Faltings's Theorem and Isolated Points

Kenji Terao

July 30, 2024

Faltings's theorem

Theorem (Faltings, 1983)

Let K be a number field, and let C be a non-singular algebraic curve defined over K of genus $g \geq 2$. Then $C(K)$ is finite.

Faltings's theorem

Theorem (Faltings, 1983)

Let K be a number field, and let C be a non-singular algebraic curve defined over K of genus $g \geq 2$. Then $C(K)$ is finite.

Theorem (Faltings, 1991)

Let K be a number field, A an abelian variety defined over K, and $X \subset A$ a closed subvariety. Then there exist finitely many translates $X_i = x_i + B_i$ of abelian subvarieties $B_i \subset A$ such that $X_i \subset X$, and

$$X(K) = \bigcup_{i=1}^{n} X_i(K).$$

Jacobians

Let K be a number field, C/K be a non-singular algebraic curve of genus g, and let $x \in C(K)$.

Jacobians

Let K be a number field, C/K be a non-singular algebraic curve of genus g, and let $x \in C(K)$.

Let J_C be the Jacobian of C. This is a g-dimensional abelian variety defined over K parametrizing degree 0 divisors on C up to linear equivalence:

$$J_C(L) = \{L\text{-rational degree 0 divisors on } C\}/\sim,$$

for all field extensions L/K.

Jacobians

Let K be a number field, C/K be a non-singular algebraic curve of genus g, and let $x \in C(K)$.

Let J_C be the Jacobian of C. This is a g-dimensional abelian variety defined over K parametrizing degree 0 divisors on C up to linear equivalence:

$$J_C(L) = \{L\text{-rational degree 0 divisors on } C\}/\sim,$$

for all field extensions L/K.

Let $A_C : C \to J_C$ be the Abel-Jacobi map, defined as follows:

$$\begin{aligned} A_C : C(L) &\to J_C(L) \\ y &\mapsto [y - x], \end{aligned}$$

for all field extensions L/K.

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

- Suppose that A_C is not an embedding, so $\exists y \neq z \in C(\overline{K})$ such that

$$A_C(y) = A_C(z)$$

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

- Suppose that A_C is not an embedding, so $\exists y \neq z \in C(\overline{K})$ such that

$$A_C(y) = A_C(z) \implies (y - x) \sim (z - x)$$

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

- Suppose that A_C is not an embedding, so $\exists y \neq z \in C(\overline{K})$ such that

$$A_C(y) = A_C(z) \implies (y - x) \sim (z - x) \implies y \sim z.$$

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

- Suppose that A_C is not an embedding, so $\exists y \neq z \in C(\overline{K})$ such that

  $$A_C(y) = A_C(z) \implies (y - x) \sim (z - x) \implies y \sim z.$$

  So C has genus 0.
- Otherwise, $C \hookrightarrow J_C$ is a closed subvariety of the abelian variety J_C.

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

- Suppose that A_C is not an embedding, so $\exists y \neq z \in C(\overline{K})$ such that

  $$A_C(y) = A_C(z) \implies (y - x) \sim (z - x) \implies y \sim z.$$

  So C has genus 0.
- Otherwise, $C \hookrightarrow J_C$ is a closed subvariety of the abelian variety J_C. By Faltings's theorem, $\exists X_i = x_i + B_i$ such that $X_i \subset C$ and

  $$C(K) = \bigcup_{i=1}^{n} X_i(K).$$

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

- Suppose that A_C is not an embedding, so $\exists y \neq z \in C(\overline{K})$ such that

$$A_C(y) = A_C(z) \implies (y - x) \sim (z - x) \implies y \sim z.$$

  So C has genus 0.
- Otherwise, $C \hookrightarrow J_C$ is a closed subvariety of the abelian variety J_C. By Faltings's theorem, $\exists X_i = x_i + B_i$ such that $X_i \subset C$ and

$$C(K) = \bigcup_{i=1}^{n} X_i(K).$$

  As $C(K)$ is infinite, $\exists B_j$ of dimension 1, ie. an elliptic curve.

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

- Suppose that A_C is not an embedding, so $\exists y \neq z \in C(\overline{K})$ such that

$$A_C(y) = A_C(z) \implies (y - x) \sim (z - x) \implies y \sim z.$$

  So C has genus 0.

- Otherwise, $C \hookrightarrow J_C$ is a closed subvariety of the abelian variety J_C. By Faltings's theorem, $\exists X_i = x_i + B_i$ such that $X_i \subset C$ and

$$C(K) = \bigcup_{i=1}^{n} X_i(K).$$

  As $C(K)$ is infinite, $\exists B_j$ of dimension 1, ie. an elliptic curve. Since $X_j \subset C$ and C is non-singular, $X_j = C$.

Proof of Faltings's theorem

Suppose that $C(K)$ is infinite.

- Suppose that A_C is not an embedding, so $\exists y \neq z \in C(\overline{K})$ such that

$$A_C(y) = A_C(z) \implies (y - x) \sim (z - x) \implies y \sim z.$$

  So C has genus 0.

- Otherwise, $C \hookrightarrow J_C$ is a closed subvariety of the abelian variety J_C. By Faltings's theorem, $\exists X_i = x_i + B_i$ such that $X_i \subset C$ and

$$C(K) = \bigcup_{i=1}^{n} X_i(K).$$

  As $C(K)$ is infinite, $\exists B_j$ of dimension 1, ie. an elliptic curve.
  Since $X_j \subset C$ and C is non-singular, $X_j = C$.
  So C has genus 1.

What next?

What about $C(L)$, for any finite extension L/K?

What next?

What about $C(L)$, for any finite extension L/K?
A: Finite if $g \geq 2$, by Faltings's theorem.

What next?

What about $C(L)$, for any finite extension L/K?
A: Finite if $g \geq 2$, by Faltings's theorem.

What about

$$\Sigma^d = \{y \in C : [K(y) : K] = d\},$$

for $d \geq 2$?

Symmetric powers of curves

Let $d \geq 1$. The d-th symmetric power of C is

$$C^{(d)} = C^d / S_d.$$

Symmetric powers of curves

Let $d \geq 1$. The d-th symmetric power of C is

$$C^{(d)} = C^d / S_d.$$

For any field extension L/K,

$$C^{(d)}(L) = \{\text{unordered tuples } (x_1, \ldots, x_d) \in C^d(\overline{K})\}^{\mathrm{Gal}(\overline{K}/L)}$$

Symmetric powers of curves

Let $d \geq 1$. The d-th symmetric power of C is

$$C^{(d)} = C^d / S_d.$$

For any field extension L/K,

$$\begin{aligned} C^{(d)}(L) &= \{\text{unordered tuples } (x_1, \ldots, x_d) \in C^d(\overline{K})\}^{\mathrm{Gal}(\overline{K}/L)} \\ &= \{L\text{-rational degree } d \text{ effective divisors on } C\}. \end{aligned}$$

Symmetric powers of curves

Let $d \geq 1$. The d-th symmetric power of C is

$$C^{(d)} = C^d / S_d.$$

For any field extension L/K,

$$\begin{aligned} C^{(d)}(L) &= \{\text{unordered tuples } (x_1, \dots, x_d) \in C^d(\overline{K})\}^{\mathrm{Gal}(\overline{K}/L)} \\ &= \{L\text{-rational degree } d \text{ effective divisors on } C\}. \end{aligned}$$

There is a map $\phi_d : C^{(d)} \to J_C$ given by

$$\begin{aligned} \phi_d : \quad C^{(d)}(L) &\to J_C(L) \\ (x_1 + \cdots + x_d) &\mapsto [x_1 + \cdots + x_d - dx]. \end{aligned}$$

Proof of Faltings's theorem (again)

Suppose that $\Sigma^d = \{y \in C : [K(y) : K] = d\}$ is infinite. Note that $\Sigma^d \hookrightarrow C^{(d)}(K)$.

Proof of Faltings's theorem (again)

Suppose that $\Sigma^d = \{y \in C : [K(y) : K] = d\}$ is infinite. Note that $\Sigma^d \hookrightarrow C^{(d)}(K)$. Then either

1. $\exists y \neq z \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$,

Proof of Faltings's theorem (again)

Suppose that $\Sigma^d = \{y \in C : [K(y) : K] = d\}$ is infinite. Note that $\Sigma^d \hookrightarrow C^{(d)}(K)$. Then either

1. $\exists y \neq z \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$,
2. $(\operatorname{im} \phi_d)(K)$ is infinite. By Faltings's theorem, $\exists$ positive rank abelian subvariety $A \subset J_C$ and $y \in \Sigma^d$ such that

$$\phi_d(y) + A \subset \operatorname{im} \phi_d.$$

Proof of Faltings's theorem (again)

Suppose that $\Sigma^d = \{y \in C : [K(y) : K] = d\}$ is infinite. Note that $\Sigma^d \hookrightarrow C^{(d)}(K)$. Then either

1. $\exists y \neq z \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$,
2. $(\operatorname{im} \phi_d)(K)$ is infinite. By Faltings's theorem, $\exists$ positive rank abelian subvariety $A \subset J_C$ and $y \in \Sigma^d$ such that

$$\phi_d(y) + A \subset \operatorname{im} \phi_d.$$

These are sufficient conditions for Σ^d to be infinite!

Proof of Faltings's theorem (again)

Suppose that $\Sigma^d = \{y \in C : [K(y) : K] = d\}$ is infinite. Note that $\Sigma^d \hookrightarrow C^{(d)}(K)$. Then either

1. $\exists y \neq z \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$,
   $\implies \exists$ infinitely many $z \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$.

2. $(\operatorname{im}\phi_d)(K)$ is infinite. By Faltings's theorem, $\exists$ positive rank abelian subvariety $A \subset J_C$ and $y \in \Sigma^d$ such that

$$\phi_d(y) + A \subset \operatorname{im}\phi_d.$$

These are sufficient conditions for Σ^d to be infinite!

Proof of Faltings's theorem (again)

Suppose that $\Sigma^d = \{y \in C : [K(y) : K] = d\}$ is infinite. Note that $\Sigma^d \hookrightarrow C^{(d)}(K)$. Then either

1. $\exists y \neq z \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$,
   $\implies \exists$ infinitely many $z \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$.
2. $(\operatorname{im}\phi_d)(K)$ is infinite. By Faltings's theorem, $\exists$ positive rank abelian subvariety $A \subset J_C$ and $y \in \Sigma^d$ such that

$$\phi_d(y) + A \subset \operatorname{im}\phi_d.$$

$\implies \exists$ infinitely many $z \in \Sigma^d$ such that $\phi_d(z) \in \phi_d(y) + A$.

These are sufficient conditions for Σ^d to be infinite!

Isolated points

Definition

Let $y \in \Sigma^d$ be a degree d point. We say that

- y is $\mathbb{P}^1$-*parametrized* if $\exists z \neq y \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$.
- y is *AV-parametrized* if $\exists$ positive rank abelian subvariety $A \subset J_C$ such that $\phi_d(y) + A \subset \operatorname{im} \phi_d$.
- y is *isolated* if it is neither $\mathbb{P}^1$- nor AV-parametrized.

Isolated points

Definition

Let $y \in \Sigma^d$ be a degree d point. We say that

- y is $\mathbb{P}^1$-*parametrized* if $\exists z \neq y \in \Sigma^d$ such that $\phi_d(y) = \phi_d(z)$.
- y is *AV-parametrized* if $\exists$ positive rank abelian subvariety $A \subset J_C$ such that $\phi_d(y) + A \subset \operatorname{im} \phi_d$.
- y is *isolated* if it is neither $\mathbb{P}^1$- nor AV-parametrized.

Theorem

Σ^d is infinite if and only if there exists a non-isolated point $y \in \Sigma^d$.

Isolated points on modular curves

Let $n \geq 3$. Consider the modular curve $X_1(n)$, which parametrizes elliptic curves with a point of order n, i.e.

$$X_1(n)(L) = \{(E,P) : E/L \text{ elliptic curve}, P \in E(L) \text{ of order } n\}.$$

Isolated points on modular curves

Let $n \geq 3$. Consider the modular curve $X_1(n)$, which parametrizes elliptic curves with a point of order n, i.e.

$$X_1(n)(L) = \{(E, P) : E/L \text{ elliptic curve}, P \in E(L) \text{ of order } n\}.$$

An isolated point on $X_1(n)$ of degree d corresponds to an "exceptional" elliptic curve with point of order n defined over a number field of degree d.

Isolated points on modular curves

Let $n \geq 3$. Consider the modular curve $X_1(n)$, which parametrizes elliptic curves with a point of order n, i.e.

$$X_1(n)(L) = \{(E, P) : E/L \text{ elliptic curve}, P \in E(L) \text{ of order } n\}.$$

An isolated point on $X_1(n)$ of degree d corresponds to an "exceptional" elliptic curve with point of order n defined over a number field of degree d.

Theorem

Let E be an elliptic curve defined over a cubic field K, and let $P \in E_{tors}(K)$. Then $\mathrm{ord}(P) \in \{1, \ldots, 16, 18, 20\}$, *each of which occurs infinitely often, or* $\mathrm{ord}(P) = 21$, $K = \mathbb{Q}(\zeta_9)^+$ *and*

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 5.$$

Isolated points on modular curves

More generally, let $H \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, for some $n \geq 1$, with $-I \in H$. There exists a modular curve X_H which parametrizes elliptic curves with mod n Galois representation contained in H.

Isolated points on modular curves

More generally, let $H \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, for some $n \geq 1$, with $-I \in H$. There exists a modular curve X_H which parametrizes elliptic curves with mod n Galois representation contained in H. In other words,

$$X_H(L) = \{E/L : \overline{\rho}_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/L)) \leq H\}/\sim .$$

Isolated points on modular curves

More generally, let $H \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, for some $n \geq 1$, with $-I \in H$. There exists a modular curve X_H which parametrizes elliptic curves with mod n Galois representation contained in H. In other words,

$$X_H(L) = \{E/L : \overline{\rho}_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/L)) \leq H\}/\sim .$$

An isolated point on X_H corresponds to an "exceptional" elliptic curve with given Galois representation.

Isolated points on modular curves

More generally, let $H \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, for some $n \geq 1$, with $-I \in H$. There exists a modular curve X_H which parametrizes elliptic curves with mod n Galois representation contained in H. In other words,

$$X_H(L) = \{E/L : \overline{\rho}_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/L)) \leq H\}/\sim .$$

An isolated point on X_H corresponds to an "exceptional" elliptic curve with given Galois representation.

Conjecture (Serre's uniformity conjecture)

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $p > 37$ be prime. Then $\overline{\rho}_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Isolated points on modular curves

More generally, let $H \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, for some $n \geq 1$, with $-I \in H$. There exists a modular curve X_H which parametrizes elliptic curves with mod n Galois representation contained in H. In other words,

$$X_H(L) = \{E/L : \overline{\rho}_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/L)) \leq H\}/\sim .$$

An isolated point on X_H corresponds to an "exceptional" elliptic curve with given Galois representation.

Conjecture (Serre's uniformity conjecture)

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $p > 37$ be prime. Then $\overline{\rho}_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Equivalently,

Conjecture

Let $p > 37$ be prime. Then $X_{ns}(p)$ has no isolated points of degree 1.