Irreducibility and Rational Points
Lecture 2. Rational Points

Arno Fehm
(Universität Konstanz)

French-German Summer School
Galois Theory and Number Theory
Konstanz, July 18-24 2015

1. Algebraic curves

Definition

A K-**curve** is a (geometrically irreducible) 1-dimensional K-variety.

1. Algebraic curves

Definition

A K-**curve** is a (geometrically irreducible) 1-dimensional K-variety.

Remark

Every K-curve has a smooth projective model, unique up to isomorphism.

1. Algebraic curves

Definition

A K-**curve** is a (geometrically irreducible) 1-dimensional K-variety.

Remark

Every K-curve has a smooth projective model, unique up to isomorphism.

Definition

Let C be a smooth projective K-curve. We define

- $\mathrm{Div}(C)$, the group of divisors on C
- $\mathrm{Pic}^0(C)$, divisors of degree 0 modulo principal divisors
- $\mathcal{L}(D) = \{f \in \overline{K}(C) : (f) \geq -D\}$, the Riemann-Roch space
- $g_C = \dim(\Omega^1_C)$, the genus of C

1. Algebraic curves

Theorem (Riemann-Roch)

Let $W \in \mathrm{Div}(C)$ *be a canonical divisor. Then for any* $D \in \mathrm{Div}(C)$,

$$\dim(\mathcal{L}(D)) = 1 + \deg(D) - g_C + \dim(\mathcal{L}(W - D)).$$

Theorem (Plücker formula)

For $C : f(x, y) = 0$ a smooth projective plane curve of degree $d = \deg(f)$,

$$g_C = \frac{(d-1)(d-2)}{2}.$$

1. Algebraic curves

Theorem (Plücker formula)

For $C : f(x,y) = 0$ a smooth projective plane curve of degree $d = \deg(f)$,

$$g_C = \frac{(d-1)(d-2)}{2}.$$

Remark

A morphism $f : C_1 \to C_0$ of smooth projective K-curves is either constant or of finite degree $\deg(f) = d$, in which case all fibers are finite, and almost all of cardinality d.

1. Algebraic curves

Theorem (Plücker formula)

For $C : f(x, y) = 0$ a smooth projective plane curve of degree $d = \deg(f)$,

$$g_C = \frac{(d-1)(d-2)}{2}.$$

Remark

A morphism $f : C_1 \to C_0$ of smooth projective K-curves is either constant or of finite degree $\deg(f) = d$, in which case all fibers are finite, and almost all of cardinality d.

Theorem (Riemann-Hurwitz formula)

For $f : C_1 \to C_0$ non-constant,

$$2g_{C_1} - 2 = \deg(f) \cdot (2g_{C_0} - 2) + \sum_{P \in C_1} (e_P - 1).$$

Example ($g_C = 0$)

1. Algebraic curves

Example ($g_C = 0$)

- $C(K) \neq \emptyset \Leftrightarrow C \cong \mathbb{P}^1$

1. Algebraic curves

Example ($g_C = 0$)

- $C(K) \neq \emptyset \Leftrightarrow C \cong \mathbb{P}^1$
- $C(K) = \emptyset \Leftrightarrow C$ is a nontrivial twist of $\mathbb{P}^1$, e.g. $C : x^2 + y^2 + 1 = 0$ over $K = \mathbb{Q}$

1. Algebraic curves

Example ($g_C = 0$)

- $C(K) \neq \emptyset \Leftrightarrow C \cong \mathbb{P}^1$
- $C(K) = \emptyset \Leftrightarrow C$ is a nontrivial twist of $\mathbb{P}^1$,
  e.g. $C : x^2 + y^2 + 1 = 0$ over $K = \mathbb{Q}$
- So, for K a number field, either $C(K) = \emptyset$ or $|C(K)| = \infty$.

1. Algebraic curves

Example ($g_C = 0$)

- $C(K) \neq \emptyset \Leftrightarrow C \cong \mathbb{P}^1$
- $C(K) = \emptyset \Leftrightarrow C$ is a nontrivial twist of $\mathbb{P}^1$, e.g. $C : x^2 + y^2 + 1 = 0$ over $K = \mathbb{Q}$
- So, for K a number field, either $C(K) = \emptyset$ or $|C(K)| = \infty$.

Corollary (Lüroth's theorem)

For $f : C_1 \to C_0$ non-constant, if C_1 is rational, then C_0 is rational. In other words, unirational curves are rational.

(A K-variety V is *rational* if it is birationally equivalent to $\mathbb{P}^n$, and *unirational* if there is a dominant rational map from $\mathbb{P}^n$ to V.)

1. Algebraic curves

Example ($g_C > 1$)

e.g.

$$C : x^n + y^n = 1, \quad n \geq 4$$

1. Algebraic curves

Example ($g_C > 1$)

e.g.

$$C : x^n + y^n = 1, \quad n \geq 4$$

Theorem (Mordell Conjecture, Falting's theorem)

For K a number field and $g_C > 1$, $|C(K)| < \infty$.

Example ($g_C = 1$)

e.g.

$$C : x^3 + y^3 = 1.$$

Example ($g_C = 1$)

e.g.

$$C : x^3 + y^3 = 1.$$

$C(K) \neq \emptyset \Leftrightarrow C$ is an elliptic curve, isomorphic to a plane projective curve

$$E : y^2 = x^3 + ax + b, \quad \Delta = 4a^3 + 27b^2 \neq 0.$$

Example ($g_C = 1$)

e.g.

$$C : x^3 + y^3 = 1.$$

$C(K) \neq \emptyset \Leftrightarrow C$ is an elliptic curve, isomorphic to a plane projective curve

$$E : y^2 = x^3 + ax + b, \quad \Delta = 4a^3 + 27b^2 \neq 0.$$

Remark

E has one point at infinity: $O_E = [0 : 1 : 0]$. The map $E \to \mathrm{Pic}^0(E)$, $P \mapsto [P - O_E]$, is bijective and induces an abelian group law on E, geometrically given by line sections.

Remark

For $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, *so*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2, \quad m \in \mathbb{N},$$

Remark

For $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, *so*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2, \quad m \in \mathbb{N},$$

e.g.

$$E[2] = \{O_E\} \cup \{(x,0) : x^3 + ax + b = 0\}.$$

Remark

For $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, *so*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2, \quad m \in \mathbb{N},$$

e.g.

$$E[2] = \{O_E\} \cup \{(x,0) : x^3 + ax + b = 0\}.$$

Theorem (Mordell–Weil)

For K *a number field and* $E|K$ *an elliptic curve,*

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\mathrm{tor}}$$

is finitely generated.