Descent on elliptic surfaces and the Brauer-Manin obstruction

Harvey Yau

July 31, 2024

Adelic points

Let X be a projective variety defined over k a number field, and let v be a place of k.

Adelic points

Let X be a projective variety defined over k a number field, and let v be a place of k.
Points in $X(k)$ may be hard to find, but points in $X(k_v)$ are easier to find.

Adelic points

Let X be a projective variety defined over k a number field, and let v be a place of k.
Points in $X(k)$ may be hard to find, but points in $X(k_v)$ are easier to find.
For finite places, they can be thought of as a series of points modulo $\mathfrak{p}^n$ for all n. For infinite places, this is equivalent to finding points in $X(\mathbb{R})$ or $X(\mathbb{C})$, which is also easier.

Adelic points

Let X be a projective variety defined over k a number field, and let v be a place of k.
Points in $X(k)$ may be hard to find, but points in $X(k_v)$ are easier to find.
For finite places, they can be thought of as a series of points modulo $\mathfrak{p}^n$ for all n. For infinite places, this is equivalent to finding points in $X(\mathbb{R})$ or $X(\mathbb{C})$, which is also easier.
Note that any rational point will yield a point in $X(k_v)$ for all v. In other words,

$$X(k) \hookrightarrow \prod_v X(k_v)$$

Adelic points

Let X be a projective variety defined over k a number field, and let v be a place of k.
Points in $X(k)$ may be hard to find, but points in $X(k_v)$ are easier to find.
For finite places, they can be thought of as a series of points modulo $\mathfrak{p}^n$ for all n. For infinite places, this is equivalent to finding points in $X(\mathbb{R})$ or $X(\mathbb{C})$, which is also easier.
Note that any rational point will yield a point in $X(k_v)$ for all v. In other words,

$$X(k) \hookrightarrow \prod_v X(k_v) = X(\mathbb{A}_k) \text{ (set of adelic points).}$$

Adelic points

Let X be a projective variety defined over k a number field, and let v be a place of k.
Points in $X(k)$ may be hard to find, but points in $X(k_v)$ are easier to find.
For finite places, they can be thought of as a series of points modulo $\mathfrak{p}^n$ for all n. For infinite places, this is equivalent to finding points in $X(\mathbb{R})$ or $X(\mathbb{C})$, which is also easier.
Note that any rational point will yield a point in $X(k_v)$ for all v. In other words,

$$X(k) \hookrightarrow \prod_v X(k_v) = X(\mathbb{A}_k) \text{ (set of adelic points).}$$

So if there are no adelic points, then there cannot be any rational points.

$$X(\mathbb{A}_k) = \varnothing \quad \Longrightarrow \quad X(k) = \varnothing.$$

The Hasse principle and weak approximation

One might hope that the converse holds, i.e.

$$X(\mathbb{A}_k) \neq \varnothing \quad \Longrightarrow \quad X(k) \neq \varnothing.$$

The Hasse principle and weak approximation

One might hope that the converse holds, i.e.

$$X(\mathbb{A}_k) \neq \varnothing \quad \Longrightarrow \quad X(k) \neq \varnothing.$$

This statement is called the *Hasse principle* (for X).

The Hasse principle and weak approximation

One might hope that the converse holds, i.e.

$$X(\mathbb{A}_k) \neq \varnothing \quad \Longrightarrow \quad X(k) \neq \varnothing.$$

This statement is called the *Hasse principle* (for X).
Related is the stronger notion of *weak approximation*, which states that $X(k)$ is dense in $X(\mathbb{A}_k)$.

The Hasse principle and weak approximation

One might hope that the converse holds, i.e.

$$X(\mathbb{A}_k) \neq \varnothing \quad \Longrightarrow \quad X(k) \neq \varnothing.$$

This statement is called the *Hasse principle* (for X).
Related is the stronger notion of *weak approximation*, which states that $X(k)$ is dense in $X(\mathbb{A}_k)$.
These are true for some classes of varieties (e.g. conics), but not all varieties. It's an interesting question to find examples where these do not hold.

The Brauer group

The *Brauer group* of a field k is

$$\mathrm{Br}(k) = H^2(k, k^\times).$$

The Brauer group

The *Brauer group* of a field k is

$$\mathrm{Br}(k) = H^2(k, k^\times).$$

Elements of $\mathrm{Br}(k)$ can be represented by *central simple algebras* over k. These are (non-commutative) algebras over k with no nontrivial two-sided ideals and with centre k.

The Brauer group

The *Brauer group* of a field k is

$$\mathrm{Br}(k) = H^2(k, k^\times).$$

Elements of $\mathrm{Br}(k)$ can be represented by *central simple algebras* over k. These are (non-commutative) algebras over k with no nontrivial two-sided ideals and with centre k.
An example of a central simple algebra is a *cyclic algebra*. If k contains ζ a primitive n^{th} root of unity, then given $a, b \in k^\times$, the algebra generated by i, j with relations

$$i^n = a, \quad j^n = b, \quad ij = \zeta ji$$

is a cyclic algebra, denoted $(a, b)_n$.

Brauer groups of fields

- $\mathrm{Br}(\mathbb{C}) = 0$, $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Brauer groups of fields

- $\mathrm{Br}(\mathbb{C}) = 0$, $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.
- $\mathrm{Br}(k_v) \cong \mathbb{Q}/\mathbb{Z}$ for k_v a local field.
  There is a canonical isomorphism $\mathrm{inv}_v : \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$, called the *invariant map*.

Brauer groups of fields

- $\mathrm{Br}(\mathbb{C}) = 0$, $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.
- $\mathrm{Br}(k_v) \cong \mathbb{Q}/\mathbb{Z}$ for k_v a local field.
  There is a canonical isomorphism $\mathrm{inv}_v : \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$, called the *invariant map*.
- For k a number field, we have

Theorem (Albert-Brauer-Hasse-Noether)

The sequence

$$0 \to \mathrm{Br}(k) \to \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0$$

is exact.

Brauer groups of schemes

The Brauer group of a scheme X is defined as

$$\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m).$$

Brauer groups of schemes

The Brauer group of a scheme X is defined as

$$\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m).$$

When X is a regular irreducible variety, we can represent elements of $\mathrm{Br}(X)$ as central simple algebras over $k(X)$.

Brauer groups of schemes

The Brauer group of a scheme X is defined as

$$\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m).$$

When X is a regular irreducible variety, we can represent elements of $\mathrm{Br}(X)$ as central simple algebras over $k(X)$.
The key property is that elements of $\mathrm{Br}(X)$ can be evaluated at points of X. In other words, there is a pairing

$$X(k) \times \mathrm{Br}(X) \to \mathrm{Br}(k).$$

Brauer groups of schemes

The Brauer group of a scheme X is defined as

$$\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m).$$

When X is a regular irreducible variety, we can represent elements of $\mathrm{Br}(X)$ as central simple algebras over $k(X)$.
The key property is that elements of $\mathrm{Br}(X)$ can be evaluated at points of X. In other words, there is a pairing

$$X(k) \times \mathrm{Br}(X) \to \mathrm{Br}(k).$$

This can be done for adelic points too: there is a pairing

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \bigoplus_v \mathrm{Br}(k_v).$$

Brauer-Manin obstruction

By summing the local invariants, one obtains a pairing

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}.$$

Brauer-Manin obstruction

By summing the local invariants, one obtains a pairing

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}.$$

Since the sum of local invariants of an element of $\mathrm{Br}(k)$ is zero, we get that the above pairing is zero for all points of $X(k) \subseteq X(\mathbb{A}_k)$.

Brauer-Manin obstruction

By summing the local invariants, one obtains a pairing

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}.$$

Since the sum of local invariants of an element of $\mathrm{Br}(k)$ is zero, we get that the above pairing is zero for all points of $X(k) \subseteq X(\mathbb{A}_k)$. This gives a new way to prove the nonexistence of rational points: if we find an element $A \in \mathrm{Br}(X)$ such that $A(P)$ is nonzero for all adelic points $P \in X(\mathbb{A}_k)$, then none of the adelic points can be rational points. We call this a *Brauer-Manin obstruction* to the Hasse principle.

Brauer-Manin obstruction

More generally, we can define the *Brauer-Manin set*

$$X(\mathbb{A}_k)^{\mathrm{Br}} = \{P \in X(\mathbb{A}_k) : \sum \mathrm{inv}\, A(P) = 0 \text{ for all } A \in \mathrm{Br}(X)\}.$$

Brauer-Manin obstruction

More generally, we can define the *Brauer-Manin set*

$$X(\mathbb{A}_k)^{\mathrm{Br}} = \{P \in X(\mathbb{A}_k) : \sum \mathrm{inv}\, A(P) = 0 \text{ for all } A \in \mathrm{Br}(X)\}.$$

We then have the inclusions

$$X(k) \subseteq \overline{X(k)} \subseteq X(\mathbb{A}_k)^{\mathrm{Br}} \subseteq X(\mathbb{A}_k).$$

Brauer-Manin obstruction

More generally, we can define the *Brauer-Manin set*

$$X(\mathbb{A}_k)^{\mathrm{Br}} = \{P \in X(\mathbb{A}_k) : \sum \mathrm{inv}\, A(P) = 0 \text{ for all } A \in \mathrm{Br}(X)\}.$$

We then have the inclusions

$$X(k) \subseteq \overline{X(k)} \subseteq X(\mathbb{A}_k)^{\mathrm{Br}} \subseteq X(\mathbb{A}_k).$$

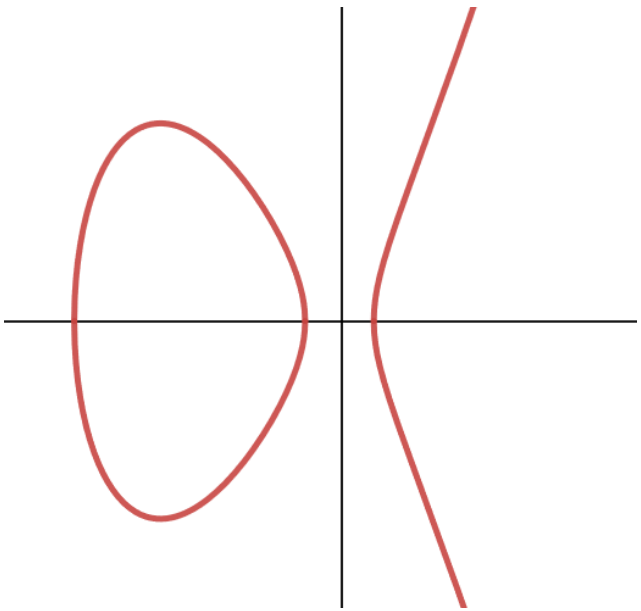
- If $X(\mathbb{A}_k)$ is nonempty but $X(\mathbb{A}_k)^{\mathrm{Br}}$ is empty, then there is a *Brauer-Manin obstruction to the Hasse principle*.
- If $X(\mathbb{A}_k)^{\mathrm{Br}} \neq X(\mathbb{A}_k)$, then there is a *Brauer-Manin obstruction to weak approximation*.

Example

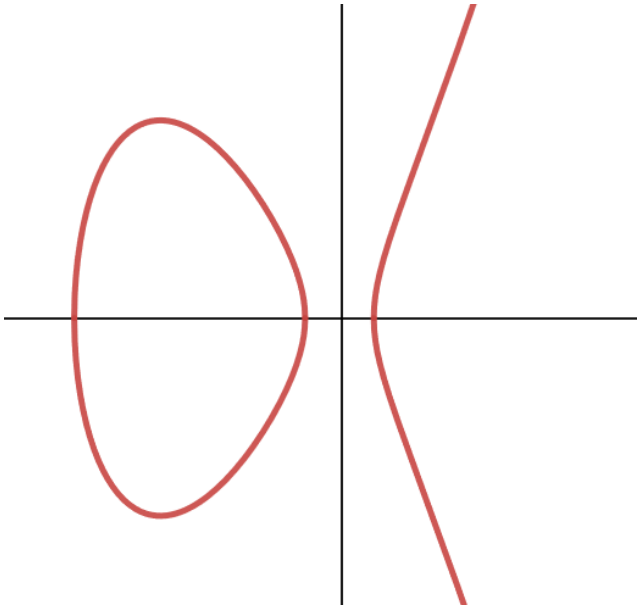
Consider the elliptic curve $E : y^2 = x^3 + 4x^2 - 1$.

Example

Consider the elliptic curve $E : y^2 = x^3 + 4x^2 - 1$. Pictured below is $E(\mathbb{R})$.

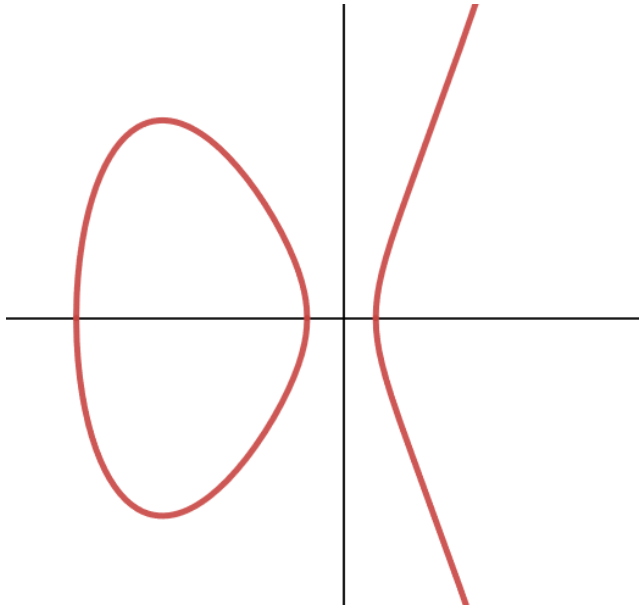


Example



Take the element of $\mathrm{Br}(E)$ represented by the cyclic algebra $A = (-1, x)_2$. Then for all adelic points P with $(v = \infty)$-part lying on the left component, we have $\sum \mathrm{inv}\, A(P) = \frac{1}{2}$.

Example



Take the element of $\mathrm{Br}(E)$ represented by the cyclic algebra $A = (-1, x)_2$. Then for all adelic points P with $(v = \infty)$-part lying on the left component, we have $\sum \mathrm{inv}\, A(P) = \frac{1}{2}$.
This shows that there are no rational points on the left component, so there is a Brauer-Manin obstruction to weak approximation.

Summary

- The *Brauer-Manin obstruction to weak approximation* is when

$$X(\mathbb{A}_k)^{\mathrm{Br}} \subsetneq X(\mathbb{A}_k).$$

- We wish to find elements of the Brauer group of a scheme X to find examples of *Brauer-Manin obstruction*.

Summary

- The *Brauer-Manin obstruction to weak approximation* is when

$$X(\mathbb{A}_k)^{\mathrm{Br}} \subsetneq X(\mathbb{A}_k).$$

- We wish to find elements of the Brauer group of a scheme X to find examples of *Brauer-Manin obstruction*.
- Some elements of the Brauer group of a field can be represented by *cyclic algebras* $(a, b)_n$.

Summary

- The *Brauer-Manin obstruction to weak approximation* is when

$$X(\mathbb{A}_k)^{\mathrm{Br}} \subsetneq X(\mathbb{A}_k).$$

- We wish to find elements of the Brauer group of a scheme X to find examples of *Brauer-Manin obstruction*.
- Some elements of the Brauer group of a field can be represented by *cyclic algebras* $(a, b)_n$.
- If we can find an adelic point P and a Brauer element A such that $\sum \mathrm{inv}_v A(P) \neq 0$, then we have a Brauer-Manin obstruction to weak approximation.

Calculating the Brauer group of a scheme

For X a regular irreducible variety (over a field of characteristic zero), we have $\mathrm{Br}(X)$ is a subgroup of $\mathrm{Br}(k(X))$.

Calculating the Brauer group of a scheme

For X a regular irreducible variety (over a field of characteristic zero), we have $\mathrm{Br}(X)$ is a subgroup of $\mathrm{Br}(k(X))$.
To determine which elements of $\mathrm{Br}(k(X))$ lie in $\mathrm{Br}(X)$, one can use *residue maps*.

Calculating the Brauer group of a scheme

For X a regular irreducible variety (over a field of characteristic zero), we have $\mathrm{Br}(X)$ is a subgroup of $\mathrm{Br}(k(X))$.
To determine which elements of $\mathrm{Br}(k(X))$ lie in $\mathrm{Br}(X)$, one can use *residue maps*.

Residue map

Let $D \subseteq X$ be an irreducible codimension-1 subvariety. Then there is a *residue map*

$$\partial_D : \mathrm{Br}(k(X)) \to H^1(k(D), \mathbb{Q}/\mathbb{Z}).$$

The kernel of this map is the subgroup of elements that can be evaluated at D.

Calculating the Brauer group of a scheme

Theorem

Let $A \in \mathrm{Br}(k(X))$. Then $A \in \mathrm{Br}(X)$ if and only if $\partial_D(A) = 0$ for all irreducible codimension-1 subvarieties $D \subseteq X$.

Calculating the Brauer group of a scheme

Theorem

Let $A \in \mathrm{Br}(k(X))$. Then $A \in \mathrm{Br}(X)$ if and only if $\partial_D(A) = 0$ for all irreducible codimension-1 subvarieties $D \subseteq X$.

This theorem allows us to find elements of $\mathrm{Br}(X)$ by just checking all the residue maps.

Brauer group of an elliptic curve

For an elliptic curve E over a field k, there is an isomorphism

$$\frac{\mathrm{Br}(E)}{\mathrm{Br}_0(E)} \cong H^1(k, E).$$

Here $\mathrm{Br}_0(E)$ are the *constant algebras*, the image of the natural map $\mathrm{Br}(k) \to \mathrm{Br}(E)$.

Brauer group of an elliptic curve

For an elliptic curve E over a field k, there is an isomorphism

$$\frac{\mathrm{Br}(E)}{\mathrm{Br}_0(E)} \cong H^1(k, E).$$

Here $\mathrm{Br}_0(E)$ are the *constant algebras*, the image of the natural map $\mathrm{Br}(k) \to \mathrm{Br}(E)$.
The group $H^1(k, E)$ is well understood, so we can use this to find elements easily. However, calculating the above isomorphism explicitly is not entirely straightforward.

Elliptic surfaces

An *elliptic surface* is a surface $\mathcal{E}$ with a map to a curve $\pi : \mathcal{E} \to C$ such that the generic fibre is an elliptic curve E over $k(C)$.

Elliptic surfaces

An *elliptic surface* is a surface $\mathcal{E}$ with a map to a curve $\pi : \mathcal{E} \to C$ such that the generic fibre is an elliptic curve E over $k(C)$.
For example, take C to be $\mathbb{P}^1$, parametrised by z. Then we can write down a Weierstrass equation with coordinates in $k(z)$, such as

$$y^2 = x^3 + 2zx^2 + (3z^2 + 2).$$

Elliptic surfaces

An *elliptic surface* is a surface $\mathcal{E}$ with a map to a curve $\pi : \mathcal{E} \to C$ such that the generic fibre is an elliptic curve E over $k(C)$.
For example, take C to be $\mathbb{P}^1$, parametrised by z. Then we can write down a Weierstrass equation with coordinates in $k(z)$, such as

$$y^2 = x^3 + 2zx^2 + (3z^2 + 2).$$

This defines an elliptic surface $\mathcal{E}$. The special fibre above a point $z = z_0$ is given by substituting in z_0 into the above equation.

Brauer group of an elliptic surface

To find the Brauer group of an elliptic surface $\mathcal{E}$, we can look at $\mathrm{Br}(k(\mathcal{E}))$ and check the residue maps for all irreducible curves lying in $\mathcal{E}$.

Brauer group of an elliptic surface

To find the Brauer group of an elliptic surface $\mathcal{E}$, we can look at $\mathrm{Br}(k(\mathcal{E}))$ and check the residue maps for all irreducible curves lying in $\mathcal{E}$.
There are two types of curve in an elliptic surface:

Brauer group of an elliptic surface

To find the Brauer group of an elliptic surface $\mathcal{E}$, we can look at $\mathrm{Br}(k(\mathcal{E}))$ and check the residue maps for all irreducible curves lying in $\mathcal{E}$.

There are two types of curve in an elliptic surface:

- Horizontal curves. For these curves D, the restriction of $\pi : \mathcal{E} \to C$ to D is surjective. These curves correspond to points of the generic fibre.

Brauer group of an elliptic surface

To find the Brauer group of an elliptic surface $\mathcal{E}$, we can look at $\mathrm{Br}(k(\mathcal{E}))$ and check the residue maps for all irreducible curves lying in $\mathcal{E}$.

There are two types of curve in an elliptic surface:

- Horizontal curves. For these curves D, the restriction of $\pi : \mathcal{E} \to C$ to D is surjective. These curves correspond to points of the generic fibre.
- Vertical curves. These are components of special fibres above points $P \in C$.

Brauer group of an elliptic surface

To find the Brauer group of an elliptic surface $\mathcal{E}$, we can look at $\mathrm{Br}(k(\mathcal{E}))$ and check the residue maps for all irreducible curves lying in $\mathcal{E}$.

There are two types of curve in an elliptic surface:

- Horizontal curves. For these curves D, the restriction of $\pi : \mathcal{E} \to C$ to D is surjective. These curves correspond to points of the generic fibre.
- Vertical curves. These are components of special fibres above points $P \in C$.

For elements of $\mathrm{Br}(E)$, the residues with respect to horizontal curves will automatically be zero, so one only needs to check the residues with respect to vertical curves.

Plan to find Brauer elements

Our plan is as follows:

Plan to find Brauer elements

Our plan is as follows:

1. Find elements $a \in H^1(K, E)$.

Plan to find Brauer elements

Our plan is as follows:

1. Find elements $a \in H^1(K, E)$.
2. Convert them into elements $A \in \mathrm{Br}(E)$.

Plan to find Brauer elements

Our plan is as follows:

1. Find elements $a \in H^1(K, E)$.
2. Convert them into elements $A \in \mathrm{Br}(E)$.
3. Calculate the residue $\partial_D(A)$ for all vertical curves D.

Plan to find Brauer elements

Our plan is as follows:

1. Find elements $a \in H^1(K, E)$.
2. Convert them into elements $A \in \mathrm{Br}(E)$.
3. Calculate the residue $\partial_D(A)$ for all vertical curves D.
4. If all the residues are trivial, we have found an element of $\mathrm{Br}(\mathcal{E})$

Plan to find Brauer elements

Our plan is as follows:

1. Find elements $a \in H^1(K, E)$.
2. Convert them into elements $A \in \mathrm{Br}(E)$.
3. Calculate the residue $\partial_D(A)$ for all vertical curves D.
4. If all the residues are trivial, we have found an element of $\mathrm{Br}(\mathcal{E})$
5. Hope the element we found obstructs weak approximation

3-descent on an elliptic curve

The generic fibre is an elliptic curve E defined over a field $K = k(C)$, and we want to find elements of $H^1(K, E)$.

3-descent on an elliptic curve

The generic fibre is an elliptic curve E defined over a field $K = k(C)$, and we want to find elements of $H^1(K, E)$.
Let's restrict ourselves to looking at 3-torsion. Then we have the exact sequence from Galois cohomology

$$0 \to E(K)/3E(K) \to H^1(K, E[3]) \to H^1(K, E)[3] \to 0.$$

3-descent on an elliptic curve

The generic fibre is an elliptic curve E defined over a field $K = k(C)$, and we want to find elements of $H^1(K, E)$.
Let's restrict ourselves to looking at 3-torsion. Then we have the exact sequence from Galois cohomology

$$0 \to E(K)/3E(K) \to H^1(K, E[3]) \to H^1(K, E)[3] \to 0.$$

The group $H^1(K, E[3])$ is easier to describe.

Describing $H^1(K, E[3])$

Let S be the subvariety of $\mathcal{E}$ consisting of all 3-torsion points of all the fibres. This will be a union of curves.

3-descent on an elliptic curve

The generic fibre is an elliptic curve E defined over a field $K = k(C)$, and we want to find elements of $H^1(K, E)$.
Let's restrict ourselves to looking at 3-torsion. Then we have the exact sequence from Galois cohomology

$$0 \to E(K)/3E(K) \to H^1(K, E[3]) \to H^1(K, E)[3] \to 0.$$

The group $H^1(K, E[3])$ is easier to describe.

Describing $H^1(K, E[3])$

Let S be the subvariety of $\mathcal{E}$ consisting of all 3-torsion points of all the fibres. This will be a union of curves. Let R be the product of the function fields of all the components of S.

3-descent on an elliptic curve

The generic fibre is an elliptic curve E defined over a field $K = k(C)$, and we want to find elements of $H^1(K, E)$.
Let's restrict ourselves to looking at 3-torsion. Then we have the exact sequence from Galois cohomology

$$0 \to E(K)/3E(K) \to H^1(K, E[3]) \to H^1(K, E)[3] \to 0.$$

The group $H^1(K, E[3])$ is easier to describe.

Describing $H^1(K, E[3])$

Let S be the subvariety of $\mathcal{E}$ consisting of all 3-torsion points of all the fibres. This will be a union of curves. Let R be the product of the function fields of all the components of S.
Then $H^1(K, E[3])$ is isomorphic to a subgroup of $R^\times$ modulo cubes.

3-descent on an elliptic curve - Example 1

Let $T_1, T_2 \in E$ be points generating $E[3]$.
If T_1, T_2 are both defined over K, then S consists of 9 sections, so $R = K^9$.

3-descent on an elliptic curve - Example 1

Let $T_1, T_2 \in E$ be points generating $E[3]$.
If T_1, T_2 are both defined over K, then S consists of 9 sections, so $R = K^9$. In this case, elements of $H^1(K, E[3]) \subseteq R^\times$ are determined by the values on the two components S_1, S_2 corresponding to the points T_1, T_2, so we may write elements of $H^1(K, E[3])$ as pairs (a_1, a_2).

3-descent on an elliptic curve - Example 1

Let $T_1, T_2 \in E$ be points generating $E[3]$.
If T_1, T_2 are both defined over K, then S consists of 9 sections, so $R = K^9$. In this case, elements of $H^1(K, E[3]) \subseteq R^\times$ are determined by the values on the two components S_1, S_2 corresponding to the points T_1, T_2, so we may write elements of $H^1(K, E[3])$ as pairs (a_1, a_2).
The corresponding Brauer element of (a_1, a_2) is given by the sum of cyclic algebras

$$(a_1, f_2)_3 + (a_2, f_1)_3$$

where f_i is a function on E with divisor $3(T_i) - 3(O)$.

3-descent on an elliptic curve - Example 2

Suppose T_1 is defined over K but T_2 is not.

3-descent on an elliptic curve - Example 2

Suppose T_1 is defined over K but T_2 is not. Then S decomposes into 5 sections: S_0, S_1, S_2 corresponding to $O, T_1, 2T_1$, and S_3, S_4 corresponding to the Galois orbits $\{T_2 + nT_1\}, \{2T_2 + nT_1\}$.

3-descent on an elliptic curve - Example 2

Suppose T_1 is defined over K but T_2 is not. Then S decomposes into 5 sections: S_0, S_1, S_2 corresponding to $O, T_1, 2T_1$, and S_3, S_4 corresponding to the Galois orbits $\{T_2 + nT_1\}, \{2T_2 + nT_1\}$. The function fields of S_0, S_1, S_2 are all isomorphic to K, while the function fields of S_3, S_4 are isomorphic to L a degree 3 Galois extension of K.

3-descent on an elliptic curve - Example 2

Suppose T_1 is defined over K but T_2 is not. Then S decomposes into 5 sections: S_0, S_1, S_2 corresponding to $O, T_1, 2T_1$, and S_3, S_4 corresponding to the Galois orbits $\{T_2 + nT_1\}, \{2T_2 + nT_1\}$.
The function fields of S_0, S_1, S_2 are all isomorphic to K, while the function fields of S_3, S_4 are isomorphic to L a degree 3 Galois extension of K.
In this case, elements of $H^1(K, E[3]) \subseteq R^\times$ are determined by the values on the two components S_1, S_3, so we may write elements of $H^1(K, E[3])$ as pairs (a, b) where $a \in K, b \in L$.

3-descent on an elliptic curve - Example 2

The corresponding Brauer element of (a_1, a_2) is given by the sum of cyclic algebras

3-descent on an elliptic curve - Example 2

The corresponding Brauer element of (a_1, a_2) is given by the sum of cyclic algebras

$$\left(af_1, \mathrm{Tr}_{L/K}(bf_2) - 3\frac{bd}{\sigma^2(d)}\frac{f_2 d'}{\sigma^2(d')}\right)_3$$
$$-\left(a, \mathrm{Tr}_{L/K}(b) - 3\frac{bd}{\sigma^2(d)}\right)_3 - \left(f_1, \mathrm{Tr}_{L/K}(f_2) - 3\frac{f_2 d'}{\sigma^2(d')}\right)_3$$

3-descent on an elliptic curve - Example 2

The corresponding Brauer element of (a_1, a_2) is given by the sum of cyclic algebras

$$\left(af_1, \mathrm{Tr}_{L/K}(bf_2) - 3\frac{bd}{\sigma^2(d)}\frac{f_2 d'}{\sigma^2(d')}\right)_3$$
$$-\left(a, \mathrm{Tr}_{L/K}(b) - 3\frac{bd}{\sigma^2(d)}\right)_3 - \left(f_1, \mathrm{Tr}_{L/K}(f_2) - 3\frac{f_2 d'}{\sigma^2(d')}\right)_3$$

where

- σ is a generator of $\mathrm{Gal}(L/K)$
- f_i is a function on E with divisor $3(T_i) - 3(O)$
- d is a cube root of $a\sigma(b)/b$
- d' is a cube root of $f_1\sigma(f_2)/f_2$

Local conditions

We want to narrow down from $H^1(K, E)$ to elements of $\mathrm{Br}(\mathcal{E})$ by checking the residue maps of vertical curves of $\mathcal{E}$.

Local conditions

We want to narrow down from $H^1(K, E)$ to elements of $\mathrm{Br}(\mathcal{E})$ by checking the residue maps of vertical curves of $\mathcal{E}$.
For each point $P \in C$, the components of the fibre $\pi^{-1}(P)$ each give residue maps. So each P gives a *local condition*

$$\partial_D(A) = 0 \text{ for all components } D \text{ of the fibre } \pi^{-1}(P).$$

Local conditions

We want to narrow down from $H^1(K, E)$ to elements of $\mathrm{Br}(\mathcal{E})$ by checking the residue maps of vertical curves of $\mathcal{E}$.
For each point $P \in C$, the components of the fibre $\pi^{-1}(P)$ each give residue maps. So each P gives a *local condition*

$$\partial_D(A) = 0 \text{ for all components } D \text{ of the fibre } \pi^{-1}(P).$$

This can then be translated into a local condition on $a \in H^1(K, E[3])$.

Local conditions

The resulting local conditions from the point P will be about the local behaviour of a at the points of S lying above P.

Local conditions

The resulting local conditions from the point P will be about the local behaviour of a at the points of S lying above P. For example:

Examples of local conditions

Local conditions

The resulting local conditions from the point P will be about the local behaviour of a at the points of S lying above P. For example:

Examples of local conditions

- If $\mathcal{E}$ has good reduction at P, then the resulting local condition is

  $\mathrm{ord}_Q(a) \equiv 0 \mod 3$ for all $Q \in S$ lying above P.

Local conditions

The resulting local conditions from the point P will be about the local behaviour of a at the points of S lying above P. For example:

Examples of local conditions

- If $\mathcal{E}$ has good reduction at P, then the resulting local condition is
  $$\mathrm{ord}_Q(a) \equiv 0 \mod 3 \text{ for all } Q \in S \text{ lying above } P.$$
- If $\mathcal{E}$ has multiplicative reduction at P, then let Q_0, Q_1, Q_2 be the intersections of S with the identity component of the special fibre above P. Then the resulting local condition is
  $$\mathrm{ord}_{Q_i}(a) \equiv 0 \mod 3, \quad a(Q_i) \text{ is a perfect cube.}$$

The Selmer group

Imposing all these local conditions will give us a subgroup of $H^1(K, E[3])$ that maps surjectively onto $(\mathrm{Br}(\mathcal{E})/\mathrm{Br}_0(\mathcal{E}))[3]$.

The Selmer group

Imposing all these local conditions will give us a subgroup of $H^1(K, E[3])$ that maps surjectively onto $(\mathrm{Br}(\mathcal{E})/\mathrm{Br}_0(\mathcal{E}))[3]$. We call the subgroup of $H^1(K, E[3])$ satisfying all the local conditions the (3-)*Selmer group* $S^{(3)}(K, E)$.

The Selmer group

Imposing all these local conditions will give us a subgroup of $H^1(K, E[3])$ that maps surjectively onto $(\mathrm{Br}(\mathcal{E})/\mathrm{Br}_0(\mathcal{E}))[3]$. We call the subgroup of $H^1(K, E[3])$ satisfying all the local conditions the (3-)*Selmer group* $S^{(3)}(K, E)$. This gives the following exact sequence

$$0 \to E(K)/3E(K) \to S^{(3)}(K, E) \to (\mathrm{Br}(\mathcal{E})/\mathrm{Br}_0(\mathcal{E}))[3] \to 0.$$

The Selmer group

Imposing all these local conditions will give us a subgroup of $H^1(K, E[3])$ that maps surjectively onto $(\mathrm{Br}(\mathcal{E})/\mathrm{Br}_0(\mathcal{E}))[3]$. We call the subgroup of $H^1(K, E[3])$ satisfying all the local conditions the (3-)*Selmer group* $S^{(3)}(K, E)$. This gives the following exact sequence

$$0 \to E(K)/3E(K) \to S^{(3)}(K, E) \to (\mathrm{Br}(\mathcal{E})/\mathrm{Br}_0(\mathcal{E}))[3] \to 0.$$

This is analagous to the Selmer group from performing descent on an elliptic curve defined over a number field. The Brauer group then plays the part of the Tate-Shafarevich group.

Example

Let $k = \mathbb{Q}(\zeta_3)$, and let $\mathcal{E}$ be the elliptic surface given by equation

$$y^2 + xy + \frac{1}{27}t^4 y = x^3.$$

Example

Let $k = \mathbb{Q}(\zeta_3)$, and let $\mathcal{E}$ be the elliptic surface given by equation

$$y^2 + xy + \frac{1}{27}t^4 y = x^3.$$

- The section $(x = 0, y = 0, t)$ gives a point of order 3 on the generic fibre E. So the curve S decomposes into five components.

Example

Let $k = \mathbb{Q}(\zeta_3)$, and let $\mathcal{E}$ be the elliptic surface given by equation

$$y^2 + xy + \frac{1}{27}t^4 y = x^3.$$

- The section $(x = 0, y = 0, t)$ gives a point of order 3 on the generic fibre E. So the curve S decomposes into five components.
- The bad fibres have reduction types

0	1	-1	$\pm i$	∞
I_{12}	I_1	I_1	I_1	IV^*

Example

The local conditions are:

Example

The local conditions are:

- $\mathrm{ord}_Q(a) \equiv 0 \mod 3$ for all $Q \in S$ except for those lying above $0, \pm 1, \pm i, \infty \in \mathbb{P}^1$.

Example

The local conditions are:

- $\mathrm{ord}_Q(a) \equiv 0 \mod 3$ for all $Q \in S$ except for those lying above $0, \pm 1, \pm i, \infty \in \mathbb{P}^1$.
- $\mathrm{ord}_Q(a) \equiv 0 \mod 3$ and $a(Q)$ is a perfect cube for $Q \in S$ on the identity component lying above $0, \pm 1, \pm i$.

Example

The local conditions are:

- $\mathrm{ord}_Q(a) \equiv 0 \mod 3$ for all $Q \in S$ except for those lying above $0, \pm 1, \pm i, \infty \in \mathbb{P}^1$.
- $\mathrm{ord}_Q(a) \equiv 0 \mod 3$ and $a(Q)$ is a perfect cube for $Q \in S$ on the identity component lying above $0, \pm 1, \pm i$.
- $\zeta_3^{\mathrm{ord}_{Q_1}(a)} a(Q_2)$ is a perfect cube for $Q_1, Q_2 \in S$ above ∞ (chosen in a specific way).

Example

The local conditions are:

- $\mathrm{ord}_Q(a) \equiv 0 \mod 3$ for all $Q \in S$ except for those lying above $0, \pm 1, \pm i, \infty \in \mathbb{P}^1$.
- $\mathrm{ord}_Q(a) \equiv 0 \mod 3$ and $a(Q)$ is a perfect cube for $Q \in S$ on the identity component lying above $0, \pm 1, \pm i$.
- $\zeta_3^{\mathrm{ord}_{Q_1}(a)} a(Q_2)$ is a perfect cube for $Q_1, Q_2 \in S$ above ∞ (chosen in a specific way).

Setting $a = \frac{t-1}{t+1}$ satisfies all of these local conditions.

Example

The corresponding central simple algebra is

$$A = \left(\frac{t-1}{t+1}, y \right)_3 .$$

Example

The corresponding central simple algebra is

$$A = \left(\frac{t-1}{t+1}, y\right)_3.$$

So we have found an element of $\mathrm{Br}(\mathcal{E})$.

Example

The corresponding central simple algebra is

$$A = \left(\frac{t-1}{t+1}, y\right)_3.$$

So we have found an element of $\mathrm{Br}(\mathcal{E})$. Evaluating this at the local point $(t = 1 - \zeta_3, x = 1, y = \ldots) \in \mathbb{Q}_3(\zeta_3)$ gives $\frac{1}{3}$, which is nonzero.

Example

The corresponding central simple algebra is

$$A = \left(\frac{t-1}{t+1}, y\right)_3.$$

So we have found an element of $\mathrm{Br}(\mathcal{E})$. Evaluating this at the local point $(t = 1 - \zeta_3, x = 1, y = \ldots) \in \mathbb{Q}_3(\zeta_3)$ gives $\frac{1}{3}$, which is nonzero.
Therefore A must take a nonzero value in a neigbourhood of the adelic point given by

$$P = \begin{cases} \text{identity point on a fibre} & v \neq 3 \\ (t = 1 - \zeta_3, x = 1, y = \ldots) & v = 3 \end{cases}$$

So A gives a Brauer-Manin obstruction to weak approximation on $\mathcal{E}$.

Thanks for listening!