Field Extensions and Elliptic Curves

Sebastiano Tronto

Bordeaux, 2019-10-19

Field Extensions

- Let K be any field (e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_2$...)

Field Extensions

- Let K be any field (e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_2$...)
- A field $L \supseteq K$ is called an **extension** of K (notation: $L \mid K$)

Field Extensions

- Let K be any field (e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_2$...)
- A field $L \supseteq K$ is called an **extension** of K (notation: $L \mid K$)
- If $L \mid K$ then L is a K-vector space ($[L : K] := \dim_K L$)

Field Extensions

- Let K be any field (e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_2$...)
- A field $L \supseteq K$ is called an **extension** of K (notation: $L \mid K$)
- If $L \mid K$ then L is a K-vector space ($[L : K] := \dim_K L$)
- Examples: $[\mathbb{C} : \mathbb{R}] = 2$ (basis $\{1, i\}$) and $[\mathbb{R} : \mathbb{Q}] = +\infty$

- If $L \mid K$ and $a_1, \ldots, a_n \in L$, we denote by $K(a_1, \ldots, a_n)$ the smallest subfield of L containing K and $a_1, \ldots, a_n$.

Field Extensions

- If $L \mid K$ and $a_1, \ldots, a_n \in L$, we denote by $K(a_1, \ldots, a_n)$ the smallest subfield of L containing K and $a_1, \ldots, a_n$.
- Example ($K = \mathbb{Q}$, $L = \mathbb{R}$, $a_1 = \sqrt{3}$):

$$\mathbb{Q}(\sqrt{3}) = \left\{ f(\sqrt{3}) \mid f(X) \in \mathbb{Q}[X] \right\}$$

Field Extensions

- If $L \mid K$ and $a_1, \ldots, a_n \in L$, we denote by $K(a_1, \ldots, a_n)$ the smallest subfield of L containing K and $a_1, \ldots, a_n$.
- Example ($K = \mathbb{Q}$, $L = \mathbb{R}$, $a_1 = \sqrt{3}$):

$$\mathbb{Q}(\sqrt{3}) = \left\{ f(\sqrt{3}) \mid f(X) \in \mathbb{Q}[X] \right\} =$$
$$= \left\{ a + b\sqrt{3} \mid a, b \in \mathbb{Q} \right\} \subseteq \mathbb{R}$$

Field Extensions

- If $L \mid K$ and $a_1, \dots, a_n \in L$, we denote by $K(a_1, \dots, a_n)$ the smallest subfield of L containing K and $a_1, \dots, a_n$.
- Example ($K = \mathbb{Q}$, $L = \mathbb{R}$, $a_1 = \sqrt{3}$):

$$\mathbb{Q}(\sqrt{3}) = \left\{ f(\sqrt{3}) \mid f(X) \in \mathbb{Q}[X] \right\} = \\ = \left\{ a + b\sqrt{3} \mid a, b \in \mathbb{Q} \right\} \subseteq \mathbb{R}$$

- Application: find integer solutions of $x^2 - 3y^2 = 1$

Galois Theory

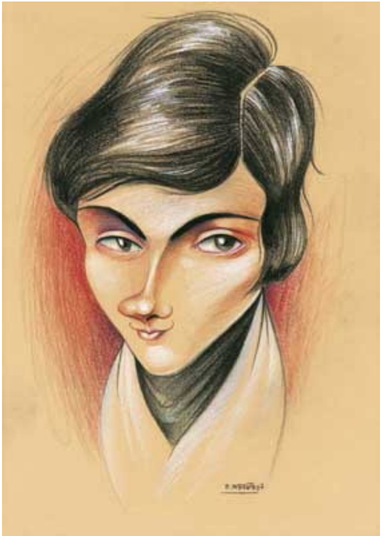


Figure: Évariste Galois

Let $L \mid K$, assume $[L : K]$ finite.

- **Separability**: $L \mid K$ is separable if the minimal polynomials of elements of L have distinct roots.
  Example: if char $K = 0$ or K is finite $L \mid K$ is separable.
- **Normality**: $L \mid K$ is normal if every irreducible $f(x) \in K[x]$ that has a root in L has **all** its roots in L.
  Example: splitting fields.

Let $L \mid K$ be normal and separable.

Galois Theory

Let $L \mid K$ be normal and separable.

- The **Galois group** of $L \mid K$ is

$$\mathrm{Gal}(L \mid K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \, \forall \, x \in K\}$$

Galois Theory

Let $L \mid K$ be normal and separable.

- The **Galois group** of $L \mid K$ is

$$\mathrm{Gal}(L \mid K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \, \forall \, x \in K\}$$

- $\# \mathrm{Gal}(L \mid K) = [L : K]$

Galois Theory

Let $L \mid K$ be normal and separable.

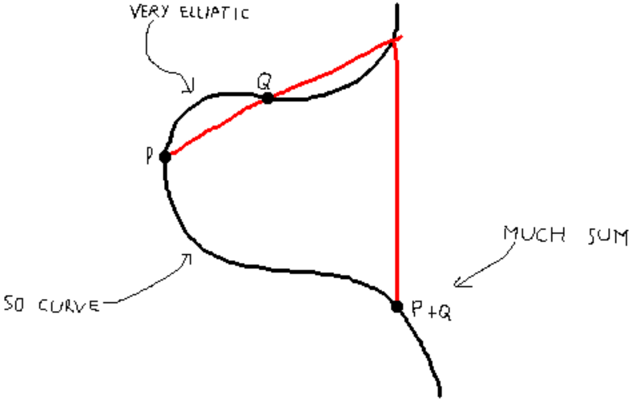
- The **Galois group** of $L \mid K$ is

$$\mathrm{Gal}(L \mid K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \,\forall\, x \in K\}$$

- $\# \mathrm{Gal}(L \mid K) = [L : K]$
- Galois correspondence

$$\begin{aligned} \{\text{extensions } K \subseteq F \subseteq L\} &\overset{1:1}{\longleftrightarrow} \{\text{subgroups } H \leq \mathrm{Gal}(L \mid K)\} \\ F &\longmapsto \mathrm{Gal}(L \mid F) \\ \text{fixed field of } H &\longleftarrow\!\shortmid\; H \end{aligned}$$

Elliptic Curves



- An elliptic curve over a field K is defined by an equation

$$Y^2 = X^3 + AX + B \qquad A, B \in K,\ 4A^3 \neq -27B^2$$

$+$ a point at infinity o.

- An elliptic curve over a field K is defined by an equation

$$Y^2 = X^3 + AX + B \qquad A, B \in K,\ 4A^3 \neq -27B^2$$

  $+$ a point at infinity o.
- For any $L \mid K$, we can consider the set of L-**points**

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + Ax + B\} \cup \{o\}$$

Elliptic Curves

- An elliptic curve over a field K is defined by an equation

$$Y^2 = X^3 + AX + B \qquad A, B \in K,\ 4A^3 \neq -27B^2$$

  $+$ a point at infinity o.

- For any $L \mid K$, we can consider the set of L-**points**

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + Ax + B\} \cup \{o\}$$

- There is an operation on $E(L)$ such that $(E(L), +)$ is a group

Elliptic Curves

- An elliptic curve over a field K is defined by an equation

$$Y^2 = X^3 + AX + B \qquad A, B \in K,\ 4A^3 \neq -27B^2$$

  $+$ a point at infinity o.
- For any $L \mid K$, we can consider the set of L-**points**

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + Ax + B\} \cup \{o\}$$

- There is an operation on $E(L)$ such that $(E(L), +)$ is a group
- Applications in Cryptography

Field Extensions from Elliptic Curves

Fix an elliptic curve E over K; let $\overline{K}$ be a separable closure of K.

Field Extensions from Elliptic Curves

Fix an elliptic curve E over K; let $\overline{K}$ be a separable closure of K.

- For points $P_1 = (x_1, y_1), \dots, P_n = (x_n, y_n) \in E(\overline{K})$ let

  $$K(P_1, \dots, P_n) := K(x_1, y_1, \dots, x_n, y_n)$$

  which is an extension of K.

Fix an elliptic curve E over K; let $\overline{K}$ be a separable closure of K.

- For points $P_1 = (x_1, y_1), \dots, P_n = (x_n, y_n) \in E(\overline{K})$ let

$$K(P_1, \dots, P_n) := K(x_1, y_1, \dots, x_n, y_n)$$

  which is an extension of K.
- Nicer definition: $K(P_1, \dots, P_n)$ is the subfield of $\overline{K}$ fixed by

$$\left\{\sigma \in \mathrm{Gal}(\overline{K} \mid K) \mid \sigma(P_i) = P_i \text{ for } i = 1, \dots, n\right\}$$

Torsion Fields

Assume $\operatorname{char} K \nmid n$.

Torsion Fields

Assume char $K \nmid n$.

- Let $\{P_1, \ldots, P_{2n}\} = E(\overline{K})[n]$ be the points of order n.

Torsion Fields

Assume char $K \nmid n$.

- Let $\{P_1, \ldots, P_{2n}\} = E(\overline{K})[n]$ be the points of order n. $K(E[n]) = K(P_1, \ldots, P_{2n})$ is called n-**th torsion field of** E.

Assume char $K \nmid n$.

- Let $\{P_1, \dots, P_{2n}\} = E(\overline{K})[n]$ be the points of order n. $K(E[n]) = K(P_1, \dots, P_{2n})$ is called n**-th torsion field of** E. It is a normal and separable extension of K.

Assume char $K \nmid n$.

- Let $\{P_1, \dots, P_{2n}\} = E(\overline{K})[n]$ be the points of order n. $K(E[n]) = K(P_1, \dots, P_{2n})$ is called n-**th torsion field of** E. It is a normal and separable extension of K.
- The action of $\mathrm{Gal}(K(E[n]) \mid K)$ on $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ gives a **Galois representation**

$$\rho_n : \mathrm{Gal}(K(E[n]) \mid K) \hookrightarrow \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

Kummer Theory

Figure: Ernst Kummer

Assume $\operatorname{char} K \nmid n$, let $a \in K^\times$ not a root of unity.

Classic Kummer Theory

Assume char $K \nmid n$, let $a \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^n - a$ (adjoin to K all possible n-th roots of a).

Classic Kummer Theory

Assume char $K \nmid n$, let $a \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^n - a$ (adjoin to K all possible n-th roots of a).
- L contains the n-th cyclotomic extension $K(\zeta_n)$.

Classic Kummer Theory

Assume char $K \nmid n$, let $a \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^n - a$ (adjoin to K all possible n-th roots of a).
- L contains the n-th cyclotomic extension $K(\zeta_n)$.
- $L \mid K$ is normal and separable.

Classic Kummer Theory

Assume $\operatorname{char} K \nmid n$, let $a \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^n - a$ (adjoin to K all possible n-th roots of a).
- L contains the n-th cyclotomic extension $K(\zeta_n)$.
- $L \mid K$ is normal and separable.
- One can e.g. compute the degree $[L : K(\zeta_n)]$.

E elliptic curve over K, char $K \nmid n$, let $P \in E(K)$ not torsion.

E elliptic curve over K, char $K \nmid n$, let $P \in E(K)$ not torsion.

- There are $2n$ points $Q_1, \ldots, Q_{2n} \in E(\overline{K})$ such that $nQ_i = P$ (notation: $n^{-1}P := \{Q_1, \ldots, Q_{2n}\}$.)

E elliptic curve over K, char $K \nmid n$, let $P \in E(K)$ not torsion.

- There are $2n$ points $Q_1, \ldots, Q_{2n} \in E(\overline{K})$ such that $nQ_i = P$ (notation: $n^{-1}P := \{Q_1, \ldots, Q_{2n}\}$.)
- Consider $L = K(Q_1, \ldots, Q_{2n})$.

E elliptic curve over K, char $K \nmid n$, let $P \in E(K)$ not torsion.

- There are $2n$ points $Q_1, \dots, Q_{2n} \in E(\overline{K})$ such that $nQ_i = P$ (notation: $n^{-1}P := \{Q_1, \dots, Q_{2n}\}$.)
- Consider $L = K(Q_1, \dots, Q_{2n})$.
- $L \mid K$ is normal and separable.

Kummer Theory for Elliptic Curves

E elliptic curve over K, char $K \nmid n$, let $P \in E(K)$ not torsion.

- There are $2n$ points $Q_1, \ldots, Q_{2n} \in E(\overline{K})$ such that $nQ_i = P$ (notation: $n^{-1}P := \{Q_1, \ldots, Q_{2n}\}$.)
- Consider $L = K(Q_1, \ldots, Q_{2n})$.
- $L \mid K$ is normal and separable.
- L contains the n-th torsion field $K(E[n])$.

Let K be a finite extension of $\mathbb{Q}$ and $P \in E(K)$ of infinite order. Assume that E does not have complex multiplication over K.

Let K be a finite extension of $\mathbb{Q}$ and $P \in E(K)$ of infinite order. Assume that E does not have complex multiplication over K.

Theorem (joint with Davide Lombardo)

There is an explicit constant C, depending only on P and on the torsion Galois representations associated to E such that

$$\frac{n^2}{[K(n^{-1}P) : K(E[n])]} \quad \textit{divides} \quad C$$

for all $n \geq 1$.

Thank you for your attention