

Leandro Vendramin

# Galois theory

Notes

Wednesday 2<sup>nd</sup> March, 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 Wednesday 2<sup>nd</sup> March, 2022 at 16:20.

Leandro Vendramin  
Brussels, Belgium



# Contents

<b>1</b>	.....	1
<b>2</b>	.....	5
<b>3</b>	.....	11
<b>4</b>	.....	15
<b>5</b>	.....	19
<b>6</b>	.....	23
<b>7</b>	.....	27
<b>8</b>	.....	31
<b>Some solutions</b>	.....	33
<b>References</b>	.....	35
<b>Index</b>	.....	37



## List of topics

<b>§1</b>	<b>Fields</b> .....	<b>1</b>
<b>§2</b>	<b>Algebraic extensions</b> .....	<b>5</b>
<b>§3</b>	<b>Artin's theorem</b> .....	<b>13</b>
<b>§4</b>	<b>Decomposition fields</b> .....	<b>16</b>
<b>§5</b>	<b>Normal extensions</b> .....	<b>19</b>
<b>§7</b>	<b>Separable extensions</b> .....	<b>24</b>
<b>§8</b>	<b>Galois extensions</b> .....	<b>27</b>
<b>§9</b>	<b>Galois' correspondence</b> .....	<b>29</b>
<b>§10</b>	<b>The fundamental theorem of algebra</b> .....	<b>31</b>





# 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  $t \geq 0$ . 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  $K \rightarrow L$  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  $K \rightarrow K, x \mapsto x^{p^n}$ , 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 1.9.** 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  $p$  a prime number.

**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  $E = \{m/1/n : m, n \in \mathbb{Z}, n \neq 0\}$ . 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 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 1.12.** 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  $a + bx = 0$  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 1.14.** A basis of  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$  is given by  $\{1, \sqrt{2}\}$ . Then  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ .

**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 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 1.17.** 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 1.18.** 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  $\sigma$  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  $\mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$ , 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 1.20.** 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 1.21.** 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 1.22.** 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  $\text{Gal}(E/\mathbb{Q})$  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  $\sigma = \text{id}$ .

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

## Lecture 2

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  $\sqrt{2}$ .

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

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  $g \in K[X] \setminus \{0\}$  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:  $f(i, \mathbb{R}) = X^2 + 1$  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  $\alpha$  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  $F$  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  $x = \sum_i \sum_j a_{ij} (f_j e_i)$ . 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

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

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  $\theta$  is an algebra homomorphism. It is injective, since  $A$  is an integral domain. Since  $\dim_K A < \infty$ , it follows that  $\theta$  is an isomorphism. In particular,  $\theta(A) = A$ , which means that there exists  $b \in A$  such that  $1 = ab$ .  $\square$

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

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

is a subring of  $E$  that contains  $K$ . 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  $E$ . Clearly,  $K[x_1, \dots, x_n]$  is a domain and

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

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 an indeterminate. 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 algebra homomorphism  $K[\{X_i : i \in I\}] \rightarrow E$  such that  $X_i \mapsto x_i$  for all  $i \in I$ . The image is denoted by  $K[S]$ .

**Exercise 2.10.** Prove that  $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ .

**Theorem 2.11.** *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). 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

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

so  $x$  is a root of  $a_n X^{n+1} + \dots + a_0 X - 1 \in K[X] \setminus \{0\}$ .  $\square$

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

**Corollary 2.12.** *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 2.13.** *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 2.14.** *Let  $E = K(S)$ . Then  $E/K$  is algebraic if and only if  $x$  is algebraic over  $K$  for all  $x \in S$ .*



§2 Algebraic extensions

*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 2.15.** *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 2.16.** Let  $E/K$  be an extension of finite type. 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  $[\overline{\mathbb{Q}} : \mathbb{Q}]$ ?



## Lecture 3

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

**Proposition 2.17.** *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  $K$ . □

**Exercise 2.18.** 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 2.19.** 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 2.20.** 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 2.21.** 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 2.22.** 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 2.23.** 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  $\varphi$  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  $\sigma$  induces a ring homomorphism  $\overline{\sigma} : A[X] \rightarrow B[X]$ ,  $\sum_i a_i X^i \mapsto \sum \sigma(a_i) X^i$ .

**Theorem 2.24.** 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 reader should explain why). The field homomorphism  $\sigma : K \rightarrow L$ ,  $a \mapsto \pi(aX^0)$ . Let  $g = \overline{\sigma}(f) \in L[X]$ .

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

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

The previous lemma states that there exists an extension  $E/K$  and an isomorphism  $\varphi : E \rightarrow L$  such that  $\varphi|_K = \sigma$ . 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

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

### §3 Artin's theorem

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 2.25.** 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 2.26.** *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  $x \in K$ .  $\square$

### §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.

pro:Artin

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

The map  $\varphi$  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  $\varphi$  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  $(F, \tau)$ , where  $F$  is a subfield of  $E$  that contains  $K$  and  $\tau: F \rightarrow C$  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  $\tau$  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  $E_1(z)/K$ , let  $\rho: E_1(z) \rightarrow C$  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  $(E_1, \theta)$ .  $\square$

## 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  $\varphi: C \rightarrow C_1$ . 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

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

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

We now prove the existence. Let us assume that  $K$  admits an extension  $E/K$  with  $E$  algebraically closed. Let

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

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  $\alpha$  in  $E$ . In particular,  $\alpha$  is algebraic over  $F$  and hence  $\alpha$  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  $\alpha_j$  in  $F$  for all  $j$ . Let

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

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  $\sigma: K \rightarrow L$  be the composition  $K \hookrightarrow R \rightarrow R/M = L$ . 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

$$E_1 \subseteq E_2 \subseteq \dots$$

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  $E_{r+1} \subseteq E$ .  $\square$

## §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  $\omega$  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.* 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  $F = E$ .  $\square$

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

**Theorem 4.6.** *Let  $f \in K[X]$ . 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  $\varphi \in \text{Hom}(E_1/K, C/K)$  such that  $\varphi|_K$  is the identity. Factorize  $f$  linearly in  $E_1[X]$  and apply  $\bar{\varphi}$ :

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

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  $\varphi(E_1) = E$ .  $\square$

**Exercise 4.7.** If  $E/K$  is finite and  $\varphi \in \text{Hom}(E/K, E/K)$ , then  $\varphi$  is an isomorphism.

Let  $C$  be an algebraic closure of  $K$  and  $G = \text{Gal}(C/K)$ . 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 4.8.** *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  $G = \text{Gal}(C/K)$ . 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

$$\begin{aligned} 0 &= \sigma \left( x^n + \sum_{i=0}^{n-1} a_i x^i \right) = \sigma(x)^n + \sum_{i=0}^{n-1} \sigma(a_i) \sigma(x)^i \\ &= \sigma(x)^n + \sum_{i=0}^{n-1} a_i \sigma(x)^i = y^n + \sum_{i=0}^{n-1} a_i y^i. \end{aligned}$$

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

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

$$\varphi: K[x] \rightarrow K[y], \quad h(x) \mapsto h(y).$$

Let us show that the map  $\varphi$  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

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

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

A straightforward calculation shows that  $\varphi$  is a field homomorphism such that  $\varphi|_K = \text{id}$ , so  $\varphi$  is an extension homomorphism such that  $\varphi(x) = y$ . There exists  $\sigma \in \text{Hom}(C/K, C/K)$  such that  $\sigma|_{K[x]} = \varphi$ . Since  $\sigma$  is a bijection,  $\sigma(x) = \varphi(x) = y$  and hence  $O_G(x) = O_G(y)$ .  $\square$

**Proposition 4.9.** *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  $\sigma \in \text{Gal}(C/K)$ . 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  $m_x = m_y$ .  $\square$

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 clearly not true if  $f$  is not irreducible. Find an example.

**Definition 4.10.** 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 the  $\{f_i : i \in I\}$  is an extension  $E/K$  such that every  $f_i$  factorizes linearly in  $E[X]$  and if  $F/K$  is a subextension of  $E/K$  such that every  $f_i$  factorizes linearly in  $F[X]$ , then  $F = E$ .

**Exercise 4.11.** 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 4.12.** 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 4.13.** Prove that there exists a decomposition field of  $\{f_i : i \in I\}$  and it is unique up to extension isomorphism.

## Lecture 5

### §5. Normal extensions

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

*Proof.* Let  $x \in E$  and  $C$  be an algebraic closure of  $K$  that contains  $E$ . There exists  $\varphi: C \rightarrow C$  such that  $\varphi|_E = \sigma$ . Thus  $\varphi|_K = \sigma|_K = \text{id}_K$ . Let  $G = \text{Gal}(C/K)$ . 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, as

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

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  $\sigma$ .  $\square$

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

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. In fact, every extension generated by algebraic elements of degree two is normal.

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

The following result is useful but technical, that is why we leave the proof as an exercise.

**Exercise 5.6.** Prove that the previous definition depends 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  $\sigma \in \text{Gal}(C/K)$ . Since  $E/K$  is normal,  $\sigma|_E : E \rightarrow C$  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,  $E/K$  normal and  $F/K$  normal do not imply  $E/F$  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  $y \in O_{\text{Gal}(C/K)}(x)$ . 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  $y \in O_{\text{Gal}(E/K)}(x)$ .

**Proposition 5.9.** *Let  $K \subseteq F \subseteq E$  be a tower of fields. If  $F/K$  is normal, then  $EF/E$  is normal.*

*Proof.* Let  $C$  be an algebraic closure of  $E$  containing  $EF$ . Let  $\sigma \in \text{Hom}(EF/E, C/E)$ . 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  $\sigma|_F \in \text{Hom}(F/K, \overline{K}/K)$ , 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  $f_1, \dots, f_m \in F$ . Then

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

**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  $G = \text{Gal}(E/K)$ . 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  $\sigma \in \text{Hom}(C/K, E/K)$ . 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  $\sigma(E) \subseteq E$ . □

## §6. Dedekind's theorem

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

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

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

xca:dim

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

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  $\text{Hom}(E/K, F/K)$ , i.e. a family of extension homomorphisms. Assume that  $\varphi_i \neq \varphi_j$  if  $i \neq j$ . Then the subset  $\{\varphi_i : i \in I\} \subseteq \text{Hom}_K(E, F)$  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  $\sum_{i=1}^n a_i \varphi_i = 0$  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

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

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

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

Thus

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

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.  $\square$

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

**Exercise 6.3.** Prove the following statements:

- 1)  $\gamma(E/K, F/K) \leq \dim_F \text{Hom}_K(E, F)$ .
- 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.

xc a : gamma\_C

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

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

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

*Proof.* If  $\sigma \in \text{Hom}(K(x)/K, C/K)$ , 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  $\tau|_{K(x)} \in \text{Hom}(K(x)/K, C/K)$  and  $\tau|_{K(x)}(x) = y$ . In particular,  $\gamma(K(x)/K)$  divides  $\deg(x, K)$ .  $\square$

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

## Lecture 6

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

**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  $G = \text{Gal}(E/F)$ . Let  $C$  be an algebraic closure of  $K$  containing  $E$ . The map

$$\lambda: \text{Hom}(E/K, C/K) \rightarrow \text{Hom}(F/K, C/K), \quad \sigma \mapsto \sigma|_F,$$

is surjective. If  $\varphi \in \text{Hom}(F/K, C/K)$ , then

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

Assume that  $\sigma|_F = \varphi$ . Then  $\sigma(x)$  is a root of  $\bar{\varphi}(f)$  in  $C$ , as

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

So there is an injective map from  $\lambda^{-1}(\{\varphi\})$  to the set  $R_\varphi$  of roots of  $\bar{\varphi}(f)$  in  $C$ . Conversely, if  $y \in R_\varphi$  and  $z \in E$ , say  $z = h(x)$  for some  $h \in F[X]$ , let  $\sigma_y(z) = \bar{\varphi}(h)(y)$ .

This is well-defined: if  $z = t(x)$  for some  $t \in F[X]$ , then, since  $(t - h)(x) = 0$ , it follows that  $f$  divides  $h - t$ . This implies that  $\bar{\varphi}(f)$  divides  $\bar{\varphi}(h) - \bar{\varphi}(t)$  and hence  $\bar{\varphi}(h)(y) = \bar{\varphi}(t)(y)$ . Since  $\sigma_y|_F = \varphi$ ,  $\sigma_y \in \lambda^{-1}(\varphi)$ . Moreover,  $\sigma_y(x) = y$ .

Since the map is surjective,  $|\lambda^{-1}(\varphi)| = |R_\varphi|$ .

We claim that  $\phi^{-1}(R_\varphi) = O_G(x)$ . Let us first prove  $\phi^{-1}(R_\varphi) \subseteq O_G(x)$ . There exists  $\phi \in G$  such that  $\phi|_F = \varphi$ . If  $y \in R_\varphi$ , then

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

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

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

Hence  $|R_\varphi| = |\phi^{-1}(R_\varphi)| = |O_G(x)|$  and therefore  $|\lambda^{-1}(\{\varphi\})| = |O_G(x)|$  for all  $\varphi$ . This implies that  $\gamma(E/K) = \gamma(F/K)|O_G(x)| = \gamma(F/K)\gamma(F(x)/F)$ .

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 previous case implies that  $\gamma(E/F) = \gamma(E/L)\gamma(L/F)$ . By the inductive assumption,  $\gamma(L/K) = \gamma(L/F)\gamma(F/K)$ . 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.  $\square$

## §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  $G = \text{Gal}(C/K)$  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  $\text{Gal}(E/\mathbb{Q}) \simeq C_2 \times C_2$ . The extension  $E/\mathbb{Q}$  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  $[E : \mathbb{Q}] = 8 = |\text{Gal}(E/\mathbb{Q})|$ .

Let us compute  $\text{Gal}(E/\mathbb{Q})$ . If  $\sigma \in \text{Gal}(E/\mathbb{Q})$ , 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

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

It follows that  $\text{Gal}(E/\mathbb{Q})$  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 proceed by induction.

xca:separable1

**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.

xca:separable2

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

If  $E/K$  is algebraic, then  $F = \{x \in E : x \text{ is separable over } K\}$  is a subfield of  $E$  that contains  $K$ . Note that  $F = K(F)$ , as  $K(F)$  is separable because it is generated by separable elements. Note that  $F/K$  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 may assume that  $K = K(x, y)$  and let  $n = [E : K]$ . Let  $C$  be an algebraic closure of  $K$  containing  $E$ . Assume that  $\text{Hom}(E/K, C/K) = \{\sigma_1, \dots, \sigma_n\}$ . Let

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

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

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

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 may assume that  $K$  is infinite, otherwise the result is trivial. Let us assume that  $E = K(x)$ . If  $F/K$  is a subextension of  $E/K$ , let  $g = f(x, F)$ . Then  $g$  divides  $f(x, K)$ . So we constructed a map that assigns to every subextension  $F/K$  a (monic) divisor of  $f(x, K)$  in  $E[X]$ . Let us show that  $g$  completely determines  $F/K$ . Let  $F_0/K$  be the subextension generated by the coefficients of  $g$ . Then  $F_0 \subseteq F$  and  $g$  is irreducible in  $F_0[X]$ . Thus

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

and hence  $F = F_0$ . This means that the assignment is injective and therefore there are finitely many fields between  $K$  and  $E$ .

Let us prove the converse. 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  $y \in L$ . Since  $K \subseteq L$ , it follows that  $x \in L$  and therefore  $L = E$ .  $\square$

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

## Lecture 7

### §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  $S \subseteq \text{Gal}(E/K)$  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  $G = \text{Gal}(E/K)$ . 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  $G = \text{Gal}(E/K)$ . Let  $F = {}^G E$ . Prove that  $\text{Gal}(E/F) = G$  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  $G = \text{Gal}(E/K)$ . Let us first assume that  $E/K$  is Galois. Let  $x \in E$  and  $f_x = \prod_{y \in O_G(x)} (X - y) \in E[X]$ . If  $\varphi \in G$ , then  $\overline{\varphi}(f_x) = \prod_{y \in O_G(x)} (X - \varphi(y)) \dots$  (pag70)  $\square$

**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.*  $\square$

In the previous case,  $\text{Gal}(E/K)$  is known as the **Galois group** of the polynomial  $f$ . The notation is  $\text{Gal}(f, K)$ .

thm:ArtinGalois

**Theorem 8.10 (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  $\text{Gal}(E/K) = G$ .

Before proving the theorem, we need a lemma.

**Lemma 8.11.** 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  $\deg(z, K) \leq \deg(y, K)$ , it follows that  $\deg(z, K) = \deg(y, K)$  and 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 8.10.* Note that  $G \subseteq \text{Gal}(E/K)$ . Let  $x \in E$  and

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

Since  $f_x \in K[X]$ , it follows that  $E/K$  is normal and separable, 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  $|G(E/K)| = |G|$ .  $\square$

## §9. Galois' correspondence

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

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

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



## Lecture 8

### §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  $G = \text{Gal}(L/\mathbb{R})$ . 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. In particular,  $|\text{Gal}(L/\mathbb{C})| = 2^{m-1}$ . If  $m > 1$ , let  $U$  be a subgroup of  $\text{Gal}(L/\mathbb{C})$  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  $E = \mathbb{C}$ .  $\square$





## Some solutions

**6.1** Let  $\{v_i : i \in I\}$  be a basis of  $V$  over  $K$ . For each  $i \in I$  let  $f_i : V \rightarrow F$ ,  $f_i(v_j) = \delta_{ij}$ . 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  $\text{Hom}_K(V, F)$  over  $F$ . If  $g \in \text{Hom}_K(V, F)$ , 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

$$\text{Hom}(E/K, C/K) \rightarrow \text{Hom}(E/K, C_1/K).$$

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



## References

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



# Index

Artin's theorem, 15, 28

Decomposition field, 16, 18

Dedekind's theorem, 21

Extension

Galois, 27

Galois' theorem, 29

Subfield, 2