K.

(2) Let $K \subset L$ be fields and $S \subset L$ a non-empty *finite* subset. Show that $K[S]$ is a field if and only if every element of S is algebraic over K.
Find a counterexample with $S = L$ to show that the condition that S is finite cannot be missed.

(3) Let $K \subset L$ be a finitely generated field extension. Prove the existence of an intermediate field M such that $K \subset M$ is purely transcendental (or $K = M$) and $[L : M] < \infty$.

2. Solving polynomial equations

Let $f \in K[x]$ be a non-constant polynomial. In general, f does not split as a product of linear factors in $K[x]$ because K does not always contain all the solutions of $f(a) = 0$. We would like to "find" or to

"construct" a larger field which contains all the roots of f. This is formalized in the next definition.

Definition 2.1. *A* splitting field *L of f over K is a field extension such that:*
(a) f splits in $L[x]$ as a product of linear factors.
(b) Let $a_1, \ldots, a_s$ denote the zeros of f in L, then $L = K(a_1, \ldots, a_s)$.

Proposition 2.2.
(1) *A splitting field exists.*
(2) *Let L_1, L_2 be two splitting fields for f over K. Then there exists a K-linear isomorphism of the fields L_1, L_2.*

Proof. (1) One uses induction with respect to the degree of f. Take a (monic) irreducible factor g (in $K[x]$) of f. Then $K_1 := K[y]/(g(y))$ contains a zero, say α of g. Thus f factors in $K_1[x]$ as $(x-\alpha)h$. By induction, a splitting field L for h over K_1 exists. It is easily seen that L is also a splitting field for f over K. We note, in passing, that $[L : K] < \infty$.
(2) We will make a proof of a somewhat more general statement:
Two fields K_1 and K_2 and an isomorphism $\phi_0 : K_1 \to K_2$ are given. Extend ϕ_0 to a ring isomorphism $K_1[x] \to K_2[x]$ by $\phi_0(\sum a_i x^i) = \sum \phi_0(a_i) x^i$. Suppose $f_1 \in K_1[x]$ and $f_2 \in K_2[x]$ satisfy $\phi_0(f_1) = f_2$. Let L_1, L_2 denote two splitting fields for f_1 and f_2 over K_1 and K_2, respectively. Then ϕ_0 extends to an isomorphism between the field L_1 and L_2.

We will construct the desired isomorphism $\phi : L_1 \to L_2$ step by step. The lowest level, $\phi_0 : K_1 \to K_2$ is given. Consider an irreducible factor g of f_1 and a zero $\alpha \in L_1$ of g. Then $\phi_0(g)$ is an irreducible factor of $\phi_0(f_1) = f_2$. Hence $\phi_0(g)$ splits completely over L_2. Choose a β in L_2 with $\phi_0(g)(\beta) = 0$. Define $\phi_1 : K_1(\alpha) \to K_2(\beta)$ by the formula $\sum_{i=0}^{n-1} a_i \alpha^i \mapsto \sum_{i=0}^{n-1} \phi_0(a_i)\beta^i$, where all $a_i \in K_1$ and where n is the degree of g. It is easily verified that ϕ_1 is indeed an isomorphism of fields. Now replace K_1, K_2, f_1, f_2 by $K_1(\alpha), K_2(\beta), f_1/(X-\alpha), f_2/(X-\beta)$. The fields L_1, L_2 are splitting fields over $K_1(\alpha)$ and $K_2(\beta)$ for the polynomials $f_1/(X-\alpha)$ and $f_2/(X-\beta)$. Induction finishes the proof. □

A polynomial $f \in K[x] \setminus K$ is called *separable* if the roots of f in any field extension L of K are distinct. It follows from Proposition 2.2 that it suffices to verify this for a splitting field L of f over K.

Corollary 2.3. *Let $L \supset K$ be the splitting field of a separable polynomial $f \in K[x] \setminus K$. Then the number of K-linear automorphisms of the field L is equal to $[L : K]$.*

Proof. In the situation given in the proof of part (2) of Proposition 2.2, we compute the dimensions and count the number of choices for extensions. We work again in the more general situation. Suppose

$\phi_0 : K_1 \to K_2$ is given. The polynomials f_1 and f_2 are by assumption separable. Thus g and $\phi_0(g)$ are separable. It is obvious that $\phi_1 : K_1(\alpha) \to L_2$ should map α to a root β of $\phi_0(g)$. The number of possibilities for β is the degree of $\phi_0(g)$ (which equals the degree of g). Thus for ϕ_1 there are $\deg(g)$ possibilities. One has $[L_1 : K_1] = [L_1 : K_1(\alpha)][K_1(\alpha) : K_1]$. By induction the number of extensions $L_1 \to L_2$ of a given ϕ_1 is equal to $[L_1 : K_1(\alpha)]$. This completes the proof. □

2.1. **Exercises.**

(1) Prove that $f \in K[x] \setminus K$ is separable if and only if f and its derivative $f' = \frac{d}{dx} f$ are relatively prime.

(2) Let L be a splitting field of f over K. Let n be the degree of f. Prove that $[L : K] \leq n!$. Try to make examples with $K = \mathbb{Q}$ and f of degree 3 with $[L : \mathbb{Q}] = 6$.

(3) Let L be the splitting field over $\mathbb{Q}$ of the polynomial $x^3 - 3$. Produce an explicit splitting field $L \subset \mathbb{C}$ and find the ($\mathbb{Q}$-linear) field automorphisms of L.

(4) The same question for the polynomial $x^8 - 1$ over $\mathbb{Q}$.

3. Galois extensions and examples

For our purposes a pleasant definition of a *Galois extension* $K \subset L$ is:

Definition 3.1. *$L \supset K$ is called a Galois extension of K if L is a splitting field of a separable polynomial f over K.*

Definition 3.2. *The* Galois group $\mathrm{Gal}(L/K)$ *of the extension $K \subset L$ is the group of all K-linear automorphisms of L.*

Observe that indeed $\mathrm{Gal}(L/K)$ is a group, with composition of automorphisms as group law and the identity automorphism as the unit element .

Lemma 3.3. *Let $K \subset L$ be a Galois extension and suppose that $a \in L$ is invariant under the action of* $\mathrm{Gal}(L/K)$*. Then $a \in K$.*

Proof. From Corollary 2.3 we know that $[L : K] = \#\mathrm{Gal}(L/K)$. Let f be a polynomial in $K[x]$ such that L is its splitting field over K. Observe that L is also the splitting field of f over the field $K(a)$. The assumption that $a \in L$ is invariant implies $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K(a))$. Thus $[L : K] = [L : K(a)]$ and hence $[K(a) : K] = 1$, which means that $a \in K$. □

Corollary 3.4. *Let $K \subset L$ be a Galois extension and $a \in L$. The minimal polynomial F of a over K is separable and all its roots are in L.*

Proof. Let the orbit $\mathrm{Gal}(L/K)a = \{ga|$ for all $g \in \mathrm{Gal}(L/K)\}$ be $\{a_1, \ldots, a_s\}$. Consider the polynomial $G := (x - a_1) \cdots (x - a_s) = x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0$ in $L[x]$. This polynomial is invariant under the action of $Gal(L/K)$ and hence Lemma 3.3 implies that $G \in K[x]$. Clearly F divides G and therefore it has the required properties. □

Proposition 3.5. *Let $K \subset L$ be a finite extension. The following are equivalent:*
(1) *$K \subset L$ is a Galois extension.*
(2) *For every element $a \in L$, the minimal polynomial $F \in K[x]$ of a has the property that all its roots lie in L and are simple.*

Proof. (1)⇒(2) is the statement of Corollary 3.4.
(2)⇒(1). Take elements $a_1, \ldots, a_s \in L$ such that $L = K(a_1, \ldots, a_s)$. Let F_i be the minimal polynomial of a_i over K. We may suppose that $F_1, \ldots, F_t$ are the distinct elements in $\{F_1, \ldots, F_s\}$. Put $F = F_1 \cdots F_t$. Then each F_i is separable and has all its roots in L. Then also F is separable and all its roots are in L. Moreover the set of the roots of F contains $\{a_1, \ldots, a_s\}$. Thus L is the splitting field of F over K. □

In several textbooks on Galois theory, part (2) of the above proposition is used as the definition of a Galois extension. To be more precise: a finite extension L/K is called *normal* if for every $a \in L$ the minimal polynomial F of a over K splits in $L[x]$ as a product of linear factors. The extension is called *separable* if for every $a \in L$, the minimal polynomial F of a over K is separable. The extension is called Galois if it is both normal and separable.

Remark
Let $f \in K[x]$ be a separable polynomial and let $L \supset K$ be a splitting field. The roots of f in L are say $\{a_1, \ldots, a_n\}$. Every $\sigma \in Gal(L/k)$ permutes this set. Thus we find a homomorphism $Gal(L/K) \to S_n$. This homomorphism is injective. Indeed, if $\sigma(a_i) = a_i$ for all i, then σ is the identity since $L = K(a_1, \ldots, a_n)$.

Example 3.6. *The Galois group of the splitting field of $x^4 - 2$ over $\mathbb{Q}$ is in this way isomorphic with the subgroup*

$$\{(1), (2\,4), (1\,2\,3\,4), (1\,2)(3\,4), (1\,3)(2\,4), (1\,3), (1\,4\,3\,2), (1\,4)(2\,3)\}$$

of S_4. Here we have written the roots as $a_k = i^{k-1}\sqrt[4]{2}$ with $k = 1, 2, 3, 4$. A permutation sending k to ℓ corresponds to a field homomorphism sending a_k to a_ℓ.

We now give some more examples and elementary properties.

Example 3.7. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *is not normal.*
This follows using Proposition 3.5. Indeed, the minimal polynomial of $\sqrt[3]{2}$ *over* $\mathbb{Q}$ *is* x^3-2. *One can consider* $\mathbb{Q}(\sqrt[3]{2})$ *as a subfield of* $\mathbb{R}$. *The other two zeros of* x^3-2 *in* $\mathbb{C}$ *are* $\omega\sqrt[3]{2}$ *and* $\omega^2\sqrt[3]{2}$, *where* $\omega = e^{2\pi i/3}$. *They do not lie in* $\mathbb{R}$ *and hence also not in* $\mathbb{Q}(\sqrt[3]{2})$.

Example 3.8. *If* $[L:K]=2$ *and the characteristic of* K *is* $\neq 2$, *then* L/K *is Galois.*
Choose $\alpha \in L \setminus K$. *Its minimal polynomial* F *has the form* $F = x^2+ax+b$. *The polynomial* F *splits in* $L[x]$ *as* $(x-\alpha)(x-\beta)$ *with* $\beta+\alpha = -a$. *If* α *would equal* β, *then one finds the contradiction* $\alpha = -\frac{a}{2} \in K$. *It follows that* L *is the splitting field of the separable polynomial* F *over* K.

Example 3.9. *If the characteristic of* K *is 0, then every finite* L/K *is separable.*
Choose $a \in L$. *Its minimal polynomial* $F \in K[x]$ *is irreducible. The derivative* $F' = \frac{dF}{dx}$ *of* F *is not 0 and thus the g.c.d. of* F *and* F' *is 1. By Exercise 1 of Section 2, one has that* F *is separable.*

Example 3.10. *A field* K *of characteristic* $p>0$ *is called* perfect *if every element of* K *is a pth power. Every finite extension* L/K *of a perfect field is separable.*
Choose $a \in L$ *with minimal polynomial* $F \in K[x]$. *If* F *is not separable then the g.c.d. of* F *and* F' *is not 1. Since* F *is irreducible this implies that* $F'=0$. *Thus* F *contains only pthe powers of* x, *i.e.,* $F = \sum a_n x^{pn}$ *with* $a_n \in K$. *Each* a_n *is written as* b_n^p *with* $b_n \in K$. *Then* $F = (\sum b_n x^n)^p$, *which contradicts the fact that* F *is irreducible.*

Example 3.11. *Every finite field is perfect. The field* $\mathbb{F}_p(t)$ *is not perfect.*
The finite fields of characteristic p *are the* $\mathbb{F}_q$ *with* q *a power of* p. *The "Frobenius map"* $Fr : z \mapsto z^p$ *on any field of characteristic* $p>0$ *is a homomorphism of the additive group. The kernel is 0 since* $z^p=0$ *implies* $z=0$. *By counting, one sees that* $Fr : \mathbb{F}_q \to \mathbb{F}_q$ *is bijective. And* $Fr : \mathbb{F}_p(t) \to \mathbb{F}_p(t)$ *is not surjective since* t *is not in the image.*

Example 3.12. *Put* $K = \mathbb{F}_p(t)$ *and let* $F = x^p - t$. *The splitting field of* F *is not separable over* K.
Indeed, the derivative of F *is 0. We note that the splitting field in question can be identified with* $\mathbb{F}_p(x)$.

3.1. **Exercises.**

(1) Show that a finite extension of a finite field is Galois.

(2) Show that $\mathbb{F}_{p^n}$ is the splitting field of the polynomial $x^{p^n}-x$ over $\mathbb{F}_p$. Prove that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and that its Galois group is $\{1, Fr, \ldots, Fr^{n-1}\}$, where Fr is the Frobenius map on $\mathbb{F}_{p^n}$

defined by $Fr(z) = z^p$.

(3) Show that $\mathbb{Q}(\sqrt[4]{3}, i)$ is a Galois extension of $\mathbb{Q}(i)$ and compute the corresponding Galois group.

(4) Determine the Galois group of $x^{12} - 2$ over $\mathbb{Q}$.

(5) Take $q = p^n$ for some prime p, and let $K \supset \mathbb{F}_q$ and $a \in K$, with the property that the polynomial $X^q - X + a$ does not split completely in $K[X]$. Let α be a zero of this polynomial in some splitting field.
   (a) Show that $K(\alpha) \neq K$.
   (b) Show that the extension $K(\alpha) \supset K$ is Galois.
   (c) Show that every $\sigma \in \mathrm{Gal}(K(\alpha)/K)$ satisfies $\sigma(\alpha) = \alpha + t$ for some $t \in \mathbb{F}_q$.
   (d) Show that $\sigma \mapsto \sigma(\alpha) - \alpha$ defines an injective homomorphism of groups: $\mathrm{Gal}(K(\alpha)/K) \to (\mathbb{F}_q, +, 0)$.
   (e) In the special case that K is itself a finite field, observe that the Galois group of a finite extension of finite fields is cyclic, and deduce that $X^q - X + a$ factors as a product of q/p distinct irreducible polynomials of degree p in $K[X]$.
   (f) Take $K = \mathbb{F}_q(t)$ and $X^q - X + t$. Explain why this polynomial is irreducible in $K[X]$, and determine the Galois group of its splitting field over K.

4. Cyclotomic fields

Let $n \geq 1$ be an integer and write $\zeta = \zeta_n = e^{2\pi i/n} \in \mathbb{C}$. The subfield $\mathbb{Q}(\zeta) \subset \mathbb{C}$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$, since all the roots of $x^n - 1$ are $\zeta^k,\ k = 0, 1, \ldots, n-1$. For $n \geq 3$, one calls $\mathbb{Q}(\zeta)$ *the nth cyclotomic field*. The minimal polynomial Φ_n of ζ over $\mathbb{Q}$ is called *the nth cyclotomic polynomial*. An explicit general formula for Φ_n is not available. Still we will need some information on $\Phi_n$in order to calculate the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$. Two tools from standard courses in algebra that we will use are:
(1) **Lemma of Gauss**: Let $f \in \mathbb{Z}[x]$ be monic and let $g, h \in \mathbb{Q}[x]$ be likewise. Then $f = gh$ implies that $g, h \in \mathbb{Z}[x]$.
(2) **Eisenstein's criterion**: Let $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ be such that all its coeffcients, with the exception of a_n, are divisible by a prime number p and p^2 does not divide a_0. Then f is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.
The proof of both statements uses "reduction modulo p, i.e., the ring homomorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$, given by $f = \sum a_n x^n \mapsto \bar{f} := \sum \bar{a}_n x^n$, where for $a \in \mathbb{Z}$ one has written $\bar{a}$ for its image in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Reduction modulo p will also be used in the proof of the next proposition, as well as the identity $\bar{f}(x^p) = \bar{f}^p$ for $\bar{f} \in \mathbb{F}_p[x]$.

Proposition 4.1.
(1) $\Phi_n \in \mathbb{Z}[x]$.
(2) *For a prime number p one has*

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

(3) *For any integer $n \geq 1$ one has*

$$\Phi_n = \prod_{1 \leq j < n,\ g.c.d.(j,n)=1} (x - \zeta_n^j).$$

In particular, the degree of Φ_n is $\phi(n)$, where ϕ is Euler's phi-function defined by $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. (1) follows from the Lemma of Gauss applied to $f = X^n - 1$ and $g = \Phi_n$.
(2) follows from (3), however, we will give here a direct proof as well. Write $f(x) = x^{p-1} + \ldots + x + 1$ and make the substitution $x = 1 + t$. Then

$$f(1+t) = \frac{(1+t)^p - 1}{(1+t) - 1} = \sum_{i=1}^{p} \binom{p}{i} t^{i-1}$$

satisfies Eisenstein's criterion and is therefore irreducible. It follows that f itself is irreducible, and since $f = (x^p - 1)/(x - 1)$, the number ζ_p is a zero of f. Hence $f = \Phi_p$ which is what we wanted to prove.
(3) $x^n - 1 = \prod_{1 \leq j \leq n} (x - \zeta^j)$ and Φ_n can only contain the factors $(x - \zeta^j)$ with $\gcd(j, n) = 1$. Indeed, $\gcd(j, n) = d > 1$ implies that ζ^j is a root of $x^{n/d} - 1$. From $\Phi_n(\zeta^j) = 0$ it would follow that Φ_n divides $x^{n/d} - 1$ which leads to the contradiction $\zeta^{n/d} = 1$.

In order to see that every $x - \zeta^j$ with $\gcd(j, n) = 1$ is a factor of Φ_n, we use a trick. Decompose j as a product $p_1 \cdots p_t$ of (not necessarily distinct) prime factors. The p_i do not divide n since $\gcd(j, n) = 1$. Write $\zeta^j = (\cdots((\zeta^{p_1})^{p_2})\cdots)^{p_t}$. We claim that the following statement holds:

(*) *if p does not divide n and if $\Phi(\alpha) = 0$, then $\Phi(\alpha^p) = 0$.*

Using this assertion one finds $\Phi_n(\zeta) = 0 \Rightarrow \Phi_n(\zeta^{p_1}) = 0 \Rightarrow \Phi_n(\zeta^{p_1 p_2}) = 0 \Rightarrow \cdots \Rightarrow \Phi_n(\zeta^j) = 0$.

We will prove (*) by deriving a contradiction from the assumptions: $p \not| n,\ \Phi_n(\alpha) = 0,\ \Phi_n(\alpha^p) \neq 0$.

The equality $x^n - 1 = \Phi_n \cdot f$ with $f(\alpha^p) = 0$ is clear. Now $f(\alpha^p) = 0$ means that α is a zero of $f(x^p)$. Therefore Φ_n divides $f(x^p)$. According to the Lemma of Gauss, this division takes place in the ring $\mathbb{Z}[x]$. Hence $\Phi_n(x^p)\Phi_n(x)$ divides $x^{pn} - 1$ in the ring $\mathbb{Z}[x]$. After reduction modulo p, one finds that $\bar{\Phi}_n^{p+1}$ divides $x^{pn} - 1 = (x^n - 1)^p$ in $\mathbb{F}_p[x]$. However $p \not| n$ and $x^n - 1$ has only simple roots. The multiplicity of any root of $(x^n - 1)^p$ is p and this is the contradiction that we wanted to find. $\square$

The proof of the following corollary is left to the reader.

Corollary 4.2. *The Galois group* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *is isomorphic to the group* $(\mathbb{Z}/n\mathbb{Z})^*$.
This isomorphism identifies the unit $a \bmod n$ *with the field automorphism sending* ζ_n *to* ζ_n^a.

Proposition 4.3 (Formulas for Φ_n)**.** *1.* $x^n - 1 = \prod_{d|n} \Phi_d$ *(i.e., the product over all divisors* d *of* n*).*
2. $\Phi_n = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$*, where* μ *is the Möbius function given by* $\mu(1) = 1$*,* $\mu(n) = 0$ *if* n *contains a square* $\neq 1$*and* $\mu(p_1 \cdots p_t) = (-1)^t$ *if* $p_1, \ldots, p_t$ *are distinct primes.*
3. $\Phi_{np}(x) = \Phi_n(x^p)$ *if the prime* p *does not divide* n*.*
4. $\Phi_{np}(x) = \Phi_n(x^p)\Phi_n(x)^{-1}$ *if the prime* p *divides* n*.*

Proof. (1) can be proved by induction and the knowledge of the degree of Φ_n.
(2) is a special case of the "Möbius inversion". This is the statement

$$\textit{If for all } n \geq 1 \textit{ the formula } f_n = \prod_{d|n} g_d \textit{ holds, then}$$

$$g_n = \prod_{d|n} f_d^{\mu(n/d)} \textit{holds for all } n \geq 1.$$

In the proof of this inversion formula one uses the easily deduced formulas $\sum_{d|n} \mu(d) = 0$ for $n > 1$ and $\sum_{d|n} \mu(d) = 1$ for $n = 1$.
The proofs of 3. and 4. are left as an exercise. □

4.1. **Exercises.**

(1) Give a proof of Corollary 4.2.

(2) Prove parts (3) and (4) of Proposition 4.3.

(3) Let $\lambda \in \mathbb{Q}$. Prove that $\cos(2\pi\lambda)$ is algebraic over $\mathbb{Q}$. Prove that $\mathbb{Q}(\cos(2\pi\lambda))$ is a Galois extension. Determine its Galois group.

(4) Determine Φ_{72} in a handy way.

5. Galois correspondence and primitive elements

Let a Galois extension L/K with Galois group G be given. One considers two sets, $\mathcal{M}$, the set of the intermediate fields, i.e., the fields M with $K \subset M \subset L$ and the set $\mathcal{G}$ of the subgroups of G.

There are two maps between those sets, $\alpha : \mathcal{M} \to \mathcal{G}$, defined by $\alpha(M) = Gal(L/M)$ and $\beta : \mathcal{G} \to \mathcal{M}$, defined by $\beta(H) = L^H$, i.e., the subfield of L consisting of the elements which are invariant under the

action of H. It is obvious that the two maps reverse inclusions. What is often called the "main theorem of Galois theory" is

Theorem 5.1 (The Galois correspondence)**.** (1) *α and β are each others inverse.*
(2) *The subgroup $H \in \mathcal{G}$ is normal if and only if $\beta(H)$ is a normal (or Galois) extension of K.*
(3) *Suppose that H is a normal subgroup of G. Then M/K is a Galois extension with Galois group G/H.*

We will first prove a lemma.

Lemma 5.2. *Suppose that the finite extension L/K has the property that there are only finitely many intermediate fields. Then there is an $\alpha \in L$ with $L = K(\alpha)$.*

Proof. For a finite field K the proof is quite easy. L is also a finite field and it is known that the multiplicative group L^* of L is cyclic, i.e., there is an element ξ with $L^* = \{\xi^n | n \in \mathbb{Z}\}$. Clearly $L = K(\xi)$. Suppose now that K is infinite and that $L \neq K$. Let $n \geq 1$ be minimal such that $L = K(a_1, \ldots, a_n)$ for certain elements $a_1, \ldots, a_n$. We have to show that $n = 1$. Suppose $n \geq 2$ and consider for every $\lambda \in K$ the element $b_\lambda := a_1 + \lambda a_2$. The fields $K(b_\lambda)$ are intermediate fields for L/K and thus there are $\lambda_1 \neq \lambda_2$ with $M := K(b_{\lambda_1}) = K(b_{\lambda_2})$. The field M contains $a_1 + \lambda_1 a_2$ and $a_1 + \lambda_2 a_2$. It follows that $M = K(a_1, a_2)$ and that $L = K(b_{\lambda_1}, a_3, \ldots, a_n)$. This contradicts the minimality of n. □

Proof. of Theorem 5.1
(1) $\beta\alpha(M)$ is the field $L^{Gal(L/M)}$. Applying Lemma 3.3 to the Galois extension L/M implies that $L^{Gal(L/M)} = M$. This implies that α is injective. Since $\mathcal{G}$ is finite, also $\mathcal{M}$ is finite. Take $H \in \mathcal{G}$ and put $M = \beta(H) = L^H$. Clearly $H \subset \alpha\beta(H)$. We have to prove equality. According to Lemma 5.2 one can write $L = M(a)$ for some $a \in L$. Consider the polynomial $G = \prod_{\sigma \in H}(x - \sigma(a)) \in L[x]$. This polynomial is invariant under the action of H. Therefore its coefficients are also invariant under H and belong to M. Then $G \in M[x]$ and the minimal polynomial of a over M divides G. Thus $[L : M] \leq \#H$ and $\#Gal(L/M) \leq \#H$. Since H is a subgroup of $Gal(L/M)$ one finds the required equality $H = Gal(L/M)$.
(2) The subgroup H corresponds to $M = \beta(H) = L^H$. For a $\sigma \in G$ one has $\beta(\sigma H \sigma^{-1}) = \sigma(M)$. Thus H is normal if and only if $\sigma(M) = M$ for all $\sigma \in G$. Using that L/K is normal and separable, one finds that the latter property of M is equivalent with M/K normal (or also Galois).
(3) H is supposed to be normal and thus $M := \beta(H) = L^H$ satisfies $\sigma(M) = M$ for all $\sigma \in G$. Thus one can define a restriction map $Gal(L/K) \to Gal(M/K)$. The kernel of this homomorphism is H. The map is surjective since $\#(G/H)$ is equal to $[M : K]$. □

Corollary 5.3 (The theorem of the primitive element)**.** *For every finite separable extension L/K there is a cyclic element, i.e., an element $a \in L$ with $L = K(a)$.*

Proof. According to Lemma 5.2, it suffices to show that there are finitely many intermediate fields for L/K. If we can show that L lies in the splitting field $\tilde{L}$ of a separable polynomial, then there are only finitely many intermediate fields for $\tilde{L}/K$ and then also for L/K. Let L/K be generated by elements $a_1, \ldots, a_s$. The minimal polynomial of a_i over K is denoted by F_i. We may suppose that $F_1, \ldots, F_t$ are the distinct minimal polynomials, then $F := F_1 \cdots F_t$ is separable and every a_i is a zero of F. The splitting field $\tilde{L}$ of F contains L and we are done. □

5.1. **Exercises.**

(1) Prove that $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ is a Galois extension of $\mathbb{Q}$. Determine the Galois group, all intermediate subfields and a primitive element.

(2) The same questions for $\mathbb{Q}(e^{2\pi i/3}, \sqrt[3]{3})/\mathbb{Q}$.

(3) Find all subfields of $\mathbb{Q}(\sqrt[4]{2}, i)$ and a primitive element for each of them. Which of these fields are normal over $\mathbb{Q}$?

(4) One of the theorems in the Ph.D. thesis of Amol Sasane (Groningen, 2001, advisor Prof. R. Curtain) states that $\tan(\pi/2001) \notin \mathbb{Q}$. Prove this theorem.

(5) (a) Write $\tan(\pi/n)$ in terms of the primitive $4n$th roots of unity $\zeta = exp(2\pi i/4n)$.
(b) Determine the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/4n\mathbb{Z})^*$ that fix $\tan(\pi/n)$.
(c) Find the degree of $\mathbb{Q}(\tan(\pi/n))$ over $\mathbb{Q}$.
(d) What are the (positive) integers $n \neq 0$ for which $\tan(\pi/n) \in \mathbb{Q}$?

(6) (a) Prove that for an odd prime number p, the field $\mathbb{Q}(\zeta_p)$ has a unique subfield K with $[K : \mathbb{Q}] = 2$.
(b) Find a condition on p such that $K \subset \mathbb{R}$.
Hint: complex conjugation is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. The question whether or not K is a real field is the same as the question whether complex conjugation is an element of the subgroup $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$.
(c) Write $\varepsilon(n) := 1$ if $n \bmod p$ is a square in $\mathbb{F}_p^*$ and $\varepsilon(n) := -1$ otherwise. Show that $K/\mathbb{Q}$ is generated by the element $\sum_{n=1}^{p-1} \varepsilon(n)\zeta_p^n$.

(7) Prove that the regular 7-gon cannot be constructed by ruler and compass. Explanation: The admissible operations with ruler and compass are: drawing a line through two points, drawing a circle with given center and radius, intersecting two lines, interseting a line with a circle and intersecting two circles. Hint: Identify the plane with $\mathbb{C}$. The points $\mathbb{Q} \subset \mathbb{C}$ are given. Prove that every "constructable" point $a \in \mathbb{C}$ gives rise to a "tower of fields" $K_n := \mathbb{Q}(a) \supset K_{n-1} \supset \cdots \supset K_0 = \mathbb{Q}$ with $[K_{i+1} : K_i] = 2$ for every i.

(8) *Cyclic extensions.*
Let K be a field and $n > 1$ an integer. Suppose that the characteristic of K is 0 or p with $p \not| n$ and that K contains all the n^{th} roots of unity. In this exercise we want to prove the following statement:
$E \supset K$ is a Galois extension with a cyclic Galois group of order n if and only if $E = K(\alpha)$ where α is a root of an irreducible polynomial $x^n - a \in K[x]$.
(a) Let $f(x) = x^n - a \in K[x]$ be an irreducible polynomial. Show that f is separable. Show that the splitting field E of $f(x)$ over K is of the form $K(\alpha)$ with α a root of $f(x) = 0$. Furthermore, show that the Galois group of E over K is generated by the map defined by $\alpha \mapsto \zeta\alpha$ where ζ is a primitive n^{th} root of unity.
(b) Let E be a Galois extension of K with a cyclic Galois group of order n. Let σ generate the Galois group.
(i) One considers σ as a K-linear map on E as vector space over K. Prove that every eigenvalue λ of σ satisfies $\lambda^n = 1$ and thus belongs to K.
(ii) Prove that there is a basis of eigenvectors for σ. (Hint: Jordan normal form).
(iii) Prove that every eigenvalue has multiplicity 1. (Hint: if $\sigma e_i = \lambda e_i$ for $i = 1, 2$ and $e_1 \neq 0 \neq e_2$, then $\sigma(\frac{e_1}{e_2}) = \frac{e_1}{e_2}$).
(iv) Prove that there is an $\alpha \in E$ with $\alpha \neq 0$, $\sigma(\alpha) = \zeta\alpha$ and ζ a primitive n^{th} root of unity.
(v) Show that the $\sigma^i(\alpha)$, $i = 0, \ldots, n-1$, are all distinct and that therefore the minimal polynomial of α over K is $x^n - a$ with $a = \alpha^n \in K$.