

Leandro Vendramin

Galois theory

Notes

Thursday 3rd February, 2022

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-hours lectures.

The material is somewhat standard. Basic texts on fields and Galois theory are for example [1]. . .

As usual, we also mention a set of great expository papers by Keith Conrad available at <https://kconrad.math.uconn.edu/blurbs/>. The notes are extremely well-written and are useful at every stage of a mathematical career.

This version was compiled on Thursday 3rd February, 2022 at 08:50.

Leandro Vendramin
Brussels, Belgium

Contents

1	1
References	13
Index	15

List of topics

§1	Fields	1
§2	Algebraic extensions	5
§3	Artin's theorem	10
§4	Decomposition fields	11

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.

$\text{xca}:\mathbb{Q}(i)$

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 $\mathbb{Z} \rightarrow R$, $m \mapsto m1$. 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 hence it is generated by some $t \in \mathbb{Z}$. 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 .

The following exercise is important.

Exercise 1.7. Prove that if K is a finite field, then $|K| = p^m$ for some prime number p and some $m \geq 1$.

Definition 1.8. 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 $K \rightarrow L$ is a field homomorphism, then K and L have the same characteristic.

Exercise 1.9. Let K be a field of characteristic p . Prove that $K \rightarrow K, x \mapsto x^{p^n}$, 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 $K \times E \rightarrow E, (\lambda, x) \mapsto \lambda x$.

Definition 1.10. 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 p a prime number.

Proposition 1.11. 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 $L = \{m1/n1 : m, n \in \mathbb{Z}, n \neq 0\}$. We claim that $K_0 = L$. Since $K_{\mathbb{Z}} \subseteq K_0$, it follows that $L \subseteq K_0$. Hence $L = K_0$, as L is a subfield of K . \square

Definition 1.12. Let E be a field and K be a subfield of E . Then E is an **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 1.13. 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 1.14. 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 $a + bx = 0$ 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 1.15. A basis of $\mathbb{Q}(\sqrt{2})$ over \mathbb{Q} is given by $\{1, \sqrt{2}\}$. Then $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Example 1.16. 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 1.17. Let K be a finite field. Then $|K| = p^m$ for some prime number p and some $m \geq 1$.

Proof. We know that the prime subfield 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

Definition 1.18. Let E be an extension of K . A **subextension** F of K is a subfield F of E that contains K , that is $K \subseteq F \subseteq E$.

Definition 1.19. Let E and E_1 be extensions over K . An extension **homomorphism** $E \rightarrow E_1$ is a field homomorphism $\sigma : E \rightarrow E_1$ such that $\sigma(x) = x$ for all $x \in K$.

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

$$\begin{array}{ccc} K & \xlongequal{\quad} & K \\ \downarrow & & \downarrow \\ E & \xrightarrow{\sigma} & E_1 \end{array}$$

We write $\text{Hom}(E/K, E_1/K)$ to denote the set of homomorphism $E \rightarrow E_1$ of extensions of K . Note that if $\sigma \in \text{Hom}(E/K, E_1/K)$, 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 1.20. The conjugation map $\mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$, is an endomorphism of \mathbb{C} as an extension over \mathbb{R} . Let $\varphi \in \text{Hom}(\mathbb{C}/\mathbb{R}, \mathbb{C}/\mathbb{R})$. 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 1.21. Prove that if K is a field and $\sigma: K \rightarrow K$ is a field homomorphism, then $\sigma \in \text{Hom}(K/K_0, K/K_0)$.

If E/K is an extension, then

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

is a group with composition.

Definition 1.22. Let E/K be an extension. The **Galois group** of E/K is the group $\text{Aut}(E/K)$ and it will be denoted by $\text{Gal}(E/K)$.

A typical example: $\text{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2$.

Example 1.23. Let $\theta = \sqrt[3]{2}$ and let $E = \{a+b\theta+c\theta^2 : a, b, c \in \mathbb{Q}\}$. Note that

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

In fact, if $abc \neq 0$, then $aX^2+bX+c \neq 0$ and thus $X^3-2 = q(X)(aX^2+bX+c) + r(X)$ for some polynomials $q(X) \in \mathbb{Q}[X]$ and $r(X) = eX+f \in \mathbb{Q}[X]$. Evaluate in θ to obtain that $r(\theta) = 0$ and hence $r(X) = 0$ in $\mathbb{Q}[X]$. This implies that aX^2+bX+c divides X^3-2 , a contradiction since X^3-2 is irreducible in $\mathbb{Q}[X]$.

Then E is an extension of \mathbb{Q} such that $[E:\mathbb{Q}] = 3$. We claim that $\text{Gal}(E/\mathbb{Q})$ is trivial. If $\sigma \in \text{Gal}(E/\mathbb{Q})$ 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 $\sigma = \text{id}$.

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

Example 1.25. The field $\mathbb{Q}(\sqrt{2})$ is precisely the extension of \mathbb{R}/\mathbb{Q} generated by $\sqrt{2}$.

§2 Algebraic extensions

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 **transcendent** over K .

If E/K is an extension, then

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

is the **algebraic closure** of K in E .

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 $X^2 + (z + \bar{z})X + |z|^2 \in \mathbb{R}[X]$.

If F/K is an algebraic extension and $x \in E$ is algebraic over K , then x is algebraic over E .

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.

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

Definition 2.5. Let E/K be an extension and $x \in E$ be an algebraic element. The monic polynomial that generates the kernel of $K[X] \rightarrow E$, $f \mapsto f(x)$, 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 2.6. Let E/K be an extension and $x \in E$.

1) If $g \in K[X]$ is such that $g(x) = 0$, then $f(x, K)$ divides g .

- 2) If $g(x) = 0$ and $g \neq 0$, then $\deg g \geq \text{gr } f(x, K)$.
 3) $f(x, K)$ is irreducible in $K[X]$.
 4) If $g(x) = 0$ and $g(X)$ is monic and irreducible, then $g = f(x, K)$.
 5) 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 . Now 2) follows from 1). To prove 3) note that if $f = gh$ for some $g, h \in K[X]$ such that $0 < \deg g, \deg h < \deg f$, then $f(x) = 0$ implies that either $g(x) = 0$ or $h(x) = 0$, a contradiction. 4) is trivial. Finally we prove 5). Since $f \in K[X] \subseteq F[X]$ and $f(x) = 0$, it follows from 3) that $f(x, F)$ divides f . \square

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

Example 2.7. 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 2.8. 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 K 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 $x = \sum_i \sum_j a_{ij} (f_j e_i)$. This means that $\{f_j e_i : i \in I, j \in J\}$ generates E as a K -vector space. Let us prove that $\{f_j e_i : i \in I, j \in J\}$ is linearly independent. If $\sum_i \sum_j a_{ij} (f_j e_i) = 0$ (finite sum) for some $a_{ij} \in K$, then

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

We state a lemma:

Lemma 2.9. 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 $\theta: A \rightarrow A, x \mapsto ax$. Clearly θ is an algebra homomorphism. 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 means that there exists $b \in A$ such that $1 = ab$. \square

Theorem 2.10. *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 $r = \sum_{i=0}^{m-1} a_i X^i$ for some $a_0, \dots, a_{m-1} \in K$. Thus $z = \sum_{i=0}^{m-1} a_i x^i$, 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). Let us prove that $K(x) \subseteq K[x]$. Since $x \neq 0$, $1/x \in K[x]$. There exists $a_0, \dots, a_n \in K$ such that $1/x = a_0 + a_1 x + \dots + a_n x^n$. Thus

$$a_n x^{n+1} + \dots + a_1 x^2 + a_0 x - 1 \neq 0$$

and x is a root of $a_n X^{n+1} + \dots + a_0 X - 1 \in K[X]$. \square

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

Corollary 2.11. *If E/K is finite, then E/K is algebraic.*

Proof. Let $n = [E : K]$ and $x \in E$. The set $\{1, x, \dots, x^n\}$ is linearly dependent, so there exist $a_0, \dots, a_n \in K$ not all zero such that $a_0 + a_1 x + \dots + a_n x^n = 0$. Thus x is a root of the non-zero polynomial $a_0 + a_1 X + \dots + a_n X^n \in K[X]$. \square

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

Corollary 2.12. *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 $K(x_1, \dots, x_n) = K[x_1, \dots, x_n]$.*

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,

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

Corollary 2.13. *Let $E = K(S)$. 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 corollary implies that $K(T)/K$ is algebraic and hence z is algebraic. \square

Corollary 2.14. *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 2.15. Let E/K be an extension. Prove that E/K is algebraic if and only if E/K is finite of finite type.

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

Proposition 2.16. *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. We know that if E/K is algebraic, then E/F and F/K are both algebraic. 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 . \square

Exercise 2.17. 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.

Exercise 2.18. 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 2.19. 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 2.20. *Let $\sigma : K \rightarrow L$ be a field homomorphism. Then there exists an extension E/K and a field isomorphism $\varphi : E \rightarrow L$ 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 $\theta: A \rightarrow L \setminus \sigma(K)$ is bijective, then let

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

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:

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

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 $x, y \in K$. \square

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

Theorem 2.21. *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 $\pi: K[X] \rightarrow L$ be the canonical map. Then L is a field. The field homomorphism $\bar{\sigma}: K \rightarrow L$, $a \mapsto \pi(aX^0)$. Let $g = \bar{\sigma}(f) \in L[X]$.

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

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

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

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

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 2.22. 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 2.23. *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 $f(x, K) = a \prod_{i=1}^n (X - \alpha_i)$ 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 $x \in K$. \square

§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} it is not.

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

Proof. Suppose 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 $\varphi: E \rightarrow C$, $z \mapsto \overline{\sigma}(g)(y)$.

The map φ is well-defined.

The map φ is a ring homomorphism. \square

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. \square

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

Proposition 4.5. 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 roots of f .

Proof.

□

References

1. J. Rotman. *Galois theory*. Universitext. Springer-Verlag, New York, second edition, 1998.

Index

Artin's theorem, 10

Subfield, 2