

Leandro Vendramin

Galois theory

Notes

Wednesday 10th November, 2021

Contents

1	1
References	7

List of topics

§1	Fields	1
-----------	---------------------	----------

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 .

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 1.7. 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 1.8. 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 1.9. Let K be a field. The following statements hold:

- 1) K contains a unique prime field, it is known as the **prime subfield** K_0 of K .
- 2) Either $K_0 \simeq \mathbb{Q}$ or $K_0 \simeq \mathbb{Z}/p$ for some prime number 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 $L = L_1$.

Suppose that K is of characteristic $p > 0$. . . □

Definition 1.10. 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 1.11. 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 1.12. 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 1.13. 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 1.14. 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 1.15. *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 1.16. 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 1.17. 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 1.18. 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 1.19. 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 1.20. 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 1.21. 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 1.22. If $\{e_1, \dots, e_n\}$ is a basis of E over K , then $E = K(e_1, \dots, e_n)$.

Example 1.23. 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 $K(S) \subseteq K(T)$.

Definition 1.24. 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 1.25. 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 1.26. \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 1.27. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 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 $K[X] \rightarrow E$, $f(X) \mapsto f(x)$, is not injective. In particular, its kernel is a non-zero ideal and hence it is generated by a monic polynomial $f(X)$. This polynomial 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 $\deg f(x, K)$.

Proposition 1.28. 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 $\deg g \geq \deg f(x, K)$.
- 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.

□

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

Example 1.29. 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 $g = X^4 - 10X^2 + 1$. The roots of g are $\sqrt{2} + \sqrt{3}$, $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$ and $-\sqrt{2} - \sqrt{3}$. g is irreducible [?]

Proposition 1.30. 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

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

Proposition 1.31. *Let E/K be an extension and $x \in E$. 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. \square

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

Corollary 1.32. *Every finite extension is algebraic.*

Corollary 1.33. *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. \square

Corollary 1.34. *Let $E = K(S)$. Then E/K is algebraic if and only if x is algebraic over K for all $x \in S$.*

Proof. \square

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. \square

Corollary 1.35. *E/K is algebraic if and only if E/K is finite.*

References