Leandro Vendramin

Galois theory

Notes

Monday 20th February, 2023

Preface

The notes correspond to the bachelor course *Galois theory* of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences. The course is divided into thirteen two-hour lectures.

The material is somewhat standard. Basic texts on fields and Galois theory are for example [2] and [3].

As usual, we also mention a set of great expository papers by Keith Conrad, the notes are extremely well-written and useful at every stage of a mathematical career.

Several chapters contain optional paragraphs which give examples of how to apply OSCAR Computer Algebra System to concrete problems in Galois theory.

Thanks go to Wouter Appelmans, Alejandro de la Cueva Merino, Wannes Malfait.

This version was compiled on Monday 20th February, 2023 at 16:35.

Leandro Vendramin
Brussels, Belgium

Contents

List of topics

Lecture 1

§1. Fields

Recall that a **field** is a commutative ring such that $1 \neq 0$ and that every non-zero element is invertible. Examples of (infinite) fields are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. If p is a prime number, then $\mathbb{Z}/p$ is a field.

Example 1.1. The abelian group $\mathbb{Z}/2 \times \mathbb{Z}/2$ is a field with multiplication

$$(a,b)(c,d) = (ac+bd, ad+bc+bd).$$

Example 1.2. $\mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$ and $\mathbb{Q}(\sqrt{2})$ are fields.

$$\begin{tikzcd}[arrows=dash]
\mathbb{C} \arrow[drr] \arrow[dd] & & \\
 & & \mathbb{R} \arrow[d] \\
\mathbb{Q}(i) \arrow[dr] & & \mathbb{Q}(\sqrt{2}) \arrow[dl] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Exercise 1.3. Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are not isomorphic as fields.

If R is a ring, there exists a unique ring homomorphism $\mathbb{Z} \to R$, $m \mapsto m1$. The image $\{m1 : m \in \mathbb{Z}\}$ of this homomorphism is a subring of R and it is known as the **ring of integers** of R. The kernel is a subgroup of $\mathbb{Z}$ and is generated by some $t \geq 0$. The integer t is the **characteristic** of the ring R.

Exercise 1.4. The characteristic of a field is either zero or a prime number.

Recall that a commutative ring R is an **integral domain** if $xy = 0 \implies x = 0$ or $y = 0$. Fields are integral domains.

Exercise 1.5. Let K be a field. Prove that the following statements are equivalent:

1) K is of characteristic zero.
2) The additive order of 1 is infinite.
3) The additive order of each $x \neq 0$ is infinite.
4) The ring of integers of K is isomorphic to $\mathbb{Z}$.

Exercise 1.6. Let K be a field. Prove that the following statements are equivalent:

1) K is of characteristic p.
2) The additive order of 1 is p.
3) The additive order of each $x \neq 0$ is p.
4) The ring of integers of K is isomorphic to $\mathbb{Z}/p$.

Definition 1.7. A **subfield** of a ring R is a subring of R that is also a field.

Note that if K is a subfield of E, then the characteristic of K coincides with the characteristic of E. Moreover, if $K \to L$ is a field homomorphism, then K and L have the same characteristic.

Exercise 1.8. Let K be a field of characteristic p. Prove that $K \to K$, $x \mapsto x^{p^n}$, is a field homomorphism for all $n \in \mathbb{Z}_{\geq 0}$.

Note that finite fields are of characteristic p.

Let K be a subfield of a field E. Then E is a K-vector space with the usual scalar multiplication $K \times E \to E$, $(\lambda, x) \mapsto \lambda x$.

Definition 1.9. A field K is **prime** if there are no proper subfields of K.

Examples of prime fields are $\mathbb{Q}$ and $\mathbb{Z}/p$ for a prime number p.

Proposition 1.10. *Let K be a field. The following statements hold:*

1) *K contains a unique prime field, it is known as the* ***prime subfield*** *of K.*
2) *The prime subfield of K is either isomorphic to $\mathbb{Q}$ if the characteristic of K is zero, or it is isomorphic to $\mathbb{Z}/p$ for some prime number p if the characteristic of K is p.*

Proof. To prove the first claim let L be the intersection of all the subfields of K. Then L is a subfield of K. If F is a subfield of L, then F is a subfield of K. Thus $L \subseteq F$ and hence $F = L$, which proves that L is prime. If L_1 is a subfield of K and L_1 is prime, then $L \subseteq L_1$ and hence $L = L_1$.

Let K_0 be the prime field of K. Suppose that K is of characteristic $p > 0$. Then the ring $K_{\mathbb{Z}}$ of integers of K is a field isomorphic to $\mathbb{Z}/p$ and hence $K_0 \simeq K_{\mathbb{Z}}$. Suppose now that the characteristic of K is zero. Let $E = \{m1/n1 : m, n \in \mathbb{Z}, n \neq 0\}$. We claim that $K_0 = E$. Since $K_{\mathbb{Z}} \subseteq K_0$, it follows that $E \subseteq K_0$. Hence $E = K_0$, as E is a subfield of K. $\square$

Definition 1.11. Let E be a field and K be a subfield of E. Then E is a **field extension** of K. We will use the notation E/K.

If E is an extension of K, then E is a K-vector space.

Definition 1.12. The degree of an extension E of K is the integer $\dim_K E$. It will be denoted by $[E : K]$.

We say that E is a finite extension of K if $[E : K]$ is finite.

Example 1.13. Let K be a field. Then $[K : K] = 1$. Conversely, if E is an extension of K and $[E : K] = 1$, then $K = E$. If not, let $x \in E \setminus K$. We claim that $\{1, x\}$ is linearly independent over K. Indeed, if $a1 + bx = 0$ for some $a, b \in K$, then $bx = -a$. If $b \neq 0$, then $x = -a/b \in K$, a contradiction. If $b = 0$, then $a = 0$.

We know that $[\mathbb{C} : \mathbb{R}] = 2$.

Example 1.14. A basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is given by $\{1, \sqrt{2}\}$. Then $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. The calculations can be easily done by computer:

```
julia> E, a = quadratic_field(2)
(Real quadratic field defined by x^2 - 2, sqrt(2))
julia> characteristic(E)
0
julia> K = prime_field(E)
Rational Field
julia> degree(E)
2
julia> basis(E)
2-element Vector{nf_elem}:
 1
 sqrt(2)
julia> one(K)==one(E)
true
julia> zero(K)==zero(E)
true
```

Example 1.15. Since $\mathbb{Q}$ is numerable and $\mathbb{R}$ is not, $[\mathbb{R} : \mathbb{Q}] > \aleph_0$. If $\{x_i : i \in \mathbb{Z}_{>0}\}$ is a numerable basis of $\mathbb{R}$ over $\mathbb{Q}$, for each n consider the $\mathbb{Q}$-vector space V_n generated by $\{x_1, \dots, x_n\}$. Then

$$\mathbb{R} = \bigcup_{n \geq 1} V_n,$$

is numerable, as each V_n is numerable, a contradiction.

If E is an extension of K and E is finite, then $[E : K]$ is finite.

Proposition 1.16. *Let K be a finite field. Then $|K| = p^m$ for some prime number p and some $m \geq 1$.*

Proof. We know the prime subfield K_0 of K is isomorphic to $\mathbb{Z}/p$. In particular, $|K_0| = p$. Since K is finite, $[K : K_0] = m$ for some m. If $\{x_1, \dots, x_m\}$ is a basis of K over K_0, then each element of K can be written uniquely as $\sum_{i=1}^m a_i x_i$ for some $a_1, \dots, a_m \in K_0$. Then $K \simeq K_0^m$ and hence $|K| = |K_0^m| = p^m$. $\square$

We now perform some basic calculations with a finite field of eight elements:

```
julia> E, x = FiniteField(2, 3, "x")
(Finite field of degree 3 over F_2, x)
julia> characteristic(E)
2
julia> prime_field(E)
Galois field with characteristic 2
julia> degree(E)
3
julia> size(E)
8
julia> [z for z in E]
8-element Vector{fq_nmod}:
 0
 1
 x
 x + 1
 x^2
 x^2 + 1
 x^2 + x
 x^2 + x + 1
```

Definition 1.17. Let E be an extension of K. A **subextension** F/K of E/K is a subfield F of E that contains K, that is $K \subseteq F \subseteq E$.

Definition 1.18. Let E and E_1 be extensions over K. An extension **homomorphism** $E \to E_1$ is a field homomorphism $\sigma\colon E \to E_1$ such that $\sigma(x) = x$ for all $x \in K$.

To describe the homomorphism $\sigma\colon E \to E_1$ of the extensions over K one typically writes the commutative diagram

$$\begin{tikzcd} K \arrow[r, equal] \arrow[d, hook] & K \arrow[d, hook] \\ E \arrow[r, "\sigma"] & E_1 \end{tikzcd}$$

We write $\mathrm{Hom}(E/K, E_1/K)$ to denote the set of homomorphism $E \to E_1$ of extensions of K. Note that if $\sigma \in \mathrm{Hom}(E/K, E_1/K)$, then σ is a K-linear map, as

$$\sigma(\lambda x) = \sigma(\lambda)\sigma(x) = \lambda\sigma(x)$$

for all $\lambda \in K$ and $x \in E$.

Example 1.19. The conjugation map $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$, is an endomorphism of $\mathbb{C}$ as an extension over $\mathbb{R}$. Let $\varphi \in \mathrm{Hom}(\mathbb{C}/\mathbb{R}, \mathbb{C}/\mathbb{R})$. Then

$$\varphi(x+iy) = \varphi(x)+\varphi(i)\varphi(y) = x+\varphi(i)y$$

for all $x, y \in \mathbb{R}$. Since $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$, it follows that $\varphi(i) \in \{-i, i\}$. Thus either $\varphi(x+iy) = x+iy$ or $\varphi(x+iy) = x-iy$.

Exercise 1.20. Prove that if K is a field and $\sigma\colon K \to K$ is a field homomorphism, then $\sigma \in \mathrm{Hom}(K/K_0, K/K_0)$.

If E/K is an extension, then

$$\mathrm{Aut}(E/K) = \{\sigma : \sigma\colon E \to E \text{ is a bijective extension homomorphism}\}$$

is a group with composition.

Definition 1.21. Let E/K be an extension. The **Galois group** of E/K is the group $\mathrm{Aut}(E/K)$ and it will be denoted by $\mathrm{Gal}(E/K)$.

A typical example: $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2$.
As an example, we show with the computer that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \simeq \mathbb{Z}/2$:

```
julia> E, x = quadratic_field(2)
(Real quadratic field defined by x^2 - 2, sqrt(2))
julia> characteristic(E)
0
julia> G, C = galois_group(E);
julia> describe(G)
"C2"
julia> order(G)
2
```

Example 1.22. Let $\theta = \sqrt[3]{2}$ and let $E = \{a+b\theta+c\theta^2 : a, b, c \in \mathbb{Q}\}$. Note that

$$a+b\theta+c\theta^2 = 0 \iff a = b = c = 0.$$

Then E is an extension of $\mathbb{Q}$ such that $[E : \mathbb{Q}] = 3$. We claim that $\mathrm{Gal}(E/\mathbb{Q})$ is trivial. If $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ and $z = a+b\theta+c\theta^2$, then $\sigma(z) = a+b\sigma(\theta)+c\sigma^2(\theta)$. Since $\sigma(\theta)^3 = \sigma(\theta^3) = \sigma(2) = 2$, it follows that $\sigma(\theta) = \theta$ and therefore $\sigma = \mathrm{id}$.

Exercise 1.23. Prove that the polynomial X^3-2 is irreducible in $\mathbb{Q}[X]$.

The previous exercise can easily be solved using computers:

```
julia> R, x = PolynomialRing(QQ, "x");
julia> is_irreducible(x^3-2)
true
```

The following exercise is known as the *Eisenstein's irreducibility criterion*:

Exercise 1.24. Let A be a unique factorization domain and K be its fraction field. Let $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ be a polynomial of degree $n > 0$. Assume that there exists a prime element $p \in A$ such that $p \mid a_i$ for all $i \in \{0, 1, \dots, n-1\}$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible in $K[X]$.

Exercise 1.25. Prove that the polynomials $f = X^{10} + 60X^7 + 82X^6 - 36X^3 + 2$ and $g = 3X^{10} + 15X^2 - 45$ are irreducible in $\mathbb{Z}[X]$.

Exercise 1.26. Is the polynomial $f = 3(X^{10} + 5X^2 - 15)$ irreducible in $\mathbb{Z}[X]$?

If E/K is an extension and S is a subset of E, then there exists a unique smallest subextension F/K of E/K such that $S \subseteq F$. In fact,

$$F = \bigcap \{T : T \text{ is a subfield of } E \text{ that contains } K \cup S\}$$

If L/K is a subextension of E/K such that $S \subseteq L$, then $F \subseteq L$ by definition. The extension F is known as the **subextension generated by** S and it will be denoted by $K(S)$. If $S = \{x_1, \dots, x_n\}$ is finite, then $K(S) = K(x_1, \dots, x_n)$ is said to be of **finite type**.

Example 1.27. If $\{e_1, \dots, e_n\}$ is a basis of E over K, then $E = K(e_1, \dots, e_n)$.

Example 1.28. The field $\mathbb{Q}(\sqrt{2})$ is precisely the extension of $\mathbb{R}/\mathbb{Q}$ generated by $\sqrt{2}$.

Let E/K be an extension and S and T be subsets of E. Then

$$K(S \cup T) = K(S)(T) = K(T)(S).$$

If, moreover, $S \subseteq T$, then $K(S) \subseteq K(T)$.

§2. Algebraic extensions

Definition 2.1. Let E/K be an extension. An element $x \in E$ is **algebraic** over K if there exists a non-zero polynomial $f(X) \in K[X]$ such that $f(x) = 0$. If x is not algebraic over K, then it is called **trascendental** over K.

If E/K is an extension, let

$$\overline{K}_E = \{x \in E : x \text{ is algebraic over } K\}.$$

Definition 2.2. An extension E/K is **algebraic** if every $x \in E$ is algebraic over K.

If K is a field, every $x \in K$ is algebraic over K, as x is a root of $X - x \in K[X]$. In particular, K/K is an algebraic extension.

Example 2.3. $\mathbb{C}/\mathbb{R}$ is an algebraic extension. If $z \in \mathbb{C} \setminus \mathbb{R}$, then z is a root of the polynomial $X^2 - (z+\overline{z})X + |z|^2 \in \mathbb{R}[X]$.

If F/K is an algebraic extension $x \in E$ is algebraic over K for some field $E \supseteq F$, then x is algebraic over F.

Example 2.4. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is algebraic, as the number $a+b\sqrt{2}$ is a root of the polynomial $X^2 - 2aX + (a^2 - 2b^2) \in \mathbb{Q}[X]$.

The extension $\mathbb{C}/\mathbb{Q}$ is not algebraic. For example, Hermite proved that e is transcendental over $\mathbb{Q}$; see [3, Therem 24.4]. Lindemann's theorem states that π is not algebraic $\mathbb{Q}$; see [3, Theorem 24.5].

Example 2.5. Let $a = \sqrt{2}$ and $b = \sqrt[3]{3}$. Both a and b are algebraic numbers over $\mathbb{Q}$. Let us show that $a+b$ is also algebraic. Let $f(X) = X^3 - 3 \in \mathbb{Q}[X]$. Then $f(b) = 0$. Note that the polynomial

$$g(X) = f(X-a) = X^3 - 3aX^2 + 3aX - a^3 - 3 \in \mathbb{Q}(a)[X]$$

is such that $g(a+b) = 0$. How can we find a polynomial with coefficients in $\mathbb{Q}$ that vanishes on $a+b$? We do the "conjugation" trick:

$$h(X) = f(X-a)f(X+a) = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1 \in \mathbb{Q}[X].$$

Note that $h(a+b) = 0$. How can you prove that ab is also algebraic over $\mathbb{Q}$?

Lecture 2

If E/K is an extension and $x \in E$ is algebraic over K, then the evaluation homomorphism $K[X] \to E$, $p \mapsto p(x)$, is not injective. In particular, its kernel is a non-zero ideal. Hence it is generated by a monic polynomial f.

Definition 2.6. Let E/K be an extension and $x \in E$ be an algebraic element. The monic polynomial that generates the kernel of $K[X] \to E$, $f \mapsto f(x)$, is known as the **minimal polynomial** of x over K and it will be denoted by $f(x,K)$. The **degree** of x over K is then $\deg f(x,K)$.

Some basic properties of the minimal polynomial of an algebraic element:

Proposition 2.7. *Let E/K be an extension and $x \in E$.*

1) *If $g \in K[X] \setminus \{0\}$ is such that $g(x) = 0$, then $f(x,K)$ divides g. In particular, $\deg f(x,K) \leq \deg g$.*
2) *$f(x,K)$ is irreducible in $K[X]$.*
3) *If F/K is a subextension of E/K, then $f(x,F)$ divides $f(x,K)$.*

Proof. Write $f = f(x,K)$ to denote the minimal polynomial of x. To prove 1) note that $g(x) = 0$ implies that g belongs to the kernel of the evaluation map, so g is a multiple of f. To prove 2) note that if $f = pq$ for some $p,q \in K[X]$ such that $0 < \deg p, \deg q < \deg f$, then $f(x) = 0$ implies that either $p(x) = 0$ or $q(x) = 0$, a contradiction. Finally, we prove 3). Since $f \in K[X] \subseteq F[X]$ and $f(x) = 0$, it follows from 1) that $f(x,F)$ divides f. $\square$

Some easy examples: $f(i,\mathbb{R}) = X^2 + 1$, $f(i,\mathbb{C}) = X - i$ and $f(\sqrt[3]{2},\mathbb{Q}) = X^3 - 2$:

```
julia> E, x = radical_extension(3, QQ(2), "x");
julia> minpoly(x)
x^3 - 2
julia> F, y = quadratic_field(-1);
julia> minpoly(y)
x^2 + 1
```

Example 2.8. Let us compute $f(\sqrt{2}+\sqrt{3},\mathbb{Q})$. Let $\alpha=\sqrt{2}+\sqrt{3}$. Then

$$\begin{aligned}\alpha-\sqrt{2}=\sqrt{3} &\implies (\alpha-\sqrt{2})^2=3 \implies \alpha^2-2\sqrt{2}\alpha+2=3\\ &\implies \alpha^2-1=2\sqrt{2}\alpha \implies (\alpha^2-1)^2=8\alpha^2 \implies \alpha^4-10\alpha^2+1=0.\end{aligned}$$

Thus α is a root of $g=X^4-10X^2+1$. To prove that $g=f(\alpha,\mathbb{Q})$ it is enough to prove that g is irreducible in $\mathbb{Q}[X]$. First note that the roots of g are $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$ and $-\sqrt{2}-\sqrt{3}$. This means that if g is not irreducible, then $g=hh_1$ for some polynomials $h,h_1\in\mathbb{Q}[X]$ such that $\deg h=\deg h_1=2$. This is not possible, as $(\sqrt{2}+\sqrt{3})+(\sqrt{2}-\sqrt{3})=2\sqrt{2}\notin\mathbb{Q}$, $(\sqrt{2}+\sqrt{3})+(-\sqrt{2}+\sqrt{3})=2\sqrt{3}\notin\mathbb{Q}$ and $(\sqrt{2}+\sqrt{3})(-\sqrt{2}-\sqrt{3})=-5-2\sqrt{6}\notin\mathbb{Q}$.

Proposition 2.9. *Let F/K be a subextension and E/K. Then*

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

Proof. Let $\{e_i : i\in I\}$ be a basis of E over F and $\{f_j : j\in J\}$ be a basis of F over K. If $x\in E$, then $x=\sum_i \lambda_i e_i$ (finite sum) for some $\lambda_i\in F$. For each i, $\lambda_i=\sum_j a_{ij}f_j$ (finite sum) for some $a_{ij}\in K$. Then $x=\sum_i\sum_j a_{ij}(f_je_i)$. This means that $\{f_je_i : i\in I, j\in J\}$ generates E as a K-vector space. Let us prove that $\{f_je_i : i\in I, j\in J\}$ is linearly independent. If $\sum_i\sum_j a_{ij}(f_je_i)=0$ (finite sum) for some $a_{ij}\in K$, then

$$\begin{aligned}0=\sum_i\left(\sum_j a_{ij}f_j\right)e_i &\implies \sum_j a_{ij}f_j=0 \text{ for all } i\in I\\ &\implies a_{ij}=0 \text{ for all } i\in I \text{ and } j\in J.\end{aligned}$$ □

We state a lemma:

Lemma 2.10. *If A is a finite-dimensional commutative algebra over K and A is an integral domain, then A is a field.*

Proof. Let $a\in A\setminus\{0\}$. We need to prove that there exists $b\in A$ such that $ab=1$. Let $\theta\colon A\to A$, $x\mapsto ax$. Note that θ is K-linear transformation, as

$$\theta(x+y)=a(x+y)=ax+ay=\theta(x)+\theta(y),\quad \theta(\lambda x)=a(\lambda x)=\lambda(ax)=\lambda\theta(x),$$

for all $x,y\in A$ and $\lambda\in K$. It is injective, since A is an integral domain. Since $\dim_K A<\infty$, it follows that θ is an isomorphism. In particular, $\theta(A)=A$, which implies that there exists $b\in A$ such that $1=ab$. □

Let E/K be an extension and $x\in E$. Then

$$K[x]=\{y=f(x) : \text{ for some } f\in K[X]\}$$

is a subring of E that contains K. Note that $K[x]$ is a K-vector space.

More generally, if $x_1,\dots,x_n\in E$, then

$$K[x_1,\dots,x_n]=\{f(x_1,\dots,x_n): f\in K[X_1,\dots,X_n]\}$$

is a subring of E. Note that $K[x_1,\dots,x_n]$ is a K-vector space. Clearly, $K[x_1,\dots,x_n]$ is a domain and

$$K(x_1,\dots,x_n)=\left\{\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)}: f,g\in K[X_1,\dots,X_m] \text{ with } g(x_1,\dots,x_n)\neq 0\right\}$$

is the extension of K generated by $x_1,\dots,x_n$. Note that

$$K(x_1,\dots,x_n)=(K(x_1,\dots,x_{n-1}))(x_n).$$

The previous construction can be generalized. Let I be a non-empty set. For each $i\in I$, let X_i be a variable. Consider the polynomial ring $K[\{X_i : i\in I\}]$ and let $S=\{x_i : i\in I\}$ be a subset of E. There exists a unique algebras homomorphism $K[\{X_i : i\in I\}]\to E$ such that $X_i\mapsto x_i$ for all $i\in I$. The image is denoted by $K[S]$.

Exercise 2.11. Prove that $\mathbb{Q}[\sqrt{2}]=\mathbb{Q}(\sqrt{2})$.

The exercise is not an accident.

Theorem 2.12. *Let E/K be an extension and $x\in E\setminus K$. The following statements are equivalent:*

1) *x is algebraic over K.*
2) $\dim_K K[x]<\infty$.
3) *$K[x]$ is a field.*
4) $K[x]=K(x)$.

Proof. We first prove 1) $\implies$ 2). Let $z\in K[x]$, say $z=h(x)$ for some $h\in K[X]$. There exists $g\in K[X]$ such that $g\neq 0$ and $g(x)=0$. Divide h by g to obtain polynomials $q,r\in K[X]$ such that $h=gq+r$, where $r=0$ or $\deg r<\deg g$. This implies that

$$z=h(x)=g(x)q(x)+r(x)=r(x).$$

If $\deg g=m$, then $r=\sum_{i=0}^{m-1}a_iX^i$ for some $a_0,\dots,a_{m-1}\in K$. Thus $z=\sum_{i=0}^{m-1}a_ix^i$, so $K[x]\subseteq\langle 1,x,\dots,x^{m-1}\rangle$.

The previous lemma proves that 2) $\implies$ 3).

It is trivial that 3) $\implies$ 4).

It remains to prove that 4) $\implies$ 1). Since $x\neq 0$, $1/x\in K(x)=K[x]$. There exists $a_0,\dots,a_n\in K$ such that $1/x=a_0+a_1x+\cdots+a_nx^n$. Thus

$$a_nx^{n+1}+\cdots+a_1x^2+a_0x-1=0,$$

and hence x is a root of $a_nX^{n+1}+\cdots+a_0X-1\in K[X]\setminus\{0\}$. □

Note that if x is algebraic over K, then $K[x]\simeq K[X]/(f(x,K))$.

Corollary 2.13. *If E/K is finite, then E/K is algebraic.*

Proof. Let $n = [E : K]$ and $x \in E \setminus K$. The set $\{1, x, \dots, x^n\}$ has $n+1$ elements, so it is linearly dependent. There exist $a_0, \dots, a_n \in K$, not all zero, such that

$$a_0 + a_1 x + \cdots + a_n x^n = 0.$$

Thus x is a root of the non-zero polynomial $a_0 + a_1 X + \cdots + a_n X^n \in K[X]$. $\square$

We note that the converse of the previous result does not hold.

Corollary 2.14. *If E/K is an extension and $x_1, \dots, x_n \in E$ are algebraic over K, then $K(x_1, \dots, x_n)/K$ is finite and $K(x_1, \dots, x_m) = K[x_1, \dots, x_n]$.*

Proof. We proceed by induction on n. The case $n = 1$ follows immediately from the theorem. So assume the result holds for some $n \geq 1$. Since the extensions $K(x_1, \dots, x_n)/K(x_1, \dots, x_{n-1})$ and $K(x_1, \dots, x_{n-1})/K$ are both finite, it follows that $K(x_1, \dots, x_n)/K$ is finite. Moreover,

$$\begin{aligned} K(x_1, \dots, x_n) &= K(x_1, \dots, x_{n-1})(x_n) \\ &= K(x_1, \dots, x_{n-1})[x_n] = K[x_1, \dots, x_{n-1}][x_n] = K[x_1, \dots, x_n]. \end{aligned}$$ $\square$

Corollary 2.15. *Let $E = K(S)$ for some set S. Then E/K is algebraic if and only if x is algebraic over K for all $x \in S$.*

Proof. Let us prove the non-trivial implication. Let $z \in K(S)$. In particular, there exists a finite subset $T \subseteq S$ such that $z \in K(T)$. The previous result implies that $K(T)/K$ is algebraic, and hence z is algebraic. $\square$

Corollary 2.16. *If E/K is an extension, then $\overline{K}_E$ is a subfield of E that contains K. Moreover, $K(\overline{K}_E)/K$ is algebraic.*

Proof. By definition, $K(\overline{K}_E)/K$ is algebraic. Thus $K(\overline{K}_E) \subseteq \overline{K}_E$. From this, it follows that $K(\overline{K}_E) = \overline{K}_E$. $\square$

The following exercise is now almost trivial:

Exercise 2.17. Let E/K be an extension of finite type; this means that $E = K(S)$ for some finite set S. Prove that E/K is algebraic if and only if E/K is finite.

Let $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$. Then $\overline{\mathbb{Q}}$ is the field of algebraic numbers. Can you compute $[\overline{\mathbb{Q}} : \mathbb{Q}]$?

Exercise 2.18. Prove that $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

For the previous exercise, you may use Eisenstein's criterion.

Exercise 2.19. Let $E = \mathbb{Q}[i, \sqrt{2}] = \mathbb{Q}[\sqrt{2}][i]$. Prove that $[E : \mathbb{Q}] = 4$.

Exercise 2.20. Let $E = \mathbb{Q}[\sqrt{2}, \sqrt[3]{5}]$.

1) Compute $[E : \mathbb{Q}]$.

2

2) Prove that $E = \mathbb{Q}[\sqrt{2} + \sqrt[3]{5}]$.
3) Find the minimal polynomial of $\sqrt{2} + \sqrt[3]{5}$ over $\mathbb{Q}$.

Exercise 2.21. Find the minimal polynomials of $\sqrt[4]{3}i$ over $\mathbb{Q}[i]$ and over $\mathbb{Q}[\sqrt{3}]$.

Exercise 2.22. Find the minimal polynomial of $\sqrt{2} + \sqrt[3]{5}i$ over $\mathbb{Q}[i]$.

Lecture 3

Algebraic field extensions form a nice class of extensions. The same happens with finite field extensions.

Proposition 2.23. *Let F/K be a subextension of E/K. Then E/K is algebraic if and only if E/F and F/K are algebraic.*

Proof. If E/K is algebraic, then E/F and F/K are both algebraic, as $K \subseteq F \subseteq E$. Let us assume that E/F and F/K are both algebraic. Let $x \in E$ and let L be the subextension over K generated by the coefficients of $f(x, F)$, the minimal polynomial of x over F. Then L/K is finite, since it is generated by finitely many algebraic elements. Moreover, x is algebraic over L. Since

$$[L(x) : K] = [L(x) : L][L : K] < \infty,$$

$L(x)/K$ is algebraic. In particular, x is algebraic over K. □

Exercise 2.24. Let F/K be a subextension of E/K. Prove that E/K is finite if and only if E/F and F/K are finite.

Let $F \subseteq E$ and $L \subseteq E$. The composite of F and L is defined as

$$FL = K(F \cup L) = F(L) = L(F)$$

and it is equal to the smallest field that contains F and L.

Exercise 2.25. If $F = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt{3})$, then $FL = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Compute $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ and $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3})$.

Exercise 2.26. Let $\xi \in \mathbb{C}$ be a primitive cubic root of one. If $F = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(\xi)$, then $FL = \mathbb{Q}(\sqrt[3]{2}, \xi)$. Compute $[\mathbb{Q}(\sqrt[3]{2}, \xi) : \mathbb{Q}]$ and $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\xi)$.

Exercise 2.27. Let E/K and F/K be extensions, where both E and F are subfields of a field L. If F/K is algebraic, then EF/E is algebraic.

Exercise 2.28. Let E/K and F/K be extensions, where both E and F are subfields of a field L. If F/K is finite, then EF/E is finite.

The solution to the previous exercise shows, in particular, that $[EF:E] \leq [F:K]$.

Lemma 2.29. *Let $\sigma\colon K \to L$ be a field homomorphism. Then there exists an extension E/K and a field isomorphism $\varphi\colon E \to L$ such that $\varphi|_K = \sigma$.*

Proof. Let A be a set in bijection with $L \setminus \sigma(K)$ and disjoint with K. Let $E = K \cup A$. If $\theta\colon A \to L \setminus \sigma(K)$ is bijective, then let

$$\varphi\colon E \to L, \quad \varphi(x) = \begin{cases} \sigma(x) & \text{if } x \in K, \\ \theta(x) & \text{if } x \in A. \end{cases}$$

Then φ is a bijective map such that $\varphi|_K = \sigma$. Transport the operations of L onto E, that is to define binary operations on E as follows:

$$(x,y) \mapsto x \oplus y = \varphi^{-1}(\varphi(x) + \varphi(y)), \qquad (x,y) \mapsto x \odot y = \varphi^{-1}(\varphi(x)\varphi(y)).$$

Then, for example,

$$x \oplus y = \varphi^{-1}(\varphi(x)+\varphi(y)) = \varphi^{-1}(\sigma(x)+\sigma(y)) = \varphi^{-1}(\sigma(x+y)) = \varphi^{-1}(\varphi(x+y)) = x+y$$

for all $x, y \in K$. □

If $\sigma\colon A \to B$ is a ring homomorphism, then σ induces a ring homomorphism $\overline{\sigma}\colon A[X] \to B[X]$, $\sum_i a_i X^i \mapsto \sum \sigma(a_i) X^i$.

Theorem 2.30. *Let K be a field and $f \in K[X]$ be such that* $\deg f > 0$. *Then there exists an extension E/K such that f admits a root in E.*

Proof. We may assume that f is irreducible over K. Let $L = K[X]/(f)$ and $\pi\colon K[X] \to L$ be the canonical map. Then L is a field (the reader should explain why). Let $\sigma\colon K \to L$, $a \mapsto \pi(aX^0)$, and $g = \overline{\sigma}(f) \in L[X]$.

We claim that $\pi(X)$ is a root of g in L. Suppose that $f = \sum_i a_i X^i$. Then

$$\begin{aligned} g(\pi(X)) &= \overline{\sigma}(f)(\pi(X)) \\ &= \sum_i \sigma(a_i)\pi(X)^i = \sum_i \pi(a_i X^0)\pi(X^i) = \pi(\sum a_i X^i) = \pi(f) = 0. \end{aligned}$$

The previous lemma states that there exists an extension E/K and an isomorphism $\varphi\colon E \to L$ such that $\varphi|_K = \sigma$. Note that $\varphi(x) = 0$ if and only if $x = 0$. If $u = \pi(X)$, then $\varphi^{-1}(u)$ is a root of f in E, as

$$\begin{aligned} \varphi(f(\varphi^{-1}(u))) &= \varphi\left(\sum_i a_i \varphi^{-1}(u)^i\right) = \varphi\left(\sum_i a_i \varphi^{-1}(u^i)\right) \\ &= \sum_i \varphi(a_i) u^i = \sum_i \sigma(a_i) u^i = g(u) = 0. \end{aligned}$$ □

As a corollary, if K is a field and $f_1, \dots, f_n \in K[X]$ are polynomials of positive degree, then there exists an extension E/K such that each f_i admits a root in E. This is proved by induction on n.

Definition 2.31. A field K is **algebraically closed** if each $f \in K[X]$ of positive degree admits a root in K.

The *fundamental theorem of algebra* states that $\mathbb{C}$ is algebraically closed. A typical proof uses complex analysis. Later we will give a proof of this result using Galois theory.

Proposition 2.32. *The following statements are equivalent:*

1) *K is algebraically closed.*
2) *If $f \in K[X]$ is irreducible, then* $\deg f = 1$.
3) *If $f \in K[X]$ is non-zero, then f decomposes linearly in $K[X]$, that is*

$$f = a \prod_{i=1}^{n} (X - \alpha_i)^{m_i}$$

for some $a \in K$ and $\alpha_1, \dots, \alpha_n \in K$.
4) *If E/K is algebraic, then $E = K$.*

Proof. 1) $\implies$ 2 $\implies$ 3) are exercises.

Let us prove that 3) $\implies$ 4). Let $x \in E$. Decompose $f(x, K)$ linearly in $K[X]$ as $f(x, K) = a \prod_{i=1}^{n} (X - \alpha_i)^{m_i}$ and evaluate on x to obtain that $x = \alpha_j$ for some j.

To prove that 4) $\implies$ 1) let $f \in K[X]$ be such that $\deg f > 0$. There exists an extension E/K such that f has a root x in E. The extension $K(x)/K$ is algebraic and hence $K(x) = K$, so $x \in K$. □

§3. Artin's theorem

Definition 3.1. The **algebraic closure** of a field K is an algebraic extension C/K such that C is algebraically closed.

For example, $\mathbb{C}/\mathbb{R}$ is an algebraic closure but $\mathbb{C}/\mathbb{Q}$ is not.

Proposition 3.2. *Let C be algebraically closed and $\sigma \colon K \to C$ be a field homomorphism. If E/K is algebraic, then there exists a field homomorphism $\varphi \colon E \to C$ such that $\varphi|_K = \sigma$.*

Proof. Suppose first that $E = K(x)$ and let $f = f(x, K)$. Let $\overline{\sigma}(f) \in C[X]$ and let $y \in C$ be a root of $\overline{\sigma}(f)$. If $z \in E$, then $z = g(x)$ for some $g \in K[X]$. Let $\varphi \colon E \to C$, $z \mapsto \overline{\sigma}(g)(y)$.

The map φ is well-defined. If $z = h(x)$ for some $h \in K[X]$, then

$$0 = g(x) - h(x) = (g-h)(x)$$

and thus f divides $g-h$. In particular, $\overline{\sigma}(f)$ divides $\overline{\sigma}(g-h) = \overline{\sigma}(g) - \overline{\sigma}(h)$ and hence $(\overline{\sigma}(g) - \overline{\sigma}(h))(y) = 0$.

It is an exercise to show that the map φ is a ring homomorphism.

Let $a \in K$. It follows that $\varphi|_K = \sigma$, as

$$\varphi(a) = \overline{\sigma}(aX^0)(y) = \sigma(a)$$

Let us now prove the proposition in full generality. Let X be the set of pairs (F,τ), where F is a subfield of E that contains K and $\tau\colon F \to C$ is a field homomorphism such that $\tau|_K = \sigma$. Note that $(K,\sigma) \in X$, so X is non-empty. Moreover, X is partially ordered by

$$(F,\tau) \leq (F_1,\tau_1) \iff F \subseteq F_1 \text{ and } \tau_1|_F = \tau.$$

If $\{(F_i,\tau_i) : i \in I\}$ is a chain in X, then $F = \cup_{i\in I} F_i$ is a subfield of E that contains K. Moreover, if $z \in F$, then $z \in F_i$ for some $i \in I$ and then one defines $\tau(z) = \tau_i(z)$. It is an exercise to prove that τ is well-defined. Since $(F,\tau) \in X$ is an upper bound, Zorn's lemma implies that there exists a maximal element $(E_1,\theta) \in X$. We claim that $E = E_1$. If not, let $z \in E \setminus E_1$. Since we know the proposition is true for the extension $E_1(z)/E_1$, let $\rho\colon E_1(z) \to C$ be a field homomorphism such that $\rho|_{E_1} = \theta$. Then, in particular, $\rho|_K = \sigma$. This implies that $(E_1(z),\rho) \in X$ and hence $(E_1,\theta) < (E_1(z),\rho)$, a contradiction to the maximality of (E_1,θ). $\square$

Lecture 4

The previous proposition will be used to prove that the algebraic closure always exists.

Theorem 3.3 (Artin). *Let K be a field. Then K admits an algebraic closure C/K. If C_1/K is an algebraic closure, then the extensions C/K and C_1/K are isomorphic.*

Proof. Let us first prove the uniqueness. The previous proposition implies the existence of an extensions homomorphism $\varphi\colon C \to C_1$. Let $y \in C_1$ and $f = f(y,K)$ be the minimal polynomial of y in K. Since f admits a factorization

$$f = \lambda \prod (X - \alpha_i)^{m_i}$$

in $C[X]$, it follows that

$$f = \overline{\varphi}(f) = \varphi(\lambda) \prod (X - \varphi(\alpha_i))^{m_i}$$

Since $0 = f(y)$, we conclude that $y = \varphi(\alpha_j)$ for some j. In particular, φ is surjective and hence φ is bijective.

We now prove the existence. Let us assume that K admits an extension E/K with E algebraically closed. We will prove later that this extension indeed exists, at the moment we only want to get an algebraic extension from this setting. Let

$$F = \{x \in E : x \text{ is algebraic over } K\}.$$

Then F/K is algebraic. Let $g \in F[X]$ be such that $\deg g > 0$. Since E is algebraically closed, g admits a root α in E. In particular, α is algebraic over F and hence α is algebraic over K. This implies that $\alpha \in F$, thus F is algebraically closed. This proves that F/K is an algebraic closure.

Let us prove that there exists an extension E_1/K such that every polynomial $f \in K[X]$ with $\deg f > 0$ has a root in E_1. Let $\{f_i : i \in I\}$ be the family of monic irreducible polynomials with coefficients in K. We may think that $f_i = f_i(X_i)$. Let $R = K[\{X_i : i \in I\}]$ and let J be the ideal of R generated by the $f_i(X_i)$. We claim that $J \neq R$. If not, $1 \in J$, so

$$1 = \sum_{j=1}^{m} g_j f_{i_j}(X_j)$$

for some $g_1, \dots, g_m \in R$. There exists an extension F/K such that f_{i_j} has a root α_j in F for all j. Let

$$\sigma \colon R \to F, \quad \sigma(X_k) = \begin{cases} \alpha_j & \text{if } k = i_j, \\ 0 & \text{if } k \notin \{i_1, \dots, i_m\}. \end{cases}$$

Then $1 = \sigma(1) = \sum_{j=1}^{m} \sigma(g_j) f_{i_j}(\alpha_j) = 0$, a contradiction.

Since J is a proper ideal, it is contained in a maximal ideal M. Let $L = R/M$ and let $\sigma \colon K \to L$ be the composition $K \hookrightarrow R \to R/M = L$, where $\pi \colon R \to R/M$ is the canonical map. As we did before, $\pi(X_i)$ is a root of $\overline{\sigma}(f_i)$ for all i. And there exists an extension E_1/K such that every f_i has a root in E_1. Proceeding in this way, we construct a sequence

$$E_1 \subseteq E_2 \subseteq \cdots$$

of fields such that every polynomial of positive degree and coefficients in E_k admits a root in E_{k+1}. Let $E = \cup E_k$. We claim that E is algebraically closed. In fact, let $g \in E[X]$ be such that $\deg g > 0$. Then, since $g \in E_r[X]$ for some r, it follows that g has a root in $E_{r+1} \subseteq E$. □

§4. Decomposition fields

Definition 4.1. Let K be a field and $f \in K[X]$ be such that $\deg f > 0$. A **decomposition field** of f over K is field E that contains K and that satisfies the following properties:

1) f factorizes linearly in $E[X]$.
2) if F is a field such that $K \subseteq F \subseteq E$ and f factorizes linearly in $F[X]$, then $F = E$.

Easy examples:

Example 4.2. $\mathbb{C}$ is a decomposition field of $X^2 + 1 \in \mathbb{R}[X]$.

Example 4.3. $\mathbb{Q}[\sqrt{2}]$ is a decomposition field of $X^2 - 2 \in \mathbb{Q}[X]$.

Example 4.4. The decomposition field of $f = X^2 - 2$ over $\mathbb{Z}/7$ is precisely $\mathbb{Z}/7$, as 3 and 4 are the roots of f in $\mathbb{Z}/7$.

Example 4.5. $\mathbb{Q}(\sqrt[3]{2})$ is not a decomposition field of $X^3 - 2 \in \mathbb{Q}[X]$. However, if ω ia a primitive cubic root of one, then $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a decomposition field of the polynomial $X^3 - 2 \in \mathbb{Q}[X]$.

Proposition 4.6. *E is a decomposition field of $f \in K[X]$ if and only if f factorizes linearly in $E[X]$ and $E = K(x_1, \dots, x_n)$, where $x_1, \dots, x_n$ are the roots of f.*

Proof. Let $f = a\prod_{i=1}^{r}(X-x_i)^{n_i}$ and $F = K(x_1,\dots,x_r)$ with $x_1,\dots,x_r \in E$. Since f factorizes linearly in $F[X]$, it follows that $F = E$. Conversely, let $E = K(x_1,\dots,x_r)$ and assume that f factorizes linearly in $F[X]$. Then, in particular, $x_1,\dots,x_r \in F$. Hence $E \subseteq F$ and $F = E$. □

One immediately obtains the following consequence: If E is a decomposition field of $f \in K[X]$, then E/K is finite.

Theorem 4.7. *Let $f \in K[X]$ be such that $\deg f > 0$. There exists a (unique up to extension isomorphism) decomposition field of f over K.*

Proof. Let C/K be an algebraic closure. Write $f = a\prod_{i=1}^{r}(X-x_i)^{n_i}$ in $C[X]$. Then $E = K(x_1,\dots,x_r)$ is a decomposition field of f over K. Let us prove uniqueness: if E_1/K is a decomposition field of f over K, then E_1/K is algebraic and thus Proposition 3.2 implies that there exists $\varphi \in \operatorname{Hom}(E_1/K, C/K)$, that is $\varphi\colon E_1 \to C$ is a field homomorphism such that $\varphi|_K$ is the identity. Factorize f linearly in $E_1[X]$ and apply $\overline{\varphi}$:

$$f = a\prod_{j=1}^{s}(X-y_j)^{m_j} \implies f = \overline{\varphi}(f) = \varphi(a)\prod_{j=1}^{s}(X-\varphi(y_j))^{m_j}$$

so f factorizes linearly in $\varphi(E_1)$. Moreover, $E_1 = K(y_1,\dots,y_s)$ and it follows that $\varphi(E_1) = K(\varphi(y_1),\dots,\varphi(y_s))$. Thus $\varphi(E_1)$ is a decomposition field of f. Since $\varphi(E_1) \subseteq C$, it follows that $\varphi(E_1) = E$. □

Exercise 4.8. If E/K is finite and $\varphi \in \operatorname{Hom}(E/K, E/K)$, then φ is an isomorphism.

Let C be an algebraic closure of K and $G = \operatorname{Gal}(C/K)$. The group G acts on C

$$\sigma \cdot x = \sigma(x), \quad \sigma \in G, x \in C.$$

The orbits are of the form

$$O_G(x) = \{\sigma(x) : \sigma \in G\} = \{y \in C : y = \sigma(x) \text{ for some } \sigma \in G\}$$

The elements $x, y \in C$ are **conjugate** if $y = \sigma(x)$ for some $\sigma \in G$.

Proposition 4.9. *Let C be an algebraic closure of K and $x, y \in C$. Then x and y are conjugate if and only if $f(x,K) = f(y,K)$. In particular, $O_G(x)$ is finite.*

Proof. Let $G = \operatorname{Gal}(C/K)$. If x and y are conjugate, say $y = \sigma(x)$ for some $\sigma \in G$, let us write $g = f(x,K)$ as

$$g = X^n + \sum_{i=0}^{n-1} a_i X^i.$$

Then $0 = g(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ and hence y is a root of g, as

$$0=\sigma\left(x^n+\sum_{i=0}^{n-1}a_ix^i\right)=\sigma(x)^n+\sum_{i=0}^{n-1}\sigma(a_i)\sigma(x)^i$$
$$=\sigma(x)^n+\sum_{i=0}^{n-1}a_i\sigma(x)^i=y^n+\sum_{i=0}^{n-1}a_iy^i.$$

Thus $f(y,K)=g$.

Conversely, assume that $f(x,K)=f(y,K)$. Let $g=f(x,K)=f(y,K)$ and let

$$\varphi\colon K[x]\to K[y],\quad h(x)\mapsto h(y).$$

Let us show that the map φ is well-defined: we need to show that if $h_1(x)=h_2(x)$, then $h_1(y)=\varphi(h_1(x))=\varphi(h_2(x))=h_2(y)$. If $h_1(x)=h_2(x)$, then

$$(h_1-h_2)(x)=h_1(x)-h_2(x)=0.$$

This implies that g divides h_1-h_2. In particular, $h_1(y)=h_2(y)$.

A straightforward calculation shows that φ is a field homomorphism such that $\varphi|_K=\mathrm{id}$, this means that φ is an extension homomorphism such that $\varphi(x)=y$. There exists $\sigma\in\mathrm{Hom}(C/K,C/K)$ such that $\sigma|_{K[x]}=\varphi$. Since σ is bijective (this is left as an exercise, you did something similar before), $\sigma(x)=\varphi(x)=y$ and hence $O_G(x)=O_G(y)$. □

Proposition 4.10. *Let C be an algebraic closure of K and x. Then*

$$f(x,K)=\prod_{y\in O_G(x)}(X-y)^m$$

for some m.

Proof. For each $y\in O_G(x)$ let m_y be the multiplicity of y in $f(x,K)$. Then, for example, $f(x,K)=(X-x)^{m_x}g$ for some g. If $y\in O_G(x)$, then $y=\sigma(x)$ for some $\sigma\in\mathrm{Gal}(C/K)$. Since

$$\overline{\sigma}(f(x,K))=f(x,K)=(X-y)^{m_x}\overline{\sigma}(g),$$

it follows that $m_y\geq m_x$. By symmetry, we conclude that $m_x=m_y$. □

The previous proposition shows, in particular, that all the roots of an irreducible polynomial $f\in K[X]$ in an algebraic closure C of K have the same multiplicity. This is not true if f is not irreducible. Find an example.

Definition 4.11. Let K be a field and $\{f_i:i\in I\}$ be a non-empty family of polynomials of positive degree with coefficients in K. A **decomposition field** of $\{f_i:i\in I\}$ is an extension E/K such that every f_i factorizes linearly in $E[X]$ and if F/K is a sub extension of E/K such that every f_i factorizes linearly in $F[X]$, then $F=E$.

Exercise 4.12. Prove that E/K is a decomposition field of $\{f_i:i\in I\}$ if and only if every f_i factorizes linearly in $E[X]$ and $E=K(S)$ where $S=\{\text{roots of } f_i \text{ for all } i\}$.

Exercise 4.13. Prove that if E/K is a decomposition field of $\{f_i : i \in I\}$, then E/K is algebraic. If, moreover, I is finite, then E/K is a decomposition field of $\prod_{i \in I} f_i$.

Exercise 4.14. Prove that there exists a decomposition field of $\{f_i : i \in I\}$ and it is unique up to extension isomorphism.

Exercise 4.15. Let $f = X^3 - X - 1 \in (\mathbb{Z}/3)[X]$ and E be a decomposition field of f. Compute $[E : \mathbb{Z}/3]$.

What about the decomposition field of $f = X^3 - X - 1 \in \mathbb{Q}[X]$?

Exercise 4.16. Let $f = X^4 - 5x^2 + 5 \in \mathbb{Q}[X]$ and E be a decomposition field of f. Compute $[E : \mathbb{Q}]$ and $\mathrm{Gal}(E/K)$.

§5. Normal extensions

Proposition 5.1. *Let E/K be an algebraic extension and $\sigma \in \mathrm{Hom}(E/K, E/K)$. Then σ is bijective.*

Proof. Let $x \in E$ and C be an algebraic closure of K that contains E. There exists $\varphi\colon C \to C$ such that $\varphi|_E = \sigma$. Thus $\varphi|_K = \sigma|_K = \mathrm{id}_K$. Let $G = \mathrm{Gal}(C/K)$. Then $\varphi \in G$. If $z \in O_G(x)$, then $z = \tau(x)$ for some $\tau \in G$ and hence

$$\varphi(z) = \varphi(\tau(x)) = (\varphi\tau)(x).$$

This implies that $\varphi(z) \in O_G(x)$ and $\varphi(O_G(x)) = O_G(x)$. Thus $\sigma|_{(E \cap O_G(x)}$ is injective and

$$\begin{aligned}\sigma(E \cap O_G(x)) &= \varphi(E \cap O_G(x)) \\ &= \varphi(E) \cap \varphi(O_G(x)) = \sigma(E) \cap O_G(x) \subseteq E \cap O_G(x).\end{aligned}$$

Since $|E \cap O_G(x)| < \infty$, it follows that $E \cap O_G(x) = \sigma(E \cap O_G(x))$ and hence x belongs to the image of σ. $\square$

Lecture 5

Definition 5.2. Let E/K be an algebraic extension and C be an algebraic closure of K containing E. Then E/K is **normal** if $\sigma(E) \subseteq E$ for all $\sigma \in \mathrm{Hom}(E/K, C/K)$.

Note that $\sigma(E) \subseteq E$ in the previous definition is equivalent to $\sigma(E) = E$.

Example 5.3. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. Why?

Some trivial examples of normal extensions: K/K is normal and if C is an algebraic closure of K, then C/K is normal.

Example 5.4. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal. Every extension generated by algebraic elements of degree two is normal.

Exercise 5.5. Let ξ be a primitive cubic root of one. Then $\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q}$ is normal.

The following result is practical but technical. That is why we leave the proof as an exercise.

Exercise 5.6. Prove that the previous definition depends only on E (and not on the algebraic closure C).

Some properties:

Proposition 5.7. *Let E/K be a normal extension and $f \in K[X]$ be an irreducible polynomial that admits a root x in E. Then f factorizes linearly in E.*

Proof. We may assume that f is monic. Let C/K be an algebraic closure of K containing E. Let y be a root of f in C. Since $f = f(x, K) = f(y, K)$, it follows that $y = \sigma(x)$ for some $\sigma \in \mathrm{Gal}(C/K)$. Since E/K is normal, $\sigma|_E \colon E \to C$ is an automorphism of E/K, that is $\sigma(E) \subseteq E$. In particular, $y \in E$. $\square$

Let $K \subseteq F \subseteq E$ be a tower of fields. If E/K is normal, then E/F is normal. However, Note that E/K normal does not imply F/K normal, as this would imply that every extension is normal. Moreover, E/F normal and F/K normal do not imply E/K normal.

Example 5.8. The extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are both normal, but $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal, as the roots of X^4-2 are $\sqrt{2}$, $-\sqrt{2}$, $\sqrt{2}i$ and $-\sqrt{2}i$.

Recall that if C is an algebraic closure of K and $x \in C$, then

$$f(x,K) = \prod (X-y)^m,$$

where the product is taken over all $y \in O_{\mathrm{Gal}(C/K)}(x)$. If E/K is normal and $x \in E$, then there exists m such that

$$f(x,K) = \prod (X-y)^m,$$

where the product is taken over all $y \in O_{\mathrm{Gal}(E/K)}(x)$.

Proposition 5.9. *Let E/K and F/K be extensions. If F/K is normal, then EF/E is normal.*

Proof. Let C be an algebraic closure of E containing EF. Let $\sigma \in \mathrm{Hom}(EF/E, C/E)$. We claim that $\sigma(EF) = EF$. Let

$$\overline{K} = \{x \in C : x \text{ is algebraic over } K\}.$$

Then $\overline{K}$ is an algebraic closure over K and $F \subseteq \overline{K}$. Since F/K is normal and $\sigma|_F \in \mathrm{Hom}(F/K, \overline{K}/K)$, it follows that $\sigma(F) = F$. If $z \in EF$, then $z = \sum_{i=1}^m e_i f_i$ for some $e_1, \dots, e_m \in E$ and $f_1, \dots, f_m \in F$. Since $\sigma(e_i) = e_i$ for all i,

$$\sigma(z) = \sum_{i=1}^m \sigma(e_i)\sigma(f_i) = \sum_{i=1}^m e_i \sigma(f_i) \in EF. \qquad \square$$

Proposition 5.10. *Let E/K be an algebraic extension. Then E/K is normal if and only if E/K is the decomposition field of a family of polynomials of $K[X]$ of positive degree.*

Proof. Let $G = \mathrm{Gal}(E/K)$. If $x \in E$ and $f(x,K) = \prod_{y \in O_G(x)} (X-y)^m$, then $f(x,K)$ factorizes linearly in $E[X]$. Thus E/K is a decomposition field of the family $\{f(x,K) : x \in E\}$. Conversely, assume that E/K is a decomposition field of the family $\{f_i : i \in I\}$. Then $E = K(S)$ where S is the set of roots of the polynomials f_i. Let C/K be an algebraic closure of K that contains E and let $\sigma \in \mathrm{Hom}(E/K, C/K)$. Let $x \in S$. Then x is a root of some $f_j = \sum a_k X^k$. Since $f_j(x) = 0$, it follows that $\sigma(x)$ is a root of f_j, as

$$f_j(\sigma(x)) = \sum a_k \sigma(x)^k = \sum \sigma(a_k)\sigma(x^k) = \sigma\left(\sum a_k x^k\right) = \sigma(0) = 0.$$

Hence $\sigma(E) \subseteq E$. $\square$

Exercise 5.11. Let $E = \mathbb{Q}[\sqrt[4]{7} + \sqrt{2}]$.

1) Prove that $E/\mathbb{Q}$ is not normal.

2) Compute $[E : \mathbb{Q}]$.
3) Compute $\mathrm{Gal}(E/\mathbb{Q})$.

§6. Dedekind's theorem

Note that every extension homomorphism $E/K \to F/K$ is, in particular, a K-linear map $E \to F$, that is

$$\mathrm{Hom}(E/K, F/K) \subseteq \mathrm{Hom}_K(E, F).$$

If F/K is an extension and V is a K-vector space, the set $\mathrm{Hom}_K(E, F)$ of K-linear maps is a vector space over F with $(a \cdot f)(v) = af(v)$ for $a \in F$, $f \in \mathrm{Hom}_K(E, F)$ and $v \in V$.

Exercise 6.1. Prove that $\dim_F \mathrm{Hom}_K(V, F) \geq \dim_K V$. Moreover, if $\dim_K V < \infty$, then $\dim_F \mathrm{Hom}_K(V, F) = \dim_K V$.

If V is a vector space and S is a (possibly infinite) subset of V, then S is linearly independent if every finite subset of S is linearly independent.

Theorem 6.2 (Dedekind). *Let E/K and F/K be extensions and let $\{\varphi_i : i \in I\}$ be a subset of* $\mathrm{Hom}(E/K, F/K)$*, i.e. a family of extension homomorphisms. Assume that $\varphi_i \neq \varphi_j$ if $i \neq j$. Then the subset $\{\varphi_i : i \in I\} \subseteq \mathrm{Hom}_K(E, F)$ is linearly independent over F.*

Proof. Assume it is not. Let $\{\varphi_1, \dots, \varphi_n\}$ be linearly dependent over F with n minimal. Clearly, $n > 1$. We may assume that

$$\sum_{i=1}^{n} a_i \varphi_i = 0 \tag{5.1}$$

for some $a_1, \dots, a_n \in F$ all different from zero. Let $z \in E \setminus \{0\}$ be such that $\varphi_1(z) \neq \varphi_2(z)$. If $x \in E$, then

$$0 = \left(\sum_{i=1}^{n} a_i \varphi_i \right)(xz) = \sum_{i=1}^{n} a_i \varphi_i(xz) = \sum_{i=1}^{n} a_i \varphi_i(x) \varphi_i(z) = \left(\sum_{i=1}^{n} (a_i \varphi_i(z)) \varphi_i \right)(x).$$

Thus

$$\sum_{i=1}^{n} (a_i \varphi_i(z)) \varphi_i = 0. \tag{5.2}$$

Since $\sum_{i=1}^{n} a_i \varphi_i = 0$ and $\varphi_1(z) \neq 0$,

$$a_1 \varphi_1 + a_2 \frac{\varphi_2(z)}{\varphi_1(z)} \varphi_2 + \dots + a_n \frac{\varphi_n(z)}{\varphi_1(z)} \varphi_n = 0.$$

Thus, subtracting (5.1) and (5.2),

$$\left(a_2 - a_2\frac{\varphi_2(z)}{\varphi_1(z)}\right)\varphi_2 + \cdots + \left(a_n - a_n\frac{\varphi_n(z)}{\varphi_1(z)}\right)\varphi_n = 0.$$

Since $a_n \neq 0$ and $\varphi_2(z) \neq \varphi_1(z)$, the scalar $a_2 - a_2\frac{\varphi_2(z)}{\varphi_1(z)} \neq 0$ and hence $\{\varphi_2, \dots, \varphi_n\}$ is linearly dependent, a contradiction. □

If E/K and F/K are extensions, let $\gamma(E/K, F/K) = |\operatorname{Hom}(E/K, F/K)|$.

Exercise 6.3. Prove the following statements:

1) $\gamma(E/K, F/K) \leq \dim_F \operatorname{Hom}_K(E, F)$.
2) If $[E:K] < \infty$, then $\gamma(E/K, F/K) \leq [E:K]$.
3) If x is algebraic over K, then $\gamma(K(x)/K, F/K) \leq \deg(x, K)$.

If C is an algebraic closure of K, then we define $\gamma(E/K) = \gamma(E/K, C/K)$. This definition does not depend on the algebraic closure.

Exercise 6.4. If C and C_1 are algebraic closures of K, then

$$|\operatorname{Hom}(E/K, C/K)| = |\operatorname{Hom}(E/K, C_1/K)|.$$

Proposition 6.5. *Let C be an algebraic closure of K and $G = \operatorname{Gal}(C/K)$. If $x \in C$, then $\gamma(K(x)/K) = |O_G(x)|$.*

Proof. If $\sigma \in \operatorname{Hom}(K(x)/K, C/K)$, then there exists $\phi \in G$ such that $\phi|_{K(x)} = \sigma$. Thus $\sigma(x) = \phi(x) \in O_G(x)$. Conversely, if $y \in O_G(x)$, then there exists $\tau \in G$ such that $y = \tau(x)$. Hence $\tau|_{K(x)} \in \operatorname{Hom}(K(x)/K, C/K)$ and $\tau|_{K(x)}(x) = y$. In particular, $\gamma(K(x)/K)$ divides $\deg(x, K)$. □

Exercise 6.6. If E/K is finite, then $|\operatorname{Gal}(E/K)| \leq [E:K]$. Moreover, E/K is normal if and only if $|\operatorname{Gal}(E/K)| = \gamma(E/K)$.

Lecture 6

If $t\colon A \to B$ is a surjective map, then $a \sim a_1 \iff t(a) = t(a_1)$ defines an equivalence relation on A. The set $\overline{A}$ of equivalence classes is in bijective correspondence with B, $\overline{A} \to B$, $\overline{a} \mapsto t(a)$. Moreover, if $|t^{-1}(\{b\})| = m$ for all $b \in B$, then $|A| = m|\overline{A}| = m|B|$.

Proposition 6.7. *Let E/K be algebraic and F/K be a subextension such that E/F is finite. Then $\gamma(E/K) = \gamma(E/F)\gamma(F/K)$.*

Proof. Assume that $E = F(x)$. Let $f = f(x,F) = \sum b_i X^i$ and let $G = \mathrm{Gal}(E/F)$. Let C be an algebraic closure of K containing E. The map

$$\lambda\colon \mathrm{Hom}(E/K,C/K) \to \mathrm{Hom}(F/K,C/K), \quad \sigma \mapsto \sigma|_F,$$

is well-defined. It is surjective: if $\varphi \in \mathrm{Hom}(F/K,C/K)$, then $\varphi\colon F \to C$ is, in particular, a field homomorphism. Since E/F is algebraic, by Proposition 3.2 there exists a field homomorphism $\sigma\colon E \to C$ such that $\sigma|_F = \varphi$. Since $\sigma|_K = \varphi|_K = \mathrm{id}$, in particular $\sigma \in \mathrm{Hom}(E/K,C/K)$.

For $\varphi \in \mathrm{Hom}(F/K,C/K)$,

$$\lambda^{-1}(\{\varphi\}) = \{\sigma \in \mathrm{Hom}(E/K,C/K) : \sigma|_F = \varphi\}$$

and let R_φ be the set of roots (in C) of the polynomial $\overline{\varphi}(f) = \sum \varphi(b_i)X^i$.

Claim. The map $\alpha\colon \lambda^{-1}(\{\varphi\}) \to R_\varphi$, $\sigma \mapsto \sigma(x)$, is well-defined.

We need to show that $\sigma(x)$ is a root of $\overline{\varphi}(f)$:

$$\begin{aligned}\overline{\varphi}(f)(\sigma(x)) &= \sum \varphi(b_i)\sigma(x)^i = \sum \sigma(b_i)\sigma(x^i) \\ &= \sum \sigma(b_i x^i) = \sigma\left(\sum b_i x^i\right) = \sigma(f(x)) = \sigma(0) = 0.\end{aligned}$$

Claim. The map $\beta\colon R_\varphi \to \lambda^{-1}(\{\varphi\})$, $y \mapsto \sigma_y$, where $\sigma_y(z) = \overline{\varphi}(h)(y)$ if $z = h(x)$, is well-defined.

We need to show that if $z = h(x)$ and $z = h_1(x)$ for some $h, h_1 \in F[X]$, then $\overline{\varphi}(h)(y) = \overline{\varphi}(h_1)(y)$. The assumptions imply that $(h-h_1)(x) = 0$ and hence f divides $h - h_1$. Since $\overline{\varphi}$ is a ring homomorphism, $\overline{\varphi}(f)$ divides $\overline{\varphi}(h) - \overline{\varphi}(h_1)$. This implies $(\overline{\varphi}(h) - \overline{\varphi}(h_1))(y) = 0$. We also need to show that $\sigma_y|_F = \varphi$: if $a \in F$, then write $a = aX^0 \in F[X]$. Thus $\sigma_y(a) = \overline{\varphi}(aX^0)(y) = \varphi(a) \in C$. It is now an exercise to prove that $\sigma_y \in \operatorname{Hom}(E/K, C/K)$.

Claim. $|\lambda^{-1}(\{\varphi\})| = |R_\varphi|$.

For this we need to show that β is the inverse of α, that is $\alpha \circ \beta = \mathrm{id}$ and $\beta \circ \alpha = \mathrm{id}$. To prove that $\beta \circ \alpha = \mathrm{id}$ let σ be such that $\sigma|_F = \varphi$. Then $y = \sigma(x) \in R_\varphi$. Let $z = h(x) = \sum a_i x^i \in F[x] = E$. Then

$$\overline{\varphi}(h)(y) = \sum \varphi(a_i) y^i = \sum \sigma(a_i) y^i = \sigma\left(\sum a_i x^i\right) = \sigma(y).$$

Conversely, if $y \in R_\varphi$, then

$$\alpha(\sigma_y) = \sigma_y(x) = y,$$

as $\sigma_y(x) = \overline{\varphi}(X)(y) = y$.

Claim. If $\phi \in G$ is such that $\phi|_F = \varphi$, then $O_G(x) = \phi^{-1}(R_\varphi)$.

Let us first prove $O_G(x) \supseteq \phi^{-1}(R_\varphi)$. If $y \in R_\varphi$, then

$$\begin{aligned} f(\phi^{-1}(y)) &= \sum b_i \phi^{-1}(y^i) = \phi^{-1}\left(\sum \phi(b_i) y^i\right) \\ &= \phi^{-1}\left(\sum \varphi(b_i) y^i\right) = \phi^{-1}\overline{\varphi}(f)(y)) = \phi^{-1}(0) = 0. \end{aligned}$$

Now we prove $O_G(x) \subseteq \phi^{-1}(R_\varphi)$. Let $z \in O_G(x)$ and $y \in C$ be such that $\phi^{-1}(y) = z$. Then $\overline{\varphi}(f)(y) = 0$, as

$$\begin{aligned} \overline{\varphi}(f)(y) &= \sum \varphi(b_i) y^i \\ &= \sum \varphi(b_i)\phi(z^i) = \sum \phi(b_i)\phi(z^i) = \phi\left(\sum b_i z^i\right) = \phi(f(z)) = \phi(0) = 0. \end{aligned}$$

It follows that $|\lambda^{-1}(\varphi)| = |O_G(x)|$ for all φ. By using the argument before the proposition,

$$\begin{aligned} \gamma(E/K) &= |\operatorname{Hom}(E/K, C/K)| \\ &= |O_G(x)||\operatorname{Hom}(F/K, C/K)| \\ &= |O_G(x)|\gamma(F/K). \end{aligned}$$

Since $\gamma(K(x)/K) = |O_G(x)|$ by Proposition 6.5, the claim follows.

For the general case we assume that $E = F(x_1, \dots, x_n)$. We proceed by induction on n. If $n = 0$, then $E = F$ and the result is trivial. If $n > 0$, let $L = F[x_1, \dots, x_{n-1}]$

and $E = L(x_n)$. The case proved implies that $\gamma(E/F) = \gamma(E/L)\gamma(L/F)$. By the inductive hypothesis, $\gamma(L/K) = \gamma(L/F)\gamma(F/K)$. Thus

$$\gamma(E/F)\gamma(F/K) = \gamma(E/L)\gamma(L/F)\gamma(F/K) = \gamma(E/L)\gamma(L/K) = \gamma(E/K),$$

again using the previous case. □

§7. Separable extensions

Definition 7.1. Let E/K be an algebraic extension and $x \in E$. Then x is **separable** over K if x is a simple root of $f(x, K)$.

An algebraic extension E/K is **separable** if every $x \in E$ is separable over K. Clearly, K/K is separable.

Exercise 7.2. Prove that an element x is separable over K if and only if x is a simple root of a polynomial with coefficients in K.

If F/K is a subextension of E/K and $x \in E$ is separable over K, then x is separable over F.

Exercise 7.3. If C is an algebraic closure of K, $x \in C$ and $G = \mathrm{Gal}(C/K)$. Prove that the following statements are equivalent:

1) x is separable over K.
2) Every $y \in O_G(x)$ is separable over K.
3) $\gamma(K(x)/K) = [K(x) : K] = \deg f(x, K)$.

Let K be any field and $g \in K[X]$. Let z be a root of g. Then z is a multiple root of g if and only if z is a root of g'.

Exercise 7.4. Prove that if K has characteristic zero or K is finite, then every algebraic extension of K is separable.

A consequence: Let E/K be a finite extension. Then E/K is separable if and only if $\gamma(E/K) = [E : K]$.

Example 7.5. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $[E : \mathbb{Q}] = 4$ and $\mathrm{Gal}(E/Q) \simeq C_2 \times C_2$. The extension E/Q is normal, as it is the decomposition field of $(X^2 - 2)(X^2 - 3)$ and it is separable as $\mathbb{Q}$ has characteristic zero.

Example 7.6. Let E be a decomposition field of $X^4 - 2$ over $\mathbb{Q}$. Then $E/\mathbb{Q}$ is normal and separable. Note that $E = \mathbb{Q}(\sqrt[4]{2}, i)$, so $[E : \mathbb{Q}] = 8 = |\mathrm{Gal}(E/\mathbb{Q})|$.

Let us compute $\mathrm{Gal}(E/\mathbb{Q})$. If $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, then $\sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i\}$ and $\sigma(i) \in \{-i, i\}$. Two examples are

$$\alpha\colon \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2}i, \\ i \mapsto i, \end{cases} \qquad \beta\colon \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2}, \\ i \mapsto -i. \end{cases}$$

It follows that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to the group $\langle \alpha, \beta \rangle$, which turns out to be isomorphic to the dihedral group of eight elements.

Another consequence: If $E = K(S)$, then E/K is separable if and only if every $x \in S$ is separable over K. One first does the case $E = K(x)$ and then proceeds by induction.

Exercise 7.7. Let $K \subseteq F \subseteq E$ be a tower of fields. Prove that if E/K is separable, then F/K and E/F are separable.

Exercise 7.8. Let E/K and F/K be extensions. Prove that if E/K is separable, then EF/E is separable.

Lecture 7

If E/K is algebraic, then

$$F = \{x \in E : x \text{ is separable over } K\}$$

is a subfield of E that contains K. It is known as the **separable closure** of K with respect to E. Note that $F = K(F)$, as $K(F)$ is separable because it is generated by separable elements. Moreover, F/K is separable and E/F is a **purely inseparable** extension, meaning that for every $x \in E \setminus F$, the polynomial $f(x,F)$ is not separable.

Proposition 7.9. *If E/K is separable and finite, then $E = K(x)$ for some $x \in E$.*

Proof. Let us assume that K is finite. Then E is finite and hence the multiplicative group $E^\times = E \setminus \{0\}$ is cyclic, say $E^\times = \langle x \rangle$. It follows that $E = K(x)$.

Let us now assume that K is infinite. We first consider the case $E = K(x,y)$. The general case $E = K(x_1,\dots,x_n)$ is left as an exercise, one needs to proceed by induction. Let $n = [E : K]$ and C be an algebraic closure of K containing E. Write $\operatorname{Hom}(E/K, C/K) = \{\sigma_1,\dots,\sigma_n\}$. Let

$$f = \prod_{1\leq i<j\leq n} \big((\sigma_i(y)-\sigma_j(y)) + X(\sigma_i(x)-\sigma_j(x))\big) \in C[X].$$

Then $f \neq 0$, as f is a product of non-zero polynomials. Since K is infinite, there exists $c \in K$ such that $f(c) \neq 0$. For any $r,s \in \{1,\dots,n\}$ with $r \neq s$,

$$\sigma_r(y) - \sigma_s(y) + c(\sigma_r(x) - \sigma_s(x)) \neq 0,$$

as $c \in K$. It follows that $\sigma_r(y+cx) \neq \sigma_s(y+cx)$. Thus $\gamma(K(y+cx)/K) \geq n$. Now

$$n \geq [K(y+cx) : K] = \gamma(K(y+cx)/K) \geq n,$$

so $[K(y+cx) : K] = n$ and hence $K(y+cx) = E$. $\square$

For example, $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}+i)$.

Proposition 7.10. *Let E/K be a finite extension. Then $E = K(x)$ for some $x \in E$ if and only if E/K admits finitely many subextensions.*

Proof. We first prove $\implies$. We may assume that K is infinite, otherwise the result is trivial. Let us assume that $E = K(x)$. We claim that the map

$$\Psi\colon \{F : K \subseteq F \subseteq E\} \to \{\text{monic divisors of } f(x,K)\}, \quad F \mapsto f(x,F),$$

is injective. Take $K \subseteq F_0 \subseteq F \subseteq E$ with $f(x,F) = f(x,F_0)$. Then

$$[E : F_0] = [F_0(x) : F_0] = \deg f(x,F_0) = m = [F(x) : F] = [E : F]$$

and hence $F = F_0$. It follows that Ψ is injective and therefore there are finitely many fields between K and E.

Let us prove $\impliedby$. As before let us assume that $E = K(x,y)$. For each $a \in K$ we consider the extension $K(ay+x)/K$. By assumption, there exist $a,b \in K$ such that $a \neq b$ and $K(x+ay) = K(x+by) = L$. We claim that $L = E$. Note that $x+ay \in L$ and $x+by \in L$, so $(a-b)y \in L$ and hence, since $K \subseteq L$, it follows that $y \in L$. Thus $x \in L$ and therefore $L = E$. □

As a consequence, if E/K is finite and separable, then E/K admits finitely many subextensions.

§8. Galois extensions

Let E/K be an algebraic extension. Assume that $E = K(S)$ and let C be an algebraic closure of K containing E. Let

$$T = \{y \in C : y \text{ is a root of } f(x,K) \text{ for some } x \in S\}$$

and let $L = K(T)$. Then $E \subseteq L$, as $S \subseteq T$. The extension L/K is normal, as L/K is a decomposition field of the family $\{f(x,K) : x \in S\}$. Moreover, L is the smallest normal extension of K containing E. The field L is the **normal closure** of E (with respect to C).

Exercise 8.1. If E/K is finite, then L/K is finite

Exercise 8.2. If E/K is separable, then L/K is separable.

Let E/K be an extension and $S \subseteq \mathrm{Gal}(E/K)$ be a subset. the set

$$^{S}E = \{x \in E : \sigma(x) = x \text{ for all } \sigma \in S\}$$

is a subfield of E that contains K. The subfield ^{S}E is known as the **fixed field** of S.

Definition 8.3. Let E/K be an algebraic extension and $G = \mathrm{Gal}(E/K)$. Then E/K is a **Galois extension** if $^{G}E = K$.

Clearly, K/K is a Galois extension. Note that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a Galois extension. Why?

Exercise 8.4. Prove that $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is a Galois extension.

Exercise 8.5. If the characteristic of K is different from two, then every quadratic extension of K is a Galois extension.

Exercise 8.6. Let E/K be an algebraic extension and $G = \mathrm{Gal}(E/K)$. Let $F = {}^G E$. Prove that $\mathrm{Gal}(E/F) = G$ and hence E/F is a Galois extension.

Proposition 8.7. *Let E/K be an algebraic extension. Then E/K is a Galois extension if and only if E/K is normal and separable.*

Proof. Let $G = \mathrm{Gal}(E/K)$. Let us first assume that E/K is Galois. For $x \in E$ let $f_x = \prod_{y\in O_G(x)}(X-y) = \sum a_i X^i \in E[X]$. If $\varphi \in G$, then

$$\overline{\varphi}(f_x) = \prod_{y\in O_G(x)} (X-\varphi(y)) = f_x,$$

as if $O_G(x) = \{\sigma_1(x),\dots,\sigma_r(x)\}$, then $\varphi(\sigma_i(x)) = (\varphi\sigma_i)(x) = \sigma_j(x)$ for some j. Since

$$\sum a_i X^i = f_x = \overline{\varphi}(f_x) = \sum \varphi(a_i) X^i,$$

it follows that $a_i \in {}^G E = K$ for all i. Thus $f_x \in K[X]$ and E/K is a decomposition field of the family $\{f_x : x \in E\}$. In particular, E/K is normal. Moreover, x is a simple root of $f_x \in K[X]$ and hence x is separable over K.

Conversely, let $x \in {}^G E$. Since E/K is normal, then $f(x,K) = \prod_{y\in O_G(x)}(X-y)^m$ for some m. Since E/K is separable, $m = 1$. Thus $f(x,K) = \prod_{y\in O_G(x)}(X-y) = X-x$ and $x \in K$. □

Definition 8.8. Let K be a field and $f \in K[X]$. Then f is **separable** if all roots of f are simple (in some algebraic closure of K).

Proposition 8.9. *Let E/K be a finite extension. Then E/K is a Galois extension if and only if E is a decomposition field over K of a separable polynomial $f \in K[X]$.*

Proof. Let us assume first that E/K is a Galois extension. Since E/K is finite and separable, $E = K(x)$ by Proposition 7.9. Then E/K is a decomposition field of $f(x,K)$ since E/K is normal. Since E/K is separable, x is separable over K. Thus x is a simple root of $f(x,K)$ and hence $f(x,K)$ is separable.

Conversely, let $x_1,\dots,x_r$ be the roots of a separable polynomial $f \in K[X]$. Then $E = K(x_1,\dots,x_r)$ is separable and normal. □

In the previous case, $\mathrm{Gal}(E/K)$ is known as the **Galois group** of the polynomial f. The notation is $\mathrm{Gal}(f,K)$. If $n = \deg f$ and $x_1,\dots,x_n$ are the roots of f, then any $\varphi \in \mathrm{Gal}(f,K)$ permutes the roots of f, that is φ permutes the set $\{x_1,\dots,x_n\}$. In particular, $\mathrm{Gal}(f,K)$ is isomorphic to a subgroup of $\mathbb{S}_n$ and hence $|\mathrm{Gal}(f,K)|$ divides $n!$.

Proposition 8.10. *Let E/K be a normal extension and F be the separable closure of K with respect to E. Then F/K is a Galois extension.*

Proof. Let C/K be an algebraic closure such that $E \subseteq C$. Let $\sigma \in \mathrm{Hom}(F/K, C/K)$. and let $\varphi \in \mathrm{Hom}(E/K, C/K)$ be such that $\varphi|_F = \sigma$. Since E/K is normal, $\varphi(E) = E$. Let $x \in F$. Then $\sigma(x) = \varphi(x) \in E$. Thus $f(\sigma(x), K) = f(x, K)$ and $\sigma(x)$ is separable over K, which implies that $\sigma(x) \in F$. Thus F/K is normal. Since F/K is separable, it follows that F/K is a Galois extension by Proposition 8.7. □

Some easy facts.

Exercise 8.11. Let E/K be a separable extension and L/K be the normal closure of E in some algebraic closure C that contains E. Prove that L/K is a Galois extension.

Exercise 8.12. Let E/K be a finite extension. Prove that E/K is Galois if and only if $[E : K] = |\mathrm{Gal}(E/K)|$.

Exercise 8.13. Let E/K be a Galois extension and F/K be a subextension of E/K. Prove that E/F is a Galois extension.

Lecture 8

Theorem 8.14 (Artin). *Let E be a field and G be a finite group of automorphisms of E. If $K = {}^{G}E$, then E/K is a Galois extension, $[E:K] = |G|$ and $\mathrm{Gal}(E/K) = G$.*

Before proving the theorem, we need a lemma.

Lemma 8.15. *Let E/K be a separable extension such that $\deg(x,K) \leq m$ for all $x \in E$. Then E/K is finite and $[E:K] \leq m$.*

Proof. Let $z \in E$ be of maximal degree. If $x \in E$, then $K(x,z)/K$ is separable. Then $K(x,z) = K(y)$ for some y. It follows that

$$K(z) \subseteq K(x,z) = K(y).$$

Since $\deg(z,K) \leq \deg(y,K)$, $\deg(z,K) = \deg(y,K)$. Hence $K(y) = K(z)$. In particular, $x \in K(z)$ and therefore $E = K(z)$. $\square$

Now we are ready to prove Artin's theorem:

Proof of Theorem 8.14. Note that $G \subseteq \mathrm{Gal}(E/K)$. Let $x \in E$ and

$$f_x = \prod_{y \in O_G(x)} (X - y).$$

Since $f_x \in K[X]$, it follows that the extension E/K is normal and separable (as it is a decomposition field of a family of separable polynomials), so E/K is a Galois extension. Moreover,

$$\deg(x,K) \leq \deg f_x = |O_G(x)| \leq |G|.$$

By the previous lemma, E/K is finite and $[E:K] \leq |G|$. This implies that $|G(E/K)| = [E:K] \leq |G|$ and hence $|G(E/K)| = |G|$. $\square$

Example 8.16. Let $E = K(X,Y)$ and $\sigma \colon K[X,Y] \to E$ be the ring homomorphism given by $\sigma(X) = Y$ and $\sigma(Y) = X$. Note that σ is bijective, as $\sigma^2 = \mathrm{id}$. The map

σ induces a field homomorphism $\overline{\sigma}\colon E \to E$ such that $\overline{\sigma}^2 = \mathrm{id}$. Recall that such a homomorphism is given by $f/g \mapsto \sigma(f)/\sigma(g)$. Let $G = \langle \overline{\sigma} \rangle$. Then $|G| = 2$. We claim that ${}^{G}E = K(X+Y, XY)$. Let $F = K(X+Y, XY)$. We only prove that ${}^{G}E \subseteq F$, as the other inclusion is trivial. Artin's theorem implies that $[E : {}^{G}E] = 2$ and $E = F(X)$, as X is a root of the polynomial $Z^2 - (X+Y)Z + XY$. Then $[E : F] \leq 2$ and $[{}^{G}E : F] = 1$.

§9. Galois' correspondence

Theorem 9.1 (Galois). *Let E/K be a finite Galois extension and $G = \mathrm{Gal}(E/K)$. There exists a bijective correspondence*

$$\{F : K \subseteq F \subseteq E \text{ subfields}\} \leftrightarrow \{\text{subgroups of } G\}$$

The correspondence is given by $F \mapsto G(E/F)$ and ${}^{S}E \leftarrow\!\shortmid S$. Moreover, normal subextensions of E/K correspond to normal subgroups of G.

$$\begin{tikzcd}[column sep=small]
 & & E \arrow[dl, dash] \arrow[dr, dash] & \\
 & F \arrow[dl, dash] \arrow[dr, dash] & & \{1\} \arrow[dl, dash] \\
K \arrow[dr, dash] & & S \arrow[dl, dash] & \\
 & G & &
\end{tikzcd}$$

Proof. Let α and β be the maps $\alpha(F) = \mathrm{Gal}(E/F)$ and $\beta(S) = {}^{S}E$. A routine exercise shows that α and β are well-defined. We first note that

$$\beta(\alpha(F)) = \beta(\mathrm{Gal}(E/F)) = {}^{\mathrm{Gal}(E/F)}E = F$$

since E/F is a Galois extension. Moreover,

$$\alpha(\beta(S)) = \alpha({}^{S}E) = \mathrm{Gal}(E/{}^{S}E) = S$$

by Artin's theorem, as S is finite.

Let F be a subfield of E containing K and $S = \alpha(F)$. Then

$$[F : K] = \frac{[E : K]}{[E : F]} = \frac{|G|}{|S|} = (G : S).$$

Let C be an algebraic closure of K that contains E. If $S = \mathrm{Gal}(E/F)$, then $F = {}^{S}E$.

We need to prove that F/K is normal if and only if S is normal in G. Let us first prove $\implies$. Let $\tau \in S$ and $\sigma \in G$. Since F/K is normal, $\sigma|_F \in \mathrm{Aut}(F)$. Thus

$\sigma^{-1}(F) = F$. In particular, if $x \in F$, then $\sigma^{-1}(x) \in F$ and

$$\sigma\tau\sigma^{-1}(x) = \sigma\sigma^{-1}(x) = x.$$

Conversely, let $\varphi \in \operatorname{Hom}(F/K, C/K)$. There exists $\Phi\colon E \to C$ such that $\Phi|_F = \varphi$. Since E/K is normal, $\Phi(E) = E$ and hence $\Phi \in G$. We claim that $\varphi(x) \in F$ for all $x \in F$. Note that $F = {}^S E$, so

$$\tau\varphi(x) = \tau\Phi(x) = \Phi\Phi^{-1}\tau\Phi(x) = \Phi(x) = \varphi(x)$$

for all $\tau \in S$, as $\Phi^{-1}\tau\Phi \in S$. This means that $\varphi(x) \in {}^S E = F$.

Let us compute $\operatorname{Gal}(F/K)$. Since F/K is normal, the map $\lambda\colon G \to \operatorname{Gal}(F/K)$, $\sigma \mapsto \sigma|_F$, is a surjective group homomorphism such that $\ker\lambda = S$. The first isomorphism theorem implies that $\operatorname{Gal}(F/K) \simeq G/S$. □

Some easy consequences.

Exercise 9.2. If E/K is a Galois extension of degree n and p is a prime number dividing n, then E/K admits a subextension of degree n/p.

Exercise 9.3. If E/K is a Galois extension of degree $p^\alpha m$ with p a prime number coprime with m, then E/K admits a subextension of degree m.

Definition 9.4. An extension E/K is **abelian** if E/K is a Galois extension with $\operatorname{Gal}(E/K)$ abelian.

Exercise 9.5. If E/K is an abelian extension of degree n and d divides n, then E/K admits a subextension of degree d.

Definition 9.6. An extension E/K is **cyclic** if E/K is a Galois extension with $\operatorname{Gal}(E/K)$ cyclic.

Example 9.7. The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ admits exactly three non-trivial subextensions:

$$\mathbb{Q}(\sqrt{2})/\mathbb{Q}, \quad \mathbb{Q}(\sqrt{3})/\mathbb{Q}, \quad \mathbb{Q}(\sqrt{6})/\mathbb{Q},$$

as $\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/Q) \simeq C_2 \times C_2$.

Example 9.8. Let $\omega \in \mathbb{C} \setminus \{1\}$ be such that $\omega^5 = 1$. Then

$$f(\omega, \mathbb{Q}) = 1 + X + X^2 + X^3 + X^4$$

and $\mathbb{Q}(\omega)/\mathbb{Q}$ has degree four. Moreover, $\mathbb{Q}(\omega)/\mathbb{Q}$ is a Galois extension and $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \simeq C_4$. If $\sigma \in \operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$, then $\sigma(\omega) = \omega^i$ for some $i \in \{1, \dots, 4\}$. Moreover, for every $i \in \{1, \dots, 4\}$ the map $\omega \mapsto \omega^i$ induces an automorphism of $\mathbb{Q}(\omega)/\mathbb{Q}$. Thus $|\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = 4$. Now

$$\sigma_i^k = \mathrm{id} \iff \omega^{i^k} = \sigma_i^k(\omega) = \omega \iff i^k \equiv 1 \bmod 5.$$

Thus the map σ_2 given by $\omega \mapsto \omega^2$ has order four.

Since $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \langle\sigma\rangle$, where $\sigma(\omega) = \omega^2$, is cyclic of order four, the extension $\mathbb{Q}(\omega)/\mathbb{Q}$ has a unique degree-two subtextension $F/\mathbb{Q}$. Note that $|\langle\sigma^2\rangle| = 2$ and $\sigma^2(\omega) = \omega^4 = \omega^{-1}$. Thus $F = {}^{\langle\sigma^2\rangle}\mathbb{Q}(\omega)$. Let $\theta = \omega + \omega^{-1}$. Then

$$\theta^2 = \omega^2 + \omega^3 + 2 = -(1 + \omega + \omega^{-1}) + 2 = 1 - \theta$$

and hence θ is a root of $X^2 + X - 1$. Since $\theta \notin \mathbb{Q}$, it follows that

$$\theta \in \{(-1 + \sqrt{5})/2, (-1 - \sqrt{5})/2\}.$$

Therefore $F = \mathbb{Q}(\sqrt{5})$.

Let us mention some other consequences.

Exercise 9.9. Let E/K be a finite Galois extension and $F_1, \dots, F_n$ fields such that $K \subseteq F_i \subseteq E$ for all $i \in \{1, \dots, n\}$. For every i let $S_i = \mathrm{Gal}(E/F_i)$. Then

$$\mathrm{Gal}\left(E/\bigcap_{i=1}^{n} F_i\right) = \left\langle \bigcup_{i=1}^{n} S_i \right\rangle, \quad \mathrm{Gal}\left(E/\prod_{i=1}^{n} F_i\right) = \bigcap_{i=1}^{n} S_i.$$

The following statement is a concrete application of the previous exercise.

Exercise 9.10. Let E/K be a finite Galois extension and $G = \mathrm{Gal}(E/K)$. Assume that G is the direct product $G = S \times T$ of the groups S and T. Let $F = {}^S E$ and $L = {}^T E$. Then $F \cap L = K$ and $FL = E$.

Proposition 9.11. *Let $E_1/K, \dots, E_r/K$ be Galois extensions. If $E = \prod_{i=1}^r E_i$, then E/K is a Galois extension. If, moreover, each E_i/K is finite, then*

$$\theta\colon \mathrm{Gal}(E/K) \to \mathrm{Gal}(E_1/K) \times \cdots \times \mathrm{Gal}(E_r/K), \quad \sigma \mapsto (\sigma|_{E_1}, \dots, \sigma|_{E_r}),$$

is an injective group homomorphism.

Proof. We only do the first part in the case $r = 2$, the general case is left as an exercise. Since E_1/K is algebraic, then E_1E_2/E_2 is algebraic. Since E_2/K is algebraic, E_1E_2/K is algebraic. Similarly, E_1E_2/K is separable.

Let C/K be an algebraic closure such that $E_1E_2 \subseteq C$. If $\sigma \in \mathrm{Hom}(E_1E_2/K, C/K)$, then $\sigma(E_1E_2) \subseteq \sigma(E_1)\sigma(E_2) = E_1E_2$ (do this calculation as an exercise). Thus E_1E_2/K is normal.

If both E_1/K and E_2/K are finite, then E_1E_2/K is finite.

Clearly, θ is a group homomorphism. We claim that the map θ is injective. Let $\sigma \in \ker\theta$. Then $\sigma|_{E_i} = \mathrm{id}_{E_i}$ for all $i \in \{1, \dots, r\}$. Let $S = \langle\sigma\rangle \subseteq \mathrm{Gal}(E/K)$ and $F = {}^S E$. Then $E_i \subseteq F$ for all $i \in \{1, \dots, r\}$ and hence $E \subseteq F$. It follows that $F = E = {}^{\{\mathrm{id}\}}E$ and therefore $S = \{\mathrm{id}\}$, so $\sigma = \mathrm{id}$. $\square$

Exercise 9.12. Let $E_1/K, \dots, E_r/K$ be finite Galois extensions such that for each j one has $E_j \cap (E_1 \cdots E_{j-1}E_{j+1} \cdots E_r) = K$. Then

$$\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(E_1/K) \times \cdots \times \mathrm{Gal}(E_r/K).$$

In this case, $[E : K] = \prod_{i=1}^{r} [E_i : K]$.

Lecture 9

§10. The fundamental theorem of algebra

We now present an easy proof of the fundamental theorem of algebra based on the ideas of Galois Theory. We need the following well-known facts:

1) Every real polynomial of odd degree admits a real root. This means that $\mathbb{R}$ does not admit extension of odd degree > 1.
2) Every complex number admits a square root in $\mathbb{C}$. This means that $\mathbb{C}$ does not admit degree-two extensions.

Theorem 10.1. *The field $\mathbb{C}$ is algebraically closed.*

Proof. Let $E/\mathbb{C}$ be an algebraic finite extension. Then $E/\mathbb{R}$ is finite separable extension of even degree. There exists a Galois extension $L/\mathbb{R}$ such that $E \subseteq L$, so $[L:\mathbb{R}]$ is even. Let $G = \mathrm{Gal}(L/\mathbb{R})$. Then $|G| = 2^m s$ for some odd number s. If T is a 2-Sylow subgroup of G, then there exists a subextension $F/\mathbb{R}$ of degree s. Since $\mathbb{R}$ does not admit extensions of odd degree > 1, $s = 1$ and hence G is a 2-group. Since $L/\mathbb{R}$ is a Galois extension, $L/\mathbb{C}$ is a Galois extension. In particular, $|\mathrm{Gal}(L/\mathbb{C})| = 2^{m-1}$. If $m > 1$, let U be a subgroup of $\mathrm{Gal}(L/\mathbb{C})$ of order 2^{m-2}. Then U corresponds to a subextension $L_1/\mathbb{C}$ of degree two, a contradiction. Hence $m = 1$ and $[L:\mathbb{C}] = 1$, so $L = \mathbb{C}$ and $E = \mathbb{C}$. □

§11. Purely inseparable extensions

Let E/K be an algebraic extension. In page 7 we defined the **separable closure** of K with respect to E as the field

$$F = \{x \in E : x \text{ is separable over } K\}.$$

Note that $K \subseteq F \subseteq E$ and $F = K(F)$. Moreover, F/K is separable and E/F is a **purely inseparable** extension, meaning that for every $x \in E \setminus F$, the polynomial $f(x,F)$ is not separable.

The number $[E : F]$ is known as the **degree of inseparability** of E/K. We write $[E : K]_{\text{ins}} = [E : F]$. Clearly, E/K is separable if and only if $[E : K]_{\text{ins}} = 1$ and E/K is purely inseparable if and only if $[E : K]_{\text{ins}} = [E : K]$.

Proposition 11.1. *Let K be a field of characteristic $p > 0$ and E/K be an algebraic extension. The following statements are equivalent:*

1) *E/K is purely inseparable.*
2) *If $x \in E$, then $x^{p^m} \in K$ for some $m \geq 0$.*
3) *If $x \in E$, then $f(x,K) = X^{p^m} - a$ for some $a \in K$ and $m \geq 0$.*
4) *$\gamma(E/K) = 1$.*

Proof. We first prove 1) $\implies$ 2). Let $x \in E$ and $f = f(x,K)$. Assume x is not separable. Then $f(x) = 0$ and $f'(x) = 0$, as x is not a simple root. Since $\deg f' < \deg f$ and f is the minimal polynomial of x, it follows that $f' = 0$. The coefficients of f' are of the form ka_k. Since E is a field, $a_k = 0$ if k is not divisible by p. If $a_k \neq 0$, then $k = pm$ for some $m \geq 0$. It follows that $f = g(X^p)$ for some $g \in K[X]$ with $\deg g < \deg f$. We now proceed by induction on the degree of x. The result is clearly true for elements of degree one. So assume the result holds for element of degree $\leq n$ for some $n \geq 1$. If $x \in E$ is such that $\deg(x,K) = n+1$, then, since $f(x,K) = g(X^p)$, the element x^p has degree $\leq n$. By the inductive hypothesis, $x^{p^{m+1}} = (x^p)^{p^m} \in K$. We now prove 2) $\implies$ 3). Let $x \in E$ and m be the minimal positive integer such that $x^{p^m} \in K$. Then x is a root of $X^{p^m} - x^{p^m} \in K[X]$. Since $X^{p^m} - x^{p^m} = (X - x)^{p^m}$, it follows that

$$f(x,K) = (X - x)^r = X^r + \cdots + (-1)^r x^r$$

for some $r \in \{1, \dots, p^m\}$. Write $r = p^s t$ for some integer t coprime with p and s such that $0 \leq s \leq m$. Let $a, b \in \mathbb{Z}$ be such that $ar + bp^m = p^s$. Then

$$x^{p^s} = x^{ar+bp^m} = (x^r)^a \left(x^{p^m}\right)^b \in K.$$

The minimality of m implies that $s \geq m$ and hence $s = m$. Now $p^m t = p^s t = r \leq p^m$, so $t = 1$. This means $f(x,K) = X^{p^m} - x^{p^m}$.

We now prove 3) $\implies$ 4). Let C/K be an algebraic closure that contains E and $\sigma \in \operatorname{Hom}(E/K, C/K)$. Let $x \in E$. We claim that $\sigma(x) = x$. Since $f(x,K) = X^{p^m} - a$,

$$(\sigma(x))^{p^m} = \sigma\left(x^{p^m}\right) = \sigma(a) = a = x^{p^m}.$$

It follows that $\sigma(x)$ is a root of $X^{p^m} - x^{p^m} = (X - x)^{p^m}$. Thus $\sigma(x) = x$.

Finally, we prove that 4) $\implies$ 1). Let C be an algebraic closure of K containing E. Then $\operatorname{Gal}(E/K) = \operatorname{Hom}(E/K, C/K) = \{\mathrm{id}\}$, as $\gamma(E/K) = 1$. If $x \in E$ is separable over K, then

$$f(x,K) = \prod_{y \in O_{\operatorname{Gal}(E/K)}(x)} (X - y) = X - x \in K[X].$$

Thus $x \in K$ and hence E/K is purely inseparable. □

Some consequences:

Exercise 11.2. Let E/K be finite and purely inseparable. Then $[E:K] = p^s$ for some prime number p and some s. Moreover, $x^{[E:K]} \in K$.

For the first part of previous exercise write $E = K(x_1, \dots, x_n)$ and proceed by induction on n.

Exercise 11.3. Let K be of characteristic $p > 0$ and E/K be a finite extension such that $[E:K]$ is not divisible by p. Then E/K is separable.

Let E/K be finite and F be the separable closure of K in E. Since

$$\gamma(E/K) = \gamma(E/F)\gamma(F/K) = \gamma(F/K),$$

it follows that

$$[E:K] = [E:F]\gamma(E/K) = [E:K]_{\text{ins}}\gamma(E/K).$$

§12. Norm and trace

Definition 12.1. Let E/K be a finite extension and C/K be an algebraic closure that contains E. Let $A = \operatorname{Hom}(E/K, C/K)$. For $x \in E$ we define the **trace** of x in E/K as

$$\operatorname{trace}_{E/K}(x) = [E:K]_{\text{ins}} \sum_{\varphi \in A} \varphi(x)$$

and the **norm** of x in E/K as

$$\operatorname{norm}_{E/K}(x) = \left(\prod_{\varphi \in A} \varphi(x)\right)^{[E:K]_{\text{ins}}}.$$

As an optional exercise, one can show that these definitions do not depend on the algebraic closure.

We collect some basic properties as an exercise:

Exercise 12.2. Let E/K be a finite extension. The following statements hold:

1) If E/K is not separable, then $\operatorname{trace}_{E/K}(x) = 0$ for all $x \in E$.
2) If $x \in K$, then $\operatorname{trace}_{E/K}(x) = [E:K]x$.
3) $\operatorname{trace}_{E/K}(x) \in K$ for all $x \in E$.
4) $\operatorname{norm}_{E/K}(x) = 0$ if and only if $x = 0$.
5) If $x \in K$, then $\operatorname{norm}_{E/K}(x) = x^{[E:K]}$.
6) $\operatorname{norm}_{E/K}(x) \in K$ for all $x \in E$.

One proves, moreover, that $\mathrm{trace}_{E/K}\colon E \to K$ satisfies

$$\mathrm{trace}_{E/K}(x+\lambda y) = \mathrm{trace}_{E/K}(x) + \lambda\,\mathrm{trace}_{E/K}(y)$$

for all $x, y \in E$ and $\lambda \in K$, that is to say that $\mathrm{trace}_{E/K}\colon E \to K$ is a linear form in E The norm $\mathrm{norm}_{E/K}\colon E^{\times} \to K^{\times}$ is a group homomorphism.

Exercise 12.3. Let E/K be a finite extension and $x \in E$. If

$$f(x,K) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0,$$

then $\mathrm{norm}_{E/K}(x) = ((-1)^n a_0)^{[E:K(x)]}$ and $\mathrm{trace}_{E/K}(x) = -[E:K(x)]a_{n-1}$.

Example 12.4. Let $E = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Then

$$\begin{aligned} &\mathrm{trace}_{E/\mathbb{Q}}(\sqrt{2}) = 0, && \mathrm{norm}_{E/\mathbb{Q}}(\sqrt{2}) = -4,\\ &\mathrm{trace}_{E/\mathbb{Q}(\sqrt{2})}(\sqrt{2}) = 2\sqrt{2}, && \mathrm{norm}_{E/\mathbb{Q}(\sqrt{2})}(\sqrt{2}) = 2. \end{aligned}$$

Example 12.5. If E/K is a finite Galois extension, then

$$\mathrm{trace}_{E/K}(x) = \sum_{\sigma\in\mathrm{Gal}(E/K)} \sigma(x) \quad\text{and}\quad \mathrm{trace}_{E/K}(x) = \prod_{\sigma\in\mathrm{Gal}(E/K)} \sigma(x)$$

for all $x \in E$. In particular, since $E = K(y)$ for some y by Proposition 7.9,

$$\mathrm{trace}_{E/K}(y) = -a_{n-1} \quad\text{and}\quad \mathrm{norm}_{E/K}(y) = (-1)^n a_0,$$

where $f(y,K) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$.

§13. Finite fields

In this section, p will be a prime number.

Proposition 13.1. *Let m be a positive integer. Up to isomorphism, there exists a unique field F_m of size p^m.*

Proof. Let C be an algebraic closure of the field $\mathbb{Z}/p$ and let $F_m = \{x \in C : x^{p^m} = x\}$ be the set of roots of $X^{p^m} - X$. Since the polynomial $X^{p^m} - X$ has no multiple roots, $|F_m| = p^m$. Moreover, F_m is the unique subfield of C of size p^m.

To prove the uniqueness it is enough to note that if K is a field of p^m elements, then K is the decomposition field of $X^{p^m} - X$ over $\mathbb{Z}/p$. □

Let $K = \mathbb{Z}/p$ and C be an algebraic closure of K. We claim that $C = \cup_k F_k$. If $x \in C$, then x is algebraic over K. Since $K(x)/K$ is finite, $K(x)$ is a finite field, say $|K| = p^r$ for some r. Then $x^{p^r} = x$ and hence $x \in F_r$.

Exercise 13.2. Prove the following statements:

1) If $x \in F_r$, then $x^{p^{rk}} = x$ for all $k \geq 0$.
2) If $m \mid n$, then $F_m \subseteq F_n$.
3) $F_m \cap F_n = F_{\gcd(m,n)}$.
4) $F_m \subseteq F_n$ if and only if $m \mid n$.

Proposition 13.3. *Every finite extension of a finite field is cyclic.*

Proof. Let $K = \mathbb{Z}/p$. It is enough to show that F_n/F_m is cyclic if m divides n.

We first prove that F_n/K is cyclic. Let $\sigma \in \mathrm{Gal}(F_n/K)$ be given by $\sigma(x) = x^p$. Note that $|\mathrm{Gal}(F_n/K)| = [F_n : K] = n$. Since $\sigma^i(x) = x^{p^i}$ for all $i \geq 0$, in particular, $\sigma^n(x) = x^{p^n} = x$. Thus $\sigma^n = \mathrm{id}$ and hence $|\sigma|$ divides n. Let $s = |\sigma|$. We know that $F_n^\times = F_n \setminus \{0\}$ is cyclic, say $F_n^\times = \langle g \rangle$. Since $|g| = p^n - 1$,

$$g = \sigma^s(g) = g^{p^s}$$

and hence $p^s \equiv 1 \bmod (p^n - 1)$. Thus $p^n - 1$ divides $p^s - 1$ and hence n divides s. Therefore $n = s$ and $\mathrm{Gal}(F_n/K) = \langle \sigma \rangle$.

For the general case note that if m divides n, then $\mathrm{Gal}(F_n/F_m)$ is a subgroup of $\mathrm{Gal}(F_n/K)$. Since $\mathrm{Gal}(F_n/K)$ is cyclic, the claim follows. □

If $K = \mathbb{Z}/p$ and m divides n, the subextension F_m corresponds to the unique subgroup of index m of $\mathrm{Gal}(F_n/K) = \langle \sigma \rangle$. This subgroup is $\langle \sigma^m \rangle$, where

$$\sigma^m(x) = x^{p^m} = x^{|F_m|}.$$

Note that $\mathrm{Gal}(F_n/F_m) = \langle \sigma^m \rangle$. The map σ^m is known as the **Frobenius automorphism**.

Exercise 13.4. Let E/K be an extension of finite fields . Then E/K is cyclic and $\mathrm{Gal}(E/K) = \langle \tau \rangle$, where $\tau(x) = x^{|K|}$.

Lecture 10

§14. Cyclotomic extensions

For $n \geq 1$ let $G_n(K) = \{x \in K : x^n = 1\}$ be the set of n-roots of one in K. Note that $G_n(K)$ is a cyclic subgroup of $K^\times$ and that $|G_n(K)|$ divides n.

Example 14.1. $G_n(\mathbb{R}) = \{-1, 1\}$ if n is odd and $G_n = \{1\}$ if n is even.

Exercise 14.2. Let K be a field of characteristic $p > 0$. Let $n = p^s m$ for some m not divisible by p. Then $G_n(K) = G_m(K)$.

Exercise 14.3. Let q be a prime number. Then $G_n(\mathbb{Z}/q) \simeq \mathbb{Z}/\gcd(n, q-1)$.

Similarly, one can prove that if K is a finite field, then $G_n(K)$ is a cyclic group of order $\gcd(n, |K^\times|)$.

Example 14.4. If C is algebraically closed of characteristic coprime with n, then $G_n(C)$ is cyclic of order n, as $X^n - 1$ has all his roots in C and does not contain multiple roots.

Let K be an algebraically closed field and n be such that n is coprime with the characteristic of K. The set of **primitive** n**-roots** is defined as

$$H_n(K) = \{x \in G_n(K) : |x| = n\}.$$

Definition 14.5. Let K be an algebraically closed field and n be such that n is coprime with the characteristic of K. The n**-th cyclotomic polynomial** is defined as

$$\Phi_n = \prod_{x \in H_n(K)} (X - x) \in K[X].$$

For $n \geq 1$ the Euler's function is defined as

$$\varphi(n) = |\{k : 1 \leq k \leq n,\ \gcd(k, n) = 1\}|.$$

For example, $\varphi(4) = 2$, $\varphi(8) = \varphi(10) = 4$ and $\varphi(p) = p - 1$ for every prime p.

Proposition 14.6. *Let K be an algebraically closed field and n be such that n is coprime with the characteristic of K. Let A be the ring of integers of K.*

1) $\deg \Phi_n = \varphi(n)$.
2) $\Phi_n \in A[X]$.

Proof. The first statement is clear. Let us prove 2) by induction on n. The case $n = 1$ is trivial, as $\Phi_1 = X - 1$. Assume that $\Phi_d \in A[X]$ for all d such that $d < n$. In particular,

$$\gamma = \prod_{\substack{d|n \\ d \neq n}} \Phi_d \in A[X].$$

Since γ is monic, it follows that $\frac{X^n - 1}{\gamma} \in A[X]$. Now the claim follows from

$$X^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \prod_{\substack{d|n \\ d \neq n}} \Phi_d = \Phi_n \gamma. \qquad \square$$

By taking degree in the equality $X^n - 1 = \prod_{d|n} \Phi_d$ one gets

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

Definition 14.7. Let $n \geq 2$ and K be a field of characteristic coprime with n. A **cyclotomic extension** of K of index n is a decomposition field of $X^n - 1$ over K.

Let C be an algebraic closure of K and $n \geq 2$ be coprime with the characteristic of K. If follows from Definition 14.7 that a cyclotomic extension of index n is of the form $K(\omega)/K$ for some $\omega \in H_n(K)$.

Proposition 14.8. *A cyclotomic extension of index n is abelian and of degree a divisor of $\varphi(n)$.*

Proof. Let C be an algebraic closure of K and $n \geq 2$ be coprime with the characteristic of K. Let $\omega \in H_n(C)$ and $K(\omega)/K$ be a cyclotomic extension. Then $K(\omega)/K$ is a Galois extension, as it is a decomposition field of a separable polynomial. Let $U = \mathcal{U}(\mathbb{Z}/n)$ be the group of units of $\mathbb{Z}/n$ and

$$\lambda\colon \operatorname{Gal}(K(\omega)/K) \to U, \quad \sigma \mapsto m_\sigma,$$

where m_σ is such that $\sigma(\omega) = \omega^{m_\sigma}$. The map λ is well-defined and it is a group homomorphism, as if $\sigma, \tau \in \operatorname{Gal}(K(\omega)/K)$, then, since

$$(\tau\sigma)(\omega) = \tau(\sigma(\omega)) = \tau(\omega^{m_\sigma}) = (\omega^{m_\sigma})^{m_\tau} = \omega^{m_\sigma m_\tau},$$

it follows that $\lambda(\sigma)\lambda(\tau) = \lambda(\sigma\tau)$. Since λ is injective, $\operatorname{Gal}(K(\omega)/K)$ is isomorphic to a subgroup of the abelian group U. Hence $\operatorname{Gal}(K(\omega)/K)$ is abelian. Moreover, $[K(\omega) : K] = |\operatorname{Gal}(K(\omega)/K)|$ is a divisor of $|U| = \varphi(n)$. $\square$

Exercise 14.9. Prove that a cyclotomic extension $K(\omega)/K$ has degree $\varphi(n)$ if and only if Φ_n is irreducible over K.

Note that Φ_n is irreducible over $\mathbb{Q}$. Some concrete examples:

$$\Phi_1 = X-1, \quad \Phi_2 = X+1, \quad \Phi_3 = X^2+X+1, \quad \Phi_6 = X^2-X+1.$$

If p is a prime number, then $\Phi_p = X^{p-1}+\cdots+X+1$.

Example 14.10. Φ_5 is irreducible over $\mathbb{Z}/2$. First note that $\Phi_5 = X^4+\cdots+X+1$ does not have roots in $\mathbb{Z}/2$. If Φ_5 is reducible, then, since X^2+X+1 is the unique monic irreducible polynomial over $\mathbb{Z}/2$, it follows that

$$\Phi_5 = (X^2+X+1)(X^2+X+1) = (X^2+X+1)^2 = X^4+X^2+1,$$

a contradiction.

Exercise 14.11. Prove that $\Phi_{12} = X^4-X^2+1$ is not irreducible over $\mathbb{Z}/5$.

§15. Hilbert's theorem

Let G be a group and A be a (left) G-module. This means that A is an abelian group and there exists a map

$$G\times A \to A, \quad (g,a)\mapsto g\cdot a$$

such that $1\cdot a = a$ for all $a\in A$, $(gh)\cdot a = g\cdot(h\cdot a)$ for all $g,h\in G$ and $a\in A$ and $g\cdot(a+b) = g\cdot a+g\cdot b$ for all $g\in G$ and $a,b\in A$.

Definition 15.1. Let A be a G-module. A **derivation** of A is a map $d\colon G\to A$ such that $d(gh) = g\cdot d(h)+d(g)$ for all $g,h\in G$.

Let A be a G-module and $a\in A$. The map $d(g) = g\cdot a-a$ is a derivation of A. Such derivations as known as **inner derivations**.

Exercise 15.2. Let E/K be a finite Galois extension and $G = \mathrm{Gal}(E/K)$. Then the (multiplicative) group $E^\times$ is a G-module with $\sigma\cdot x = \sigma(x)$.

In the context of the previous exercise, let $d\colon G\to E^\times$ be a derivation. For $\tau\in G$ let $x_\tau = d(\tau)$. Then

$$x_{\sigma\tau} = d(\sigma\tau) = (\sigma\cdot d(\tau))d(\sigma) = \sigma(x_\tau)x_\sigma.$$

Is this true that $x_\sigma = \frac{\sigma(c)}{c} = (\sigma\cdot c)c^{-1}$ for some $c\in E^\times$?

Proposition 15.3. *Let E/K be a finite Galois extension and $G = \mathrm{Gal}(E/K)$.*

1) *Let $\{x_\tau:\tau\in G\}\subseteq E^\times$ be such that $x_{\sigma\tau} = \sigma(x_\tau)x_\sigma$. Then there exists $c\in E^\times$ such that $x_\sigma = \frac{\sigma(c)}{c}$ for all $\sigma\in G$.*

2) *Let $\{x_\tau : \tau \in G\} \subseteq E$ be such that $x_{\sigma\tau} = \sigma(x_\tau) + x_\sigma$. Then there exists $c \in E$ such that $x_\sigma = \sigma(c) - c$ for all $\sigma \in G$.*

Proof. We prove 1). By Dedekind's theorem, the homomorphism $\sum_{\tau\in G} x_\tau^{-1}\tau$ is non-zero. Thus there exists $a \in E^\times$ such that $\sum_{\tau\in G} x_\tau^{-1}\tau(a) = c \in E^\times$. If $\sigma \in G$, then

$$\sigma(c) = \sum_{\tau\in G} \sigma(x_\tau^{-1})(\sigma\tau)(a) = \sum_{\tau\in G} x_{\sigma\tau}^{-1} x_\tau \sigma\tau(a) = x_\sigma \sum_{\tau\in G} x_{\sigma\tau}^{-1}\sigma\tau(a) = x_\sigma c.$$

We now prove 2). By Dedekind's theorem, $\sum_{\tau\in G}\tau \neq 0$. Since it is a linear form in E, it is surjective. In particular, there exists $a \in E$ such that $\sum_{\tau\in G}\tau(a) = 1$. Let $c = -\sum_{\tau\in G} x_\tau\tau(a)$. If $\sigma \in G$, then

$$\begin{aligned}\sigma(c) &= -\sum_{\tau\in G}\sigma(x_\tau)\sigma\tau(a)\\ &= -\sum_{\tau\in G}(x_{\sigma\tau} - x_\sigma)\sigma\tau(a)\\ &= -\sum_{\tau\in G} x_{\sigma\tau}\sigma\tau(a) + \sum_{\tau\in G} x_\sigma\sigma\tau(a) = c + x_\sigma.\end{aligned}$$

Hence $x_\sigma = \sigma(c) - c$. □

The following result is known as Hilbert's 90 theorem.

Theorem 15.4 (Hilbert). *Let E/K be a cyclic extension of degree n and let $G = \mathrm{Gal}(E/K) = \langle\sigma\rangle$.*

1) *Let $x \in E^\times$ be such that $\mathrm{norm}_{E/K}(x) = 1$, There exists $b \in E^\times$ such that $x = \sigma(b)/b$.*
2) *Let $x \in E$ be such that $\mathrm{trace}_{E/K}(x) = 0$. There exists $b \in E$ such that $x = \sigma(b) - b$.*

Proof. Let us prove 1). Note that $G = \{\sigma^i : 0 \le i < n\}$. For $i \in \{0, \dots, n-1\}$ let $x_{\sigma^i} = \prod_{k=0}^{i-1}\sigma^k(x)$. In particular, $x_\sigma = x$. We now check that $\{x_{\sigma^i}\}$ satisfy the assumptions of the previous proposition:

$$\begin{aligned}\sigma^j(x_{\sigma^i}) &= \prod_{k=0}^{i-1}\sigma^{k+j}(x) = \prod_{k=j}^{i+j-1}\sigma^k(x)\\ &= \prod_{k=0}^{i+j-1}\sigma^k(x)\left(\prod_{k=0}^{j-1}\sigma^k(x)\right)^{-1} = \prod_{k=0}^{i+j-1}\sigma^k(x)x_{\sigma^j}^{-1}.\end{aligned}$$

If $i + j < n$, then

$$\sigma^j\sigma^i = \sigma^{i+j} \implies \sigma^j(x_{\sigma^i}) = x_{\sigma^i\sigma^j}x_{\sigma^j}^{-1} \implies x_{\sigma^j\sigma^i} = \sigma^j(x_{\sigma^i})x_{\sigma^j}.$$

If $i + j = n + r$ for some $r \in \{0, \dots, n-1\}$, then, since $i + j < 2n$ and $\sigma^i\sigma^j = \sigma^r$,

$$\sigma^j(x_{\sigma^i}) = \prod_{k=0}^{n-1}\sigma^k(x)\prod_{k=n}^{n+r-1}\sigma^k(x)x_{\sigma^j}^{-1} = \prod_{k=0}^{r-1}\sigma^k(x)x_{\sigma^j}^{-1} = x_{\sigma^r}x_{\sigma^j}^{-1} = x_{\sigma^j\sigma^i}x_{\sigma^j}^{-1}$$

and hence $x_{\sigma^j\sigma^i} = \sigma^j(x_{\sigma^i})x_{\sigma^j}$. By the previous lemma, there exists $c \in E^\times$ such that $x_{\sigma^i} = \frac{\sigma^i(c)}{c}$. In particular, $x = x_\sigma = \sigma(c)/c$.

The second statement is similar and it is left as an exercise. $\square$

If A, B and C are groups (written multiplicatively) and $f\colon A \to B$ and $g\colon B \to C$ are group homomorphism, the sequence

$$A \xrightarrow{f} B \xrightarrow{g} C$$

of groups and homomorphisms is said to be **exact** if $f(A) = \ker g$. For example, the sequence

$$1 \longrightarrow B \xrightarrow{g} C$$

is exact if and only if g is injective, as the first map represents the trivial homomorphism. Similarly, the sequence

$$A \xrightarrow{f} B \longrightarrow 1$$

is exact if and only if f is surjective.

Corollary 15.5. *Let E/K be finite and cyclic with* $\mathrm{Gal}(E/K) = \langle\sigma\rangle$.

1) *The sequence*

$$1 \longrightarrow K^\times \hookrightarrow E^\times \xrightarrow{\rho} E^\times \xrightarrow{\mathrm{norm}_{E/K}} K^\times$$

is exact, where $\rho(z) = \sigma(z)/z$.

2) *The sequence*

$$0 \longrightarrow K \hookrightarrow E \xrightarrow{\lambda} E \xrightarrow{\mathrm{trace}\,E/K} K$$

is exact, where $\lambda(z) = \sigma(z) - z$.

Proof. We only prove 1). Note that $K^\times \hookrightarrow E^\times$ is the inclusion map. If $z \in \ker\rho$, then $\sigma(z) = z$ and hence $z \in K$. The sequence

$$E^\times \xrightarrow{\rho} E^\times \xrightarrow{\mathrm{norm}_{E/K}} K^\times$$

is exact by Hilbert's theorem. $\square$

Lecture 11

Proposition 15.6. *Let $n \geq 2$ and K be a field containing a primitive n-root of one. If $a \in K^\times$ and E/K is a decomposition field of $f = X^n - a$, then E/K is cyclic of degree d, where d divides n. Moreover,*

$$d = \min\{k : a^k \in K^n\},$$

where $K^n = \{x \in K : x = y^n$ for some $y \in K\}$. Conversely, if E/K is cyclic of degree n, then E/K is a decomposition field of an irreducible polynomial of the form $X^n - a$ for some $a \in K^\times$.

Proof. A decomposition field of f over K is of the form $K(\alpha)$, where $\alpha^n = a$. Thus $K(\alpha)/K$ is a Galois extension. If $\sigma \in \mathrm{Gal}(K(\alpha)/K)$, then $\sigma(\alpha)$ is a root of f, so $\sigma(\alpha) = \omega_\sigma \alpha$, where $\omega_\sigma \in G_n(K)$. This means that there exists an injective map

$$\lambda\colon \mathrm{Gal}(K(\alpha)/K) \to G_n(K), \quad \sigma \mapsto \omega_\sigma.$$

Moreover, λ is a group homomorphism, as

$$\sigma\tau(\alpha) = \sigma(\tau(\alpha)) = \sigma(\omega_\tau \alpha) = \omega_\tau \sigma(\alpha) = \omega_\tau \omega_\sigma \alpha.$$

Therefore $\mathrm{Gal}(K(\alpha)/K)$ is isomorphic to a subgroup of $G_n(K)$. In particular, $\mathrm{Gal}(K(\alpha)/K)$ is cyclic and $|\mathrm{Gal}(K(\alpha)/K)|$ divides n.

Let $d = |\mathrm{Gal}(K(\alpha)/K)|$. Since $a = \alpha^n$,

$$\mathrm{norm}(\alpha)^n = \mathrm{norm}(a) = a^d.$$

Thus $a^d \in K^n$, as $\mathrm{norm}(\alpha) \in K$. If $a^k \in K^n$, say $a^k = c^n$ for some $c \in K$, then

$$a^k = c^n = (\alpha^n)^k = (\alpha^k)^n \implies \alpha^k = c\omega \in K$$

for some $\omega \in G_n(K)$. Thus α is a root of $X^k - \alpha^k \in K[X]$ and hence $k \geq d$.

Note that $f(\alpha, K) = X^d - \alpha^d$.

Let E/K be cyclic of degree n. Assume that $\mathrm{Gal}(E/K) = \langle\sigma\rangle$. If ω is a primitive n-root of one,

$$\mathrm{norm}_{E/K}(\omega) = 1 = \omega^n.$$

By Hilbert's theorem, there exists $b \in E^\times$ such that $\omega = \sigma(b)/b$. Thus $\sigma(b) = \omega b$ and hence $\sigma^i(b) = \omega^i b$ for all $i \geq 0$. Since $|\{b, \sigma(b), \dots, \sigma^{n-1}(b)\}| = n$, it follows that $E = K(b)$. Moreover,

$$\sigma(b^n) = \sigma(b)^n = (\omega b)^n = b^n$$

and hence $b^n \in K$. This means that E/K is a decomposition field of $X^n - b^n$. Note that $X^n - b^n$ is irreducible, as $[E:K] = [K(b):K] = n$. □

Proposition 15.7. *Let K be a field of characteristic $p > 0$.*

1) *Let $a \in K$ and $f = X^p - X - a$. Then f is irreducible over K or all the roots of f belong to K. In the first case, if b is a root of f, then $K(b)/K$ is a cyclic extension of degree p.*
2) *Every cyclic extension of degree p is a decomposition field of an irreducible polynomial of the form $X^p - X - a$.*

Proof. We first prove 1). Let K_0 be the prime field of K. Note that $K_0 \simeq \mathbb{Z}/p$. Let b be a root of f and let $x \in K_0$. Then

$$f(b+x) = (b+x)^p - (b+x) - a = (b^p - b - a) + (x^p - x) = 0$$

and thus $\{b + x : x \in K_0\}$ is the set of roots of f. Note that $f' = -1$, so f has no multiple roots.

We claim that if $b \notin K$, then f is irreducible. If f is not irreducible, then $f = gh$ for some $g, h \in K[X]$ such that $0 < \deg g < p$. There exists a subset S of K_0 such that $g = \prod_{x \in S}(X - (b+x))$ and hence

$$|S|b + \sum_{x \in S} x = \sum_{x \in S}(b+x) \in K.$$

This implies that $|S|b \in K$ and hence, since $|S| \in K^\times$, it follows that $b \in K$.

Since $K(b)/K$ is a decomposition field of a separable polynomial, $K(b)/K$ is a Galois extension. Moreover, $|\mathrm{Gal}(K(b)/K)| = [K(b):K] = p$ and hence $\mathrm{Gal}(K(b)/K)$ is cyclic.

We now prove 2). Let E/K be cyclic of degree p. Assume that $\mathrm{Gal}(E/K) = \langle\sigma\rangle$. Since $\mathrm{trace}_{E/K}(1) = p = 0$, Hilbert's theorem implies that there exists $b \in E$ such that $\sigma(b) = b + 1$. In particular, $b \notin K$ and thus $E = K(b)$. Moreover, since

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

it follows that $b^p - b \in K$. Thus $f(b, K) = X^p - X - (b^p - b) \in K[X]$. □

§16. Symmetric polynomials

Let K be a field and $\{t_1,\dots,t_n\}$ be an algebraic independent set over K. Let $E = K(t_1,\dots,t_n)$ and $f = \prod_{i=1}^n (X-t_i) \in E[X]$. Then

$$f = X^n + \sum_{i=1}^n (-1)^i s_i X^{n-i},$$

where

$$\begin{aligned} s_1 &= t_1+t_2+\cdots+t_n,\\ s_2 &= \sum_{1\leq i<j\leq n} t_it_j,\\ &\vdots\\ s_n &= t_1t_2\cdots t_n. \end{aligned}$$

For example,

$$(X-t_1)(X-t_2)(X-t_3) = X^3-(t_1+t_2+t_3)X^2+(t_1t_2+t_2t_3+t_1t_3)X-t_1t_2t_3.$$

The polynomials $s_1,s_2,\dots,s_n$ are known as the **elementary symmetric polynomials** in the variables $t_1,\dots,t_n$. Note that $\deg s_i = i$.

Let $\sigma \in \mathbb{S}_n$ and

$$\alpha_\sigma\colon K[t_1,\dots,t_n]\to K[t_1,\dots,t_n],\quad t_i\mapsto t_{\sigma(i)}\quad\text{for all } i.$$

Then α_σ is a bijective homomorphism of K-algebras. In fact, $\alpha_\sigma^{-1} = \alpha_{\sigma^{-1}}$. Note that

$$\alpha_\sigma(h(t_1,\dots,t_n)) = h(t_{\sigma(1)},\dots,t_{\sigma(n)}).$$

Since α_σ is injective, it induces an element $\widehat{\sigma}\in \mathrm{Gal}(E/K)$ given by

$$\widehat{\sigma}\left(\frac{h}{g}\right) = \frac{\alpha_\sigma(h)}{\alpha_\sigma(h)}.$$

The map $\mathbb{S}_n\to \mathrm{Gal}(E/K)$, $\sigma\mapsto\widehat{\sigma}$, is an injective group homomorphism. Thus $\{\widehat{\sigma} : \sigma\in\mathbb{S}_n\}\simeq\mathbb{S}_n$.

Definition 16.1. Let $g\in K[t_1,\dots,t_n]$. Then g is **symmetric** if $\widehat{\sigma}(g) = g$ for all $\sigma\in\mathbb{S}_n$.

We write P to denote the set of symmetric polynomials in $K[t_1,\dots,t_n]$. Clearly, P is a subalgebra of $K[t_1,\dots,t_n]$. The following statements hold:

1) $K\subseteq P$.
2) $\sum_{i=1}^n t_i^r \in P$ for all $r\geq 1$.

3) $s_i \in P$ for all i.
4) $K(P) \subseteq {}^G E$, where $G = \{\widehat{\sigma} : \sigma \in \mathbb{S}_n\}$.

Let $F = K(s_1, s_2, \dots, s_n)$. Then E/F is a Galois extension, as it is a decomposition field of f.

Proposition 16.2. $[E : F] \leq n!$.

Proof. We proceed by induction on n. The case $n = 1$ is clear, as $E = F$. Assume that $n > 1$. Let $u_1, \dots, u_{n-1}$ be the elementary symmetric polynomials in $t_1, \dots, t_{n-1}$. Then

$$s_i = u_i + t_n u_{i-1}$$

for all $i \in \{1, \dots, n\}$, where $u_0 = 1$ and $u_n = 0$. Note that $u_1 = s_1 - t_n$ and $u_i = s_i - t_n u_{i-1}$ for all i. Since $K(s_1, \dots, s_n, t_n) = K(u_1, \dots, u_{n-1}, t_n)$,

$$F(t_n) = K(u_1, \dots, u_{n-1}, t_n) = K(t_n)(u_1, \dots, u_{n-1})$$

and

$$[E : F] = [E : F(t_n)][F(t_n) : F] \leq n[E : F(t_n)].$$

Note that $E = K(t_1, \dots, t_n) = K(t_n)(t_1, \dots, t_{n-1})$. By the inductive hypothesis, $[E : F(t_n)] \leq (n-1)!$ and hence $[E : F] \leq n!$, as desired. □

Theorem 16.3. ${}^G E = F$.

Proof. By Artin's theorem,

$$\left[{}^G E : F\right] = \frac{[E : F]}{\left[E : {}^G E\right]} \leq \frac{n!}{\left[E : {}^G E\right]} = 1$$

and hence ${}^G E = F$. □

Exercise 16.4. Prove that $\operatorname{Gal}(E/F) \simeq \mathbb{S}_n$.

Exercise 16.5. Prove that $\{s_1, \dots, s_n\}$ is algebraically independent over K.

Exercise 16.6. Prove that every symmetric polynomial in $t_1, \dots, t_n$ can be written as a rational fraction in $s_1, \dots, s_n$.

§17. Solvable groups

Let G be a group. If $x, y \in G$ we define the **commutator** of x and y as

$$[x, y] = xyx^{-1}y^{-1}.$$

Note that $[x, y] = 1$ if and only if $xy = yx$. Moreover, $[x, y]^{-1} = [y, x]$. The **commutator subgroup** $[G, G]$ of G is defined as the subgroup of G generated by all commutators, i.e.

$$[G,G] = \langle [x,y] : x,y \in G \rangle.$$

This means that every element of $[G,G]$ is a finite product of commutators, so every element of $[G,G]$ is of the form $\prod_{i=1}^{m}[x_i,y_i]$. In general, the commutator subgroup is not equal to the set of commutators!

Exercise 17.1. Let G be a group. Prove the following facts:

1) G is abelian if and only if $[G,G] = \{1\}$.
2) $[G,G]$ is a normal subgroup of G.
3) $G/[G,G]$ is abelian.
4) If H is a subgroup of G and $[G,G] \subseteq H$, then H is normal in G.
5) If H is a normal subgroup of G, then G/H is abelian if and only if $[G,G] \subseteq H$.

Definition 17.2. Let G be a group. The **derived series** of G is defined as $G^{(0)} = G$ and $G^{(k+1)} = [G^{(k)}, G^{(k)}]$ for $k \geq 0$.

Exercise 17.3. Prove that $G^{(k)}$ is normal in G for all k.

Why derived series? We cannot explain this here, but let us use the following notation. We write $G' = [G,G]$, $G'' = [G',G']$... Note that

$$G \supseteq G' \supseteq G'' \supseteq \cdots$$

Exercise 17.4. Let $n \geq 3$. Prove that $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$.

Example 17.5. Let $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Then K is a normal subgroup of $\mathbb{A}_4$. One proves that $[\mathbb{A}_4, \mathbb{A}_4] = K$.

Example 17.6. Let $n \geq 5$. Since $\mathbb{A}_n$ is a non-abelian simple group, it follows that $[\mathbb{A}_n, \mathbb{A}_n] = \mathbb{A}_n$.

Let us show that $\mathbb{A}_5$ is a non-abelian simple group. Hence it is not solvable:

```
julia> A5 = alternating_group(5)
Alt( [ 1 .. 5 ] )
julia> is_abelian(A5)
false
julia> is_simple(A5)
true
julia> is_solvable(A5)
false
```

Definition 17.7. A group G is **solvable** if and only if $G^{(m)} = \{1\}$ for some m.

Clearly, every abelian group is solvable.

Exercise 17.8. Prove that $\mathbb{S}_n$ is solvable if and only if $n \leq 4$.

Let us compute (with the computer software Oscar) the derived series of the symmetric group $\mathbb{S}_4$. The calculation shows that $\mathbb{S}_4$ is solvable:

```
julia> G = symmetric_group(4);
julia> derived_series(G)
4-element Vector{PermGroup}:
 Sym( [ 1 .. 4 ] )
 Alt( [ 1 .. 4 ] )
 Group([ (1,4)(2,3), (1,2)(3,4) ])
 Group(())
julia> [order(x) for x in derived_series(G)]
4-element Vector{fmpz}:
 24
 12
 4
 1
julia> is_solvable(G)
true
```

Proposition 17.9. *Let G be a group and H be a subgroup of G. The following statements hold:*

1) *If G is solvable, then H is solvable.*
2) *If H is normal in G and G is solvable, then G/H is solvable.*
3) *If H is normal in G and H and G/H are solvable, then G is solvable.*

Proof. The first statement follows from the fact that $H^{(i)} \subseteq G^{(i)}$ holds for all i.

Assume now that H is normal in G. Let $Q = G/H$ and $\pi\colon G \to Q$ be the canonical map. By induction one proves that $\pi(G^{(i)}) = Q^{(i)}$ for all $i \geq 0$. The case where $i = 0$ is trivial, as π is surjective. If the result holds for some $i \geq 0$, then

$$\pi(G^{(i+1)}) = \pi([G^{(i)}, G^{(i)}]) = [\pi(G^{(i)}), \pi(G^{(i)})] = [Q^{(i)}, Q^{(i)}] = Q^{(i+1)}.$$

We now prove 2). Since G is solvable, $G^{(n)} = \{1\}$ for some n. Thus Q is solvable, as $Q^n = \pi(G^{(n)}) = \pi(\{1\}) = \{1\}$.

We finally prove 3). Since Q is solvable, $Q^{(n)} = \{1\}$ for some n. Since $\pi(G^{(n)}) = Q^{(n)} = \{1\}$, it follows that $G^{(n)} \subseteq H$. Since H is solvable,

$$G^{(n+m)} \subseteq (G^{(n)})^{(m)} \subseteq H^{(m)} = \{1\}$$

for some m. Thus G is solvable. ◻

An application:

Proposition 17.10. *Let G be a finite p-group. Then G is solvable.*

Proof. Assume the result is not true. Let G be a finite p-group of minimal order that is not solvable. Since G is a p-group, $Z(G) \neq \{1\}$. Since $|G|$ is minimal, $G/Z(G)$ is a solvable p-group. Since $Z(G)$ is abelian, $Z(G)$ is solvable. Now G is solvable by Proposition 17.9. $\square$

We finish this discussion with two important theorems (without proof) about finite solvable groups.

Theorem 17.11 (Burnside). *Let p and q be prime numbers. If G is a group of order $p^a q^b$, then G is solvable.*

The proof appears in courses on representation theory of finite groups.

Theorem 17.12 (Feit–Thompson). *Every finite group of odd order is solvable.*

The proof of the theorem is extremely hard. It occupies a full volume of *Pacific Journal of Mathematics*, see [1].

Lecture 12

§18. Radical extensions

Definition 18.1. An extension E/K is **radical** if $E = K(x_1, \dots, x_m)$ such that for each $i \in \{1, \dots, m\}$ there exists $a_i \in \mathbb{Z}$ such that $x_i^{a_i} \in K(x_1, \dots, x_{i-1})$.

Note that radical extensions are finite.

Example 18.2. Let E be a decomposition field of $X^4 - 2$ over $\mathbb{Q}$. Then $E/\mathbb{Q}$ is radical, as $E = \mathbb{Q}(\sqrt[4]{2}, i)$.

Example 18.3. Let $\alpha, \beta \in \mathbb{C}$ be such that $\alpha^2 = 2$ and $\beta^5 = 1 + \alpha$. The number $\sqrt[5]{1+\sqrt{2}}$ belongs to the radical extension $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$.

Theorem 18.4. *Let K be of characteristic zero and R/K be a radical extension. If E/K is a subextension of R/K, then* $\mathrm{Gal}(E/K)$ *is solvable.*

Proof. Without loss of generality, we may assume that E/K is a Galois extension. In fact, let $G = \mathrm{Gal}(E/K)$ and $K_0 = {}^G E$. Then E/K_0 is a Galois extension and $\mathrm{Gal}(E/K_0) = G$ by Artin's theorem. Thus, replacing K by K_0 if needed, we may assume that E/K is Galois.

Let L be the normal closure of R in some algebraic closure C that contains R. Note that if $R = K(x_1, \dots, x_m)$, then

$$L = K(\{\sigma_i(x_j) : 1 \leq i \leq s,\ 1 \leq j \leq m\}),$$

where $\mathrm{Hom}(R/K, C/K) = \{\sigma_1, \dots, \sigma_s\}$.

Claim. L/K is radical.

Since $x_j^{a_j} \in K(x_1, \dots, x_{j-1})$ for some integer a_j,

$$\sigma_i(x_j)^{a_j} = \sigma_i\left(x_j^{a_j}\right) \in \sigma_i(K(x_1, \dots, x_{j-1}) = K(\sigma_i(x_1), \dots, \sigma_i(x_{j-1}))$$

Thus L/K is radical and Galois.

We may assume then that E/K and R/K are both Galois.

Since $\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(R/K)/\mathrm{Gal}(R/E)$, we only need to prove that $\mathrm{Gal}(R/K)$ is solvable.

Let ξ be a primitive n-th root of one (in some algebraic closure of K that contains R). Consider the diagram

$$\begin{tikzcd}[column sep=small] & R(\xi) \arrow[dl, dash] \arrow[dr, dash] & \\ R \arrow[dr, dash] & & K(\xi) \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Then

1) $K(\xi)/K$ and $R(\xi)/R$ are abelian.
2) $R(\xi)/K$ is Galois.
3) $\mathrm{Gal}(R/K) \simeq \mathrm{Gal}(R(\xi)/K)/\mathrm{Gal}(R(\xi)/R)$.
4) $\mathrm{Gal}(K(\xi)/K) \simeq \mathrm{Gal}(R(\xi)/K)/\mathrm{Gal}(R(\xi)/K(\xi))$.

The third item implies that we need to show that $\mathrm{Gal}(R(\xi)/K)$ is solvable. By the fourth item it suffices to show that $\mathrm{Gal}(R(\xi)/K(\xi))$ is solvable.

Since $R = K(x_1, \dots, x_m)$,

$$R(\xi) = K(x_1, \dots, x_m, \xi) = K(\xi)(x_1, \dots, x_m)$$

and hence $R(\xi)/K(\xi)$ is radical. This means that without loss of generality we may assume that K contains primitive n-roots of one. For example, if $R = K(x_1, \dots, x_m)$ and $x_i^{a_i} \in K(x_1, \dots, x_{i-1})$, then we may assume that K contains a primitive a_i-root of one. We proceed by induction on m. The case $m = 0$ is trivial. Assume that the claim holds for some $m \geq 0$. Let $L = K(x_1)$. Then L/K is a decomposition field of $X^{a_1} - x_1^{a_1}$, and hence L/K is a cyclic extension. Thus $\mathrm{Gal}(L/K)$ is cyclic (and hence, in particular, solvable). Let H be the subgroup that corresponds to L, that is $H = \mathrm{Gal}(R/L)$ (here we use Galois' correspondence). Then H is normal in $\mathrm{Gal}(R/K)$. Since $R = K(x_1, \dots, x_m) = L(x_2, \dots, x_m)$, R/L is radical and Galois. By the inductive hypothesis, $\mathrm{Gal}(R/L)$ is solvable. Since

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(R/K)/\mathrm{Gal}(R/L),$$

it follows that $\mathrm{Gal}(R/K)$ is solvable. $\square$

Definition 18.5. Let $f \in K[X]$ and E be a decomposition field of f over K. We say that f is **solvable by radicals** if there is a radical extension R/K such that $E \subseteq R$.

The general polynomial of degree two is solvable by radicals, as its Galois group is solvable (in fact, it is isomorphic to $\mathbb{S}_2$).

Exercise 18.6. Prove that $f = X^2 - s_1 X + s_2 \in \mathbb{Q}[X]$ is solvable by radicals.

Theorem 18.4 translates into the following result:

Exercise 18.7. If $f \in K[X]$ is solvable by radicals, then $\mathrm{Gal}(f, K)$ is solvable.

As a consequence, the general polynomial of degree $n \geq 5$ is not solvable by radicals, as its Galois group is isomorphic to $\mathbb{S}_5$.

Example 18.8. Let p be a prime number and $f = X^5 - 2pX + p \in \mathbb{Q}[X]$. We claim that f is not solvable by radicals.

By Gauss' theorem one proves that f has no rational roots.

Since $f(-1)f(1) < 0$ and $\deg f$ is odd, one proves that f has at least three real roots. Moreover, f has exactly three real roots, as $f' = 5X^4 - 2p$. Let $x_1, x_2 \in \mathbb{C} \setminus \mathbb{R}$ and $x_3, x_4, x_5 \in \mathbb{R}$ be the roots of f.

By Eisenstein's theorem, f is irreducible.

Let $E/\mathbb{Q}$ be a decomposition field of f. Then $\mathrm{Gal}(f, \mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to a subgroup G of $\mathbb{S}_5$. Since f is irreducible, 5 divides $[E : \mathbb{Q}] = |G|$. In particular, by Cauchy's theorem, G contains an element σ of order five. This element is a 5-cycle, so without loss of generality we may assume that $\sigma = (x_1x_2x_3x_4x_5)$. Note that $(x_1x_2) \in G$. Thus $G \simeq \mathbb{S}_5$ and hence G is not solvable.

Exercise 18.9. Let $f = X^6 + 2X^5 - 5X^4 + 9X^3 - 5X^2 + 2X + 1 \in \mathbb{Q}[X]$ is solvable by radicals.

Some solutions

6.1 Let $\{v_i : i \in I\}$ be a basis of V over K. For each $i \in I$ let $f_i : V \longrightarrow F$, $f_i(v_j) = \delta_{ij}$. Then $\{f_i : i \in I\}$ is linearly independent over F. In fact, let $\sum a_i f_i = 0$, where each $a_i \in F$. Then $a_i = 0$ for almost all i. If $j \in I$, then

$$0 = \left(\sum a_i f_i\right)(v_j) = \sum a_i f_i(v_j) = a_j.$$

Now assume that $\dim_K V = n$. Let $\{v_1, \dots, v_n\}$ be a basis of V over K. We claim that $\{f_1, \dots, f_n\}$ is a basis of $\mathrm{Hom}_K(V, F)$ over F. If $g \in \mathrm{Hom}_K(V, F)$, then $g = \sum g(v_i) f_i$. If $1 \leq k \leq n$, then

$$\left(\sum g(v_i) f_i\right)(v_k) = \sum g(v_i) f_i(v_k) = g(v_k).$$

6.4 We need to find a bijective map

$$\mathrm{Hom}(E/K, C/K) \longrightarrow \mathrm{Hom}(E/K, C_1/K).$$

If $\sigma \in \mathrm{Hom}(E/K, C/K)$, then $\theta^{-1}\sigma \in \mathrm{Hom}(E/K, C_1/K)$. If $\varphi \in \mathrm{Hom}(E/K, C_1/K)$, then $\theta\varphi \in \mathrm{Hom}(E/K, C/K)$. The maps $\sigma \mapsto \theta^{-1}\sigma$ and $\varphi \mapsto \theta\varphi$ are inverse to each other.

References

1. W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.
2. J. Rotman. *Galois theory*. Universitext. Springer-Verlag, New York, second edition, 1998.
3. I. Stewart. *Galois theory*. CRC Press, Boca Raton, FL, fourth edition, 2015.

Index