Étale cohomology of points and curves

With an interlude into number theory

Gabriel Ribeiro

École Polytechnique

Summary

1. Brauer groups
2. Galois cohomology
3. Calculating étale cohomology

Brauer groups

Central simple algebras

Let k be a field. In this section, a *k-algebra* is a ring morphism $\varphi : k \to A$, where A is not necessarily commutative, such that $\varphi(k)$ is contained in the center of A.

Central simple algebras

Let k be a field. In this section, a *k-algebra* is a ring morphism $\varphi : k \to A$, where A is not necessarily commutative, such that $\varphi(k)$ is contained in the center of A. If, moreover, every nonzero element of A is invertible, A is a *division algebra*.

Central simple algebras

Let k be a field. In this section, a *k-algebra* is a ring morphism $\varphi : k \to A$, where A is not necessarily commutative, such that $\varphi(k)$ is contained in the center of A. If, moreover, every nonzero element of A is invertible, A is a *division algebra*.

Definition - Central simple algebra

Let A be a finite dimensional k-algebra. We say that A is *simple* if it has no two-sided ideal other than $\{0\}$ and A itself.

Central simple algebras

Let k be a field. In this section, a *k-algebra* is a ring morphism $\varphi : k \to A$, where A is not necessarily commutative, such that $\varphi(k)$ is contained in the center of A. If, moreover, every nonzero element of A is invertible, A is a *division algebra*.

Definition - Central simple algebra

Let A be a finite dimensional k-algebra. We say that A is *simple* if it has no two-sided ideal other than $\{0\}$ and A itself. Also, A is *central* if its center equals k.

Examples

Example - Division algebras

Let D be a division algebra over k.

Example - Division algebras

Let D be a division algebra over k. As with fields, any nonzero ideal contains 1 and so equals D. That is, D is simple.

Examples

Example - Division algebras

Let D be a division algebra over k. As with fields, any nonzero ideal contains 1 and so equals D. That is, D is simple.

Also, if $x \in Z(D)$ is nonzero, then x is invertible.

Example - Division algebras

Let D be a division algebra over k. As with fields, any nonzero ideal contains 1 and so equals D. That is, D is simple.

Also, if $x \in Z(D)$ is nonzero, then x is invertible. Inverting $xy = yx$, we get that $x^{-1} \in Z(D)$, proving that $Z(D)$ is a field.

Examples

Example - Division algebras

Let D be a division algebra over k. As with fields, any nonzero ideal contains 1 and so equals D. That is, D is simple.

Also, if $x \in Z(D)$ is nonzero, then x is invertible. Inverting $xy = yx$, we get that $x^{-1} \in Z(D)$, proving that $Z(D)$ is a field. Thus, D is a CSA over $Z(D)$.

Examples

Example - Division algebras

Let D be a division algebra over k. As with fields, any nonzero ideal contains 1 and so equals D. That is, D is simple.

Also, if $x \in Z(D)$ is nonzero, then x is invertible. Inverting $xy = yx$, we get that $x^{-1} \in Z(D)$, proving that $Z(D)$ is a field. Thus, D is a CSA over $Z(D)$.

If $D = \mathbb{H}$ is the quaternions, a quick calculation shows that $Z(\mathbb{H}) = \mathbb{R}$ and so $\mathbb{H}$ is a CSA over $\mathbb{R}$.

Examples

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

Examples

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

$M_n(D)$ is simple:

Examples

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

$M_n(D)$ is simple: it suffices to show that if $M \in M_n(D)$ is nonzero, then the ideal $\langle M \rangle = M_n(D)$.

Examples

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

$M_n(D)$ is simple: it suffices to show that if $M \in M_n(D)$ is nonzero, then the ideal $\langle M \rangle = M_n(D)$. Since the E_{ij} generate the D-module $M_n(D)$, it suffices to show that $E_{ij} \in \langle M \rangle$.

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

$M_n(D)$ is simple: it suffices to show that if $M \in M_n(D)$ is nonzero, then the ideal $\langle M \rangle = M_n(D)$. Since the E_{ij} generate the D-module $M_n(D)$, it suffices to show that $E_{ij} \in \langle M \rangle$. Actually, we can do even less: as $E_{ij}E_{jk}E_{kl} = E_{il}$, we may only show that $E_{ij} \in \langle M \rangle$ for some i, j.

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

$M_n(D)$ is simple: it suffices to show that if $M \in M_n(D)$ is nonzero, then the ideal $\langle M \rangle = M_n(D)$. Since the E_{ij} generate the D-module $M_n(D)$, it suffices to show that $E_{ij} \in \langle M \rangle$. Actually, we can do even less: as $E_{ij}E_{jk}E_{kl} = E_{il}$, we may only show that $E_{ij} \in \langle M \rangle$ for some i, j. Now, if $M_{ij} \neq 0$, it follows that $E_{ij} = M_{ij}^{-1}E_{ii}ME_{jj} \in \langle M \rangle$, and we're done.

$Z(M_n(D)) = Z(D)$:

Examples

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

$M_n(D)$ is simple: it suffices to show that if $M \in M_n(D)$ is nonzero, then the ideal $\langle M \rangle = M_n(D)$. Since the E_{ij} generate the D-module $M_n(D)$, it suffices to show that $E_{ij} \in \langle M \rangle$. Actually, we can do even less: as $E_{ij}E_{jk}E_{kl} = E_{il}$, we may only show that $E_{ij} \in \langle M \rangle$ for some i, j. Now, if $M_{ij} \neq 0$, it follows that $E_{ij} = M_{ij}^{-1} E_{ii} M E_{jj} \in \langle M \rangle$, and we're done.

$Z(M_n(D)) = Z(D)$: if M in $Z(M_n(D))$, then $E_{ij}M = ME_{ij}$ for all i, j.

Examples

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

$M_n(D)$ is simple: it suffices to show that if $M \in M_n(D)$ is nonzero, then the ideal $\langle M \rangle = M_n(D)$. Since the E_{ij} generate the D-module $M_n(D)$, it suffices to show that $E_{ij} \in \langle M \rangle$. Actually, we can do even less: as $E_{ij}E_{jk}E_{kl} = E_{il}$, we may only show that $E_{ij} \in \langle M \rangle$ for some i, j. Now, if $M_{ij} \neq 0$, it follows that $E_{ij} = M_{ij}^{-1} E_{ii} M E_{jj} \in \langle M \rangle$, and we're done.

$Z(M_n(D)) = Z(D)$: if M in $Z(M_n(D))$, then $E_{ij}M = ME_{ij}$ for all i, j. This implies that $M = d \cdot \mathrm{id}$, for some $d \in D$.

Proposition

Let D be a division algebra over k. Then $M_n(D)$ is a CSA over $Z(D)$.

$M_n(D)$ is simple: it suffices to show that if $M \in M_n(D)$ is nonzero, then the ideal $\langle M \rangle = M_n(D)$. Since the E_{ij} generate the D-module $M_n(D)$, it suffices to show that $E_{ij} \in \langle M \rangle$. Actually, we can do even less: as $E_{ij}E_{jk}E_{kl} = E_{il}$, we may only show that $E_{ij} \in \langle M \rangle$ for some i, j. Now, if $M_{ij} \neq 0$, it follows that $E_{ij} = M_{ij}^{-1}E_{ii}ME_{jj} \in \langle M \rangle$, and we're done.

$Z(M_n(D)) = Z(D)$: if M in $Z(M_n(D))$, then $E_{ij}M = ME_{ij}$ for all i, j. This implies that $M = d \cdot \mathrm{id}$, for some $d \in D$. Moreover, since M commutes with every matrix of the form $d' \cdot \mathrm{id}$, it follows that $d \in Z(D)$.

Wedderburn's theorem

Theorem - Wedderburn

Let A be a simple algebra over k. Then there's a unique integer $n \geq 1$ and a division algebra D over k such that $A \cong M_n(D)$.

Wedderburn's theorem

Theorem - Wedderburn

Let A be a simple algebra over k. Then there's a unique integer $n \geq 1$ and a division algebra D over k such that $A \cong M_n(D)$. Moreover, D is uniquely determined up to isomorphism.

Wedderburn's theorem

Theorem - Wedderburn

Let A be a simple algebra over k. Then there's a unique integer $n \geq 1$ and a division algebra D over k such that $A \cong M_n(D)$. Moreover, D is uniquely determined up to isomorphism.

We won't have time to prove this today, but please check the proof in [GS, Theorem 2.1.3]. It's absolutely wonderful.

Corollaries of Wedderburn's thm

Corollary

The center of a finite-dimensional simple algebra is a field.

Corollaries of Wedderburn's thm

Corollary

The center of a finite-dimensional simple algebra is a field.

Indeed, $A \cong M_n(D)$ and $Z(A) \cong Z(D)$, which is a field.

Corollaries of Wedderburn's thm

Corollary

The center of a finite-dimensional simple algebra is a field.

Indeed, $A \cong M_n(D)$ and $Z(A) \cong Z(D)$, which is a field.

Corollary

If $k = \bar{k}$, every CSA over k is isomorphic to $M_n(k)$ for some $n \geq 1$.

Corollaries of Wedderburn's thm

Corollary

The center of a finite-dimensional simple algebra is a field.

Indeed, $A \cong M_n(D)$ and $Z(A) \cong Z(D)$, which is a field.

Corollary

If $k = \bar{k}$, every CSA over k is isomorphic to $M_n(k)$ for some $n \geq 1$.

It suffices to show that the only (finite-dimensional) division algebra D over k is k itself.

Corollaries of Wedderburn's thm

Corollary

The center of a finite-dimensional simple algebra is a field.

Indeed, $A \cong M_n(D)$ and $Z(A) \cong Z(D)$, which is a field.

Corollary

If $k = \overline{k}$, every CSA over k is isomorphic to $M_n(k)$ for some $n \geq 1$.

It suffices to show that the only (finite-dimensional) division algebra D over k is k itself. If there exists some $a \in D \setminus k$, $k[a]$ is a finite extension of k.

Corollaries of Wedderburn's thm

Corollary

The center of a finite-dimensional simple algebra is a field.

Indeed, $A \cong M_n(D)$ and $Z(A) \cong Z(D)$, which is a field.

Corollary

If $k = \overline{k}$, every CSA over k is isomorphic to $M_n(k)$ for some $n \geq 1$.

It suffices to show that the only (finite-dimensional) division algebra D over k is k itself. If there exists some $a \in D \setminus k$, $k[a]$ is a finite extension of k. Absurd!

Stability under tensor product

Theorem

Let A and B be k-algebras. Then $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$. In particular, if A and B are central, so is $A \otimes_k B$.

Stability under tensor product

Theorem

Let A and B be k-algebras. Then $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$. In particular, if A and B are central, so is $A \otimes_k B$. If, moreover, they're simple, then $A \otimes_k B$ is a CSA.

Stability under tensor product

Theorem

Let A and B be k-algebras. Then $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$. In particular, if A and B are central, so is $A \otimes_k B$. If, moreover, they're simple, then $A \otimes_k B$ is a CSA.

That's another cool proof, you should check out! (My favorite proof is, of course, the one in my notes about Brauer groups. 🤭)

More important corollaria

Corollary

Let K/k be a field extension and A a finite dimensional k-algebra. Then A is a CSA iff $A_K = A \otimes_k K$ is.

More important corollaria

Corollary

Let K/k be a field extension and A a finite dimensional k-algebra. Then A is a CSA iff $A_K = A \otimes_k K$ is.

One direction follows from the preceding theorem.

More important corollaria

Corollary

Let K/k be a field extension and A a finite dimensional k-algebra. Then A is a CSA iff $A_K = A \otimes_k K$ is.

One direction follows from the preceding theorem. Conversely, if A_K is simple central, the formula for the center implies that A is central. (For $Z(A) \otimes_k K = K$.)

More important corollaria

Corollary

Let K/k be a field extension and A a finite dimensional k-algebra. Then A is a CSA iff $A_K = A \otimes_k K$ is.

One direction follows from the preceding theorem. Conversely, if A_K is simple central, the formula for the center implies that A is central. (For $Z(A) \otimes_k K = K$.) Also, if I is a non-trivial two-sided ideal of A, then $I \otimes_k K$ is a non-trivial two-sided ideal of A_K by faithful flatness of K; finishing the proof.

More important corollaria

Let A be a finite dimensional k-algebra. If K/k is a field extension such that $A_K \cong M_n(K)$ for some $n \geq 1$, we say that K is a splitting field for A, or that A splits over K.

More important corollaria

Let A be a finite dimensional k-algebra. If K/k is a field extension such that $A_K \cong M_n(K)$ for some $n \geq 1$, we say that K is a splitting field for A, or that A splits over K.

Corollary

Let A be a finite dimensional k-algebra. Then A is a CSA iff it splits over some finite Galois extension of k.

More important corollaria

Let A be a finite dimensional k-algebra. If K/k is a field extension such that $A_K \cong M_n(K)$ for some $n \geq 1$, we say that K is a splitting field for A, or that A splits over K.

Corollary

Let A be a finite dimensional k-algebra. Then A is a CSA iff it splits over some finite Galois extension of k.

Sufficiency follows from the previous corollary.

More important corollaria

Let A be a finite dimensional k-algebra. If K/k is a field extension such that $A_K \cong M_n(K)$ for some $n \geq 1$, we say that K is a splitting field for A, or that A splits over K.

Corollary

Let A be a finite dimensional k-algebra. Then A is a CSA iff it splits over some finite Galois extension of k.

Sufficiency follows from the previous corollary. For necessity, observe that $A_{\bar{k}} \cong M_n(\bar{k})$ for some $n \geq 1$.

More important corollaria

Let A be a finite dimensional k-algebra. If K/k is a field extension such that $A_K \cong M_n(K)$ for some $n \geq 1$, we say that K is a splitting field for A, or that A splits over K.

Corollary

Let A be a finite dimensional k-algebra. Then A is a CSA iff it splits over some finite Galois extension of k.

Sufficiency follows from the previous corollary. For necessity, observe that $A_{\bar{k}} \cong M_n(\bar{k})$ for some $n \geq 1$. By flatness,

$$A_{\bar{k}} = A \otimes_k \bar{k} = \bigcup_K A \otimes_k K = \bigcup_K A_K,$$

where K ranges over all finite extensions of K contained in $\bar{k}$.

More important corollaria

Let A be a finite dimensional k-algebra. If K/k is a field extension such that $A_K \cong M_n(K)$ for some $n \geq 1$, we say that K is a splitting field for A, or that A splits over K.

Corollary

Let A be a finite dimensional k-algebra. Then A is a CSA iff it splits over some finite Galois extension of k.

Sufficiency follows from the previous corollary. For necessity, observe that $A_{\bar{k}} \cong M_n(\bar{k})$ for some $n \geq 1$. By flatness,

$$A_{\bar{k}} = A \otimes_k \bar{k} = \bigcup_K A \otimes_k K = \bigcup_K A_K,$$

where K ranges over all finite extensions of K contained in $\bar{k}$. Some K large enough contains a basis (e_i) of $M_n(\bar{k})$, so we may map (e_i) to the standard basis of $M_n(K)$; yielding an isomorphism $A_K \cong M_n(K)$.

More important corollaria

Let A be a finite dimensional k-algebra. If K/k is a field extension such that $A_K \cong M_n(K)$ for some $n \geq 1$, we say that K is a splitting field for A, or that A splits over K.

Corollary

Let A be a finite dimensional k-algebra. Then A is a CSA iff it splits over some finite Galois extension of k.

Sufficiency follows from the previous corollary. For necessity, observe that $A_{\bar{k}} \cong M_n(\bar{k})$ for some $n \geq 1$. By flatness,

$$A_{\bar{k}} = A \otimes_k \bar{k} = \bigcup_K A \otimes_k K = \bigcup_K A_K,$$

where K ranges over all finite extensions of K contained in $\bar{k}$. Some K large enough contains a basis (e_i) of $M_n(\bar{k})$, so we may map (e_i) to the standard basis of $M_n(K)$; yielding an isomorphism $A_K \cong M_n(K)$. Proving that K may be taken Galois is a little harder.

Noether-Skolem

The last fundamental theorem on central simple algebras is the following.

Theorem - Noether-Skolem

All automorphisms of a central simple algebra are inner.

Noether-Skolem

The last fundamental theorem on central simple algebras is the following.

Theorem - Noether-Skolem

All automorphisms of a central simple algebra are inner.

I have two interesting proofs of this in my notes. You should take a look at 'em!

Reduced norm

Let's put all these theorems to use!

Reduced norm

Let's put all these theorems to use! Let A be a CSA over k. We define its *reduced norm* to be the composition

$$\mathrm{Nrd} : A \to A_{\bar{k}} \cong M_n(\bar{k}) \xrightarrow{\det} \bar{k}.$$

Reduced norm

Let's put all these theorems to use! Let A be a CSA over k. We define its *reduced norm* to be the composition

$$\mathrm{Nrd} : A \to A_{\bar{k}} \cong M_n(\bar{k}) \xrightarrow{\det} \bar{k}.$$

Proposition

The image of Nrd is contained in k.

Reduced norm

Let's put all these theorems to use! Let A be a CSA over k. We define its *reduced norm* to be the composition

$$\mathrm{Nrd} : A \to A_{\bar{k}} \cong M_n(\bar{k}) \xrightarrow{\det} \bar{k}.$$

Proposition

The image of Nrd is contained in k.

Let $\psi \in \mathrm{Aut}(M_n(\bar{k} \otimes_k \bar{k}))$ be defined by the commutative diagram

$$\begin{array}{ccc} A \otimes_k \bar{k} \otimes_k \bar{k} & \xrightarrow{\sim} & M_n(\bar{k} \otimes_k \bar{k}) \\ \downarrow & & \downarrow \psi \\ \bar{k} \otimes_k A \otimes_k \bar{k} & \xrightarrow{\sim} & M_n(\bar{k} \otimes_k \bar{k}), \end{array}$$

where the arrow on the left is $x \otimes a \otimes y \mapsto a \otimes x \otimes y$.

Reduced norm

By Noether-Skolem, ψ is inner and so $\det(A) = \det(\psi(A))$ for all $A \in M_n(\overline{k} \otimes_k \overline{k})$.

Reduced norm

By Noether-Skolem, ψ is inner and so $\det(A) = \det(\psi(A))$ for all $A \in M_n(\bar{k} \otimes_k \bar{k})$. In particular, if $\alpha : A \otimes_k \bar{k} \to M_n(\bar{k})$ is the natural isomorphism,

$$\det(\alpha(a \otimes 1)) \otimes 1 = 1 \otimes \det(\alpha(a \otimes 1)) \in \bar{k} \otimes_k \bar{k}.$$

Reduced norm

By Noether-Skolem, ψ is inner and so $\det(A) = \det(\psi(A))$ for all $A \in M_n(\bar{k} \otimes_k \bar{k})$. In particular, if $\alpha : A \otimes_k \bar{k} \to M_n(\bar{k})$ is the natural isomorphism,

$$\det(\alpha(a \otimes 1)) \otimes 1 = 1 \otimes \det(\alpha(a \otimes 1)) \in \bar{k} \otimes_k \bar{k}.$$

But the second fundamental lemma of last week says that the sequence

$$0 \longrightarrow k \longrightarrow \bar{k} \xrightarrow{\delta} \bar{k} \otimes_k \bar{k},$$

where $\delta(x) = x \otimes 1 - 1 \otimes x$, is exact.

Reduced norm

By Noether-Skolem, ψ is inner and so $\det(A) = \det(\psi(A))$ for all $A \in M_n(\bar{k} \otimes_k \bar{k})$. In particular, if $\alpha : A \otimes_k \bar{k} \to M_n(\bar{k})$ is the natural isomorphism,

$$\det(\alpha(a \otimes 1)) \otimes 1 = 1 \otimes \det(\alpha(a \otimes 1)) \in \bar{k} \otimes_k \bar{k}.$$

But the second fundamental lemma of last week says that the sequence

$$0 \longrightarrow k \longrightarrow \bar{k} \xrightarrow{\delta} \bar{k} \otimes_k \bar{k},$$

where $\delta(x) = x \otimes 1 - 1 \otimes x$, is exact. It follows that

$$\mathrm{Nrd}(a) = \det(\alpha(a \otimes 1)) \in k.$$

Reduced norm

Basically the same idea shows that we may take any splitting field in the definition of Nrd.

Reduced norm

Basically the same idea shows that we may take any splitting field in the definition of Nrd. We actually have even more: we may associate a *reduced characteristic polynomial* to elements of A, which has coefficients in k.

Reduced norm

Basically the same idea shows that we may take any splitting field in the definition of Nrd. We actually have even more: we may associate a *reduced characteristic polynomial* to elements of A, which has coefficients in k.

We also remark that $a \in A$ is invertible iff $\mathrm{Nrd}(a) \neq 0$, and that $N_{A/k}(a) = \mathrm{Nrd}(a)^n$, where $\dim_k A = n^2$.

Brauer group

Our theorems will also allow us to define a group classifying division algebras over k.

Brauer group

Our theorems will also allow us to define a group classifying division algebras over k.

Definition - Brauer equivalence

Two CSAs are said to be *Brauer equivalent* if their underlying division algebras are isomorphic.

Brauer group

Our theorems will also allow us to define a group classifying division algebras over k.

Definition - Brauer equivalence

Two CSAs are said to be *Brauer equivalent* if their underlying division algebras are isomorphic.

This notion has interesting characterizations.

Proposition

Let A and B be two CSAs over k. TFAE:

- A and B are Brauer equivalent;

Brauer group

Our theorems will also allow us to define a group classifying division algebras over k.

Definition - Brauer equivalence

Two CSAs are said to be *Brauer equivalent* if their underlying division algebras are isomorphic.

This notion has interesting characterizations.

Proposition

Let A and B be two CSAs over k. TFAE:

- A and B are Brauer equivalent;
- $M_n(A) = A \otimes_k M_n(k) \cong B \otimes_k M_m(k) = M_m(k)$ for some n, m;

Brauer group

Our theorems will also allow us to define a group classifying division algebras over k.

Definition - Brauer equivalence

Two CSAs are said to be *Brauer equivalent* if their underlying division algebras are isomorphic.

This notion has interesting characterizations.

Proposition

Let A and B be two CSAs over k. TFAE:

- A and B are Brauer equivalent;
- $M_n(A) = A \otimes_k M_n(k) \cong B \otimes_k M_m(k) = M_m(k)$ for some n, m;
- A and B are Morita equivalent.

Brauer group

Our theorems will also allow us to define a group classifying division algebras over k.

Definition - Brauer equivalence

Two CSAs are said to be *Brauer equivalent* if their underlying division algebras are isomorphic.

This notion has interesting characterizations.

Proposition

Let A and B be two CSAs over k. TFAE:

- A and B are Brauer equivalent;
- $M_n(A) = A \otimes_k M_n(k) \cong B \otimes_k M_m(k) = M_m(k)$ for some n, m;
- A and B are Morita equivalent.

Brauer group

Our theorems will also allow us to define a group classifying division algebras over k.

Definition - Brauer equivalence

Two CSAs are said to be *Brauer equivalent* if their underlying division algebras are isomorphic.

This notion has interesting characterizations.

Proposition

Let A and B be two CSAs over k. TFAE:

- A and B are Brauer equivalent;
- $M_n(A) = A \otimes_k M_n(k) \cong B \otimes_k M_m(k) = M_m(k)$ for some n, m;
- A and B are Morita equivalent.

By the 2nd point, every equivalence class contains precisely one division algebra.

Brauer group

The following def motivates much of the theory.

Brauer group

The following def motivates much of the theory.

Definition - Brauer group

The *Brauer group* of a field k is the group $\mathrm{Br}(k)$ composed by the equivalence classes of CSAs over k, under the tensor product.

The following def motivates much of the theory.

Definition - Brauer group

The *Brauer group* of a field k is the group $\mathrm{Br}(k)$ composed by the equivalence classes of CSAs over k, under the tensor product.

As we saw, if $k = \overline{k}$, every CSA over k is isomorphic to $M_n(k)$ for some $n \geq 1$; yielding that $\mathrm{Br}(\overline{k}) = 0$.

Brauer group

The following def motivates much of the theory.

Definition - Brauer group

The *Brauer group* of a field k is the group $\mathrm{Br}(k)$ composed by the equivalence classes of CSAs over k, under the tensor product.

As we saw, if $k = \bar{k}$, every CSA over k is isomorphic to $M_n(k)$ for some $n \geq 1$; yielding that $\mathrm{Br}(\bar{k}) = 0$. We'll also consider a relative variant.

Definition - Brauer group

Let K/k be a field extension and consider the *restriction map*

$$\begin{aligned} \mathrm{res} : \mathrm{Br}(k) &\to \mathrm{Br}(K) \\ [A] &\mapsto [A_K]. \end{aligned}$$

The *relative Brauer group* $\mathrm{Br}(K/k)$ is the kernel of res.

C_1 fields

We can actually give a better reason for the fact that $\mathrm{Br}(\overline{k}) = 0$!

C_1 fields

We can actually give a better reason for the fact that $\mathrm{Br}(\overline{k}) = 0$!

Definition

A field k is said to be C_1 if every homogeneous $f \in k[x_1, \ldots, x_n]$ of degree $d < n$ has a nontrivial zero.

C_1 fields

We can actually give a better reason for the fact that $\mathrm{Br}(\overline{k}) = 0$!

Definition

A field k is said to be C_1 if every homogeneous $f \in k[x_1, \ldots, x_n]$ of degree $d < n$ has a nontrivial zero.

Algebraically closed fields are C_1.

C_1 fields

We can actually give a better reason for the fact that $\mathrm{Br}(\overline{k}) = 0$!

Definition

A field k is said to be C_1 if every homogeneous $f \in k[x_1, \ldots, x_n]$ of degree $d < n$ has a nontrivial zero.

Algebraically closed fields are C_1. The reason d'être of this condition is the following result.

Proposition

Let k be a C_1 field. Then $\mathrm{Br}(k) = 0$.

C_1 fields

We can actually give a better reason for the fact that $\mathrm{Br}(\overline{k}) = 0$!

Definition

A field k is said to be C_1 if every homogeneous $f \in k[x_1, \ldots, x_n]$ of degree $d < n$ has a nontrivial zero.

Algebraically closed fields are C_1. The reason d'être of this condition is the following result.

Proposition

Let k be a C_1 field. Then $\mathrm{Br}(k) = 0$.

Let's prove this!

C_1 fields

Let D be a division algebra of dimension n^2 over k.

C_1 fields

Let D be a division algebra of dimension n^2 over k. Given a basis $e_1, \dots, e_{n^2}$ of D over k, the polynomial

$$f(x_1, \dots, x_{n^2}) := N(x_1 e_1 + \cdots x_{n^2} e_{n^2})$$

is homogeneous with degree n in n^2 variables with no non-trivial zeros.

C_1 fields

Let D be a division algebra of dimension n^2 over k. Given a basis $e_1, \dots, e_{n^2}$ of D over k, the polynomial

$$f(x_1, \dots, x_{n^2}) := N(x_1 e_1 + \cdots x_{n^2} e_{n^2})$$

is homogeneous with degree n in n^2 variables with no non-trivial zeros. If $n > 1$ this contradicts the C_1 condition.

Chevalley-Warning

Theorem - Chevalley-Warning

Let $k = \mathbb{F}_q$ be a finite field of characteristic p and $f \in k[x_1, \ldots, x_n]$ of degree $d < n$. The number of solutions of $f = 0$ is divisible by p.

Theorem - Chevalley-Warning

Let $k = \mathbb{F}_q$ be a finite field of characteristic p and $f \in k[x_1, \ldots, x_n]$ of degree $d < n$. The number of solutions of $f = 0$ is divisible by p.

Since $x^{q-1} = 1$ for all $x \in k \setminus \{0\}$, the number mod p of solutions is

$$\sum_{x \in k^n} \left(1 - f(x)^{q-1}\right).$$

Chevalley-Warning

Theorem - Chevalley-Warning

Let $k = \mathbb{F}_q$ be a finite field of characteristic p and $f \in k[x_1, \ldots, x_n]$ of degree $d < n$. The number of solutions of $f = 0$ is divisible by p.

Since $x^{q-1} = 1$ for all $x \in k \setminus \{0\}$, the number mod p of solutions is

$$\sum_{x \in k^n} \left(1 - f(x)^{q-1}\right).$$

We prove that every monomial of $1 - f^{q-1}$ sums to $0 \in k$. Let $x_1^{a_1} \cdots x_n^{a_n}$ be one such monomial.

Theorem - Chevalley-Warning

Let $k = \mathbb{F}_q$ be a finite field of characteristic p and $f \in k[x_1, \ldots, x_n]$ of degree $d < n$. The number of solutions of $f = 0$ is divisible by p.

Since $x^{q-1} = 1$ for all $x \in k \setminus \{0\}$, the number mod p of solutions is

$$\sum_{x \in k^n} \left(1 - f(x)^{q-1}\right).$$

We prove that every monomial of $1 - f^{q-1}$ sums to $0 \in k$. Let $x_1^{a_1} \cdots x_n^{a_n}$ be one such monomial. Since its degree is $< (q-1)n$, we have $a_i < q - 1$ for at least one i. Let j be this index.

Recall that $a_j < q - 1$. As

$$\sum_{(x_i) \in k^n} x_1^{a_1} \dots x_n^{a_n} = \prod_{i=1}^{n} \left(\sum_{x_i \in k} x_i^{a_i} \right),$$

it suffices to show that $\sum_{x_j \in k} x_j^{a_j} = 0$.

Recall that $a_j < q - 1$. As

$$\sum_{(x_i) \in k^n} x_1^{a_1} \dots x_n^{a_n} = \prod_{i=1}^{n} \left(\sum_{x_i \in k} x_i^{a_i} \right),$$

it suffices to show that $\sum_{x_j \in k} x_j^{a_j} = 0$. If $a_j = 0$, this is clear.

Chevalley-Warning

Recall that $a_j < q-1$. As

$$\sum_{(x_i)\in k^n} x_1^{a_1}\dots x_n^{a_n} = \prod_{i=1}^{n}\left(\sum_{x_i\in k} x_i^{a_i}\right),$$

it suffices to show that $\sum_{x_j\in k} x_j^{a_j} = 0$. If $a_j = 0$, this is clear. Else, let y be a generator of $k^\times$. Then,

$$\sum_{x_j\in k} x_j^{a_j} = \sum_{x_j\in k^\times} x_j^{a_j} = \sum_{m=0}^{q-2}(y^m)^{a_j} = \sum_{m=0}^{q-2}(y^{a_j})^m = \frac{1-(y^{a_j})^{q-1}}{1-y^{a_j}} = 0,$$

concluding our proof.

Tsen's theorem

Theorem - Tsen

Let k be an algebraically closed field and K be the function field of an algebraic curve over k. Then K is C_1.

Tsen's theorem

Theorem - Tsen

Let k be an algebraically closed field and K be the function field of an algebraic curve over k. Then K is C_1.

By Noether normalization, we may assume that $K = k(t)$. (Little HW: prove that if K is C_1, so is every finite extension.)

Tsen's theorem

Theorem - Tsen

Let k be an algebraically closed field and K be the function field of an algebraic curve over k. Then K is C_1.

By Noether normalization, we may assume that $K = k(t)$. (Little HW: prove that if K is C_1, so is every finite extension.)

Given $f \in k(t)[x_1, \ldots, x_n]$ of degree $d < n$, we may also assume the coefs to be in $k[t]$ and look for solutions in $k[t]^n$.

Tsen's theorem

Theorem - Tsen

Let k be an algebraically closed field and K be the function field of an algebraic curve over k. Then K is C_1.

By Noether normalization, we may assume that $K = k(t)$. (Little HW: prove that if K is C_1, so is every finite extension.)

Given $f \in k(t)[x_1, \ldots, x_n]$ of degree $d < n$, we may also assume the coefs to be in $k[t]$ and look for solutions in $k[t]^n$. So, let's fix (for now) an integer $N > 0$ and look for x_i of the form

$$x_i = \sum_{j=0}^{N} a_{ij} t^j,$$

where the $a_{ij} \in k$ are to be determined.

Tsen's theorem

Plugging this into the equation $f = 0$, we get a decomposition

$$0 = f(x_1, \ldots, x_n) = \sum_{l=0}^{dN+r} f_l(a_{10}, \ldots, a_{nN})t^l,$$

where r is the maximal degree of the coefs of f, and the f_l are homogeneous polynomials in the a_{ij}.

Tsen's theorem

Plugging this into the equation $f = 0$, we get a decomposition

$$0 = f(x_1, \ldots, x_n) = \sum_{l=0}^{dN+r} f_l(a_{10}, \ldots, a_{nN})t^l,$$

where r is the maximal degree of the coefs of f, and the f_l are homogeneous polynomials in the a_{ij}. Since $d < n$, for $N \gg 1$ the number $dN + r + 1$ of polynomials f_l is smaller than the number $n(N + 1)$ of indeterminates a_{ij}.

Tsen's theorem

Plugging this into the equation $f = 0$, we get a decomposition

$$0 = f(x_1, \ldots, x_n) = \sum_{l=0}^{dN+r} f_l(a_{10}, \ldots, a_{nN})t^l,$$

where r is the maximal degree of the coefs of f, and the f_l are homogeneous polynomials in the a_{ij}. Since $d < n$, for $N \gg 1$ the number $dN + r + 1$ of polynomials f_l is smaller than the number $n(N + 1)$ of indeterminates a_{ij}. Now, in the chain

$$V(f_0) \supset V(f_0, f_1) \supset \cdots \supset V(f_0, \ldots, f_{dN+r})$$

of closed sets in $\mathbb{P}^{nN+n-1}$, the dimension drops by at most one in each step, proving that $V(f_0, \ldots, f_{dN+r})$ is positive dimensional and so contains a k point.

Tsen's theorem

Plugging this into the equation $f = 0$, we get a decomposition

$$0 = f(x_1, \ldots, x_n) = \sum_{l=0}^{dN+r} f_l(a_{10}, \ldots, a_{nN})t^l,$$

where r is the maximal degree of the coefs of f, and the f_l are homogeneous polynomials in the a_{ij}. Since $d < n$, for $N \gg 1$ the number $dN + r + 1$ of polynomials f_l is smaller than the number $n(N+1)$ of indeterminates a_{ij}. Now, in the chain

$$V(f_0) \supset V(f_0, f_1) \supset \cdots \supset V(f_0, \ldots, f_{dN+r})$$

of closed sets in $\mathbb{P}^{nN+n-1}$, the dimension drops by at most one in each step, proving that $V(f_0, \ldots, f_{dN+r})$ is positive dimensional and so contains a k point. That is, we have some a_{ij} composing a nontrivial zero of f.

Galois cohomology

Elements of group cohomology

For this whole section, let G be a finite group.

For this whole section, let G be a finite group.

Definition

The category of G-*modules* is the category of left modules over the group algebra $\mathbb{Z}[G]$.

Elements of group cohomology

For this whole section, let G be a finite group.

Definition

The category of *G-modules* is the category of left modules over the group algebra $\mathbb{Z}[G]$.

A surprisingly important example is the abelian group $\mathbb{Z}$, along with the trivial action of G.

Elements of group cohomology

For this whole section, let G be a finite group.

Definition

The category of *G-modules* is the category of left modules over the group algebra $\mathbb{Z}[G]$.

A surprisingly important example is the abelian group $\mathbb{Z}$, along with the trivial action of G.

As usual, this category has all the nice bells and whistles. Particularly, it has enough injectives and projectives.

Elements of group cohomology

In particular, we may define the cohomology of a G-module.

Definition

For a G-module M, denote by M^G the submodule defined by the $x \in M$ satisfying $g \cdot x = x$ for all $g \in G$.

In particular, we may define the cohomology of a G-module.

Definition

For a G-module M, denote by M^G the submodule defined by the $x \in M$ satisfying $g \cdot x = x$ for all $g \in G$. Since $M^G = \mathrm{Hom}_G(\mathbb{Z}, M)$, $(-)^G$ is left exact.

Elements of group cohomology

In particular, we may define the cohomology of a G-module.

Definition

For a G-module M, denote by M^G the submodule defined by the $x \in M$ satisfying $g \cdot x = x$ for all $g \in G$. Since $M^G = \mathrm{Hom}_G(\mathbb{Z}, M)$, $(-)^G$ is left exact. We denote its right derived functor by $H^i(G, -) = \mathrm{Ext}^i_G(\mathbb{Z}, -)$.

Since Ext's may be also calculated using projective resolutions of the first fact, the following lemma is very useful.

Since Ext's may be also calculated using projective resolutions of the first fact, the following lemma is very useful.

Lemma

The sequence

$$\cdots \to \mathbb{Z}[G^3] \xrightarrow{d_2} \mathbb{Z}[G^2] \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{d_0} \mathbb{Z} \to 0,$$

where $d_n(g_0, \ldots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_n)$, is exact. In particular, its a free (hence projective) resolution of $\mathbb{Z}$.

Elements of group cohomology

Since Ext's may be also calculated using projective resolutions of the first fact, the following lemma is very useful.

Lemma

The sequence

$$\cdots \to \mathbb{Z}[G^3] \xrightarrow{d_2} \mathbb{Z}[G^2] \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{d_0} \mathbb{Z} \to 0,$$

where $d_n(g_0, \ldots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_n)$, is exact. In particular, its a free (hence projective) resolution of $\mathbb{Z}$.

By applying the functor $\mathrm{Hom}_G(-, M)$ (and dropping the last term) we obtain a very explicit description of the complex $\mathrm{R}\,\mathrm{Hom}_G(\mathbb{Z}, M)$, whose i-th cohomology is $H^i(G, M)$.

We won't go further in the cohomology of finite groups, since we won't need much. But we urge the reader to read more about it, for this simple theory has a lot of similarities with other cohomology theories.

Elements of group cohomology

We won't go further in the cohomology of finite groups, since we won't need much. But we urge the reader to read more about it, for this simple theory has a lot of similarities with other cohomology theories.

Examples: there exists a cup product

$$\cup : H^i(G, M) \otimes H^j(G, N) \to H^{i+j}(G, M \otimes N),$$

very similar to the wedge product of differential forms in de Rham cohomology.

Elements of group cohomology

We won't go further in the cohomology of finite groups, since we won't need much. But we urge the reader to read more about it, for this simple theory has a lot of similarities with other cohomology theories.

Examples: there exists a cup product

$$\cup : H^i(G, M) \otimes H^j(G, N) \to H^{i+j}(G, M \otimes N),$$

very similar to the wedge product of differential forms in de Rham cohomology. There exists the so called *Herbrand quotient*, analogous to the Euler characteristic in topology.

Elements of group cohomology

We won't go further in the cohomology of finite groups, since we won't need much. But we urge the reader to read more about it, for this simple theory has a lot of similarities with other cohomology theories.

Examples: there exists a cup product

$$\cup : H^i(G, M) \otimes H^j(G, N) \to H^{i+j}(G, M \otimes N),$$

very similar to the wedge product of differential forms in de Rham cohomology. There exists the so called *Herbrand quotient*, analogous to the Euler characteristic in topology. There's a Kunneth formula...

If k is a field, its *absolute Galois group* $G_k := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ is the projective limit of $\mathrm{Gal}(K/k)$, where K runs over all finite Galois extensions of k.

Cohomology of profinite groups

If k is a field, its *absolute Galois group* $G_k := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ is the projective limit of $\mathrm{Gal}(K/k)$, where K runs over all finite Galois extensions of k. This gives G_k the structure of a profinite group.

Cohomology of profinite groups

If k is a field, its *absolute Galois group* $G_k := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ is the projective limit of $\mathrm{Gal}(K/k)$, where K runs over all finite Galois extensions of k. This gives G_k the structure of a profinite group. In what follows G will always be a profinite group.

Cohomology of profinite groups

If k is a field, its *absolute Galois group* $G_k := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ is the projective limit of $\mathrm{Gal}(K/k)$, where K runs over all finite Galois extensions of k. This gives G_k the structure of a profinite group. In what follows G will always be a profinite group.

Definition

Let M be a discrete $\mathbb{Z}[G]$-module. We say that M is a G-module if G acts continuously on M.

If k is a field, its *absolute Galois group* $G_k := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ is the projective limit of $\mathrm{Gal}(K/k)$, where K runs over all finite Galois extensions of k. This gives G_k the structure of a profinite group. In what follows G will always be a profinite group.

Definition

Let M be a discrete $\mathbb{Z}[G]$-module. We say that M is a G-module if G acts continuously on M. That is, if for all $x \in M$, the map $g \mapsto g \cdot x$ is continuous.

If k is a field, its *absolute Galois group* $G_k := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ is the projective limit of $\mathrm{Gal}(K/k)$, where K runs over all finite Galois extensions of k. This gives G_k the structure of a profinite group. In what follows G will always be a profinite group.

Definition

Let M be a discrete $\mathbb{Z}[G]$-module. We say that M is a G-module if G acts continuously on M. That is, if for all $x \in M$, the map $g \mapsto g \cdot x$ is continuous.

The category of G-modules is a full abelian subcategory of $\mathbb{Z}[G]$-Mod, which has enough injectives but not enough projectives.

Examples

If G is a commutative algebraic group over k, G_k acts naturally on $G(k_{\mathrm{sep}})$.

Examples

If G is a commutative algebraic group over k, G_k acts naturally on $G(k_{\mathrm{sep}})$. In particular, we obtain the following G_k-modules:

- $\underline{M}(k_{\mathrm{sep}}) = M$;

Examples

If G is a commutative algebraic group over k, G_k acts naturally on $G(k_{\text{sep}})$. In particular, we obtain the following G_k-modules:

- $\underline{M}(k_{\text{sep}}) = M$;
- $\mathbb{G}_a(k_{\text{sep}}) = k_{\text{sep}}$;

Examples

If G is a commutative algebraic group over k, G_k acts naturally on $G(k_{\text{sep}})$. In particular, we obtain the following G_k-modules:

- $\underline{M}(k_{\text{sep}}) = M$;
- $\mathbb{G}_a(k_{\text{sep}}) = k_{\text{sep}}$;
- $\mathbb{G}_m(k_{\text{sep}}) = k_{\text{sep}}^{\times}$;

Examples

If G is a commutative algebraic group over k, G_k acts naturally on $G(k_{\mathrm{sep}})$. In particular, we obtain the following G_k-modules:

- $\underline{M}(k_{\mathrm{sep}}) = M$;
- $\mathbb{G}_a(k_{\mathrm{sep}}) = k_{\mathrm{sep}}$;
- $\mathbb{G}_m(k_{\mathrm{sep}}) = k_{\mathrm{sep}}^{\times}$;
- $\mu_n(k_{\mathrm{sep}}) = \{x \in k_{\mathrm{sep}} \mid x^n = 1\}$.

Since G-Mod has enough injectives, we could simply define the right derived functors of $M \mapsto M^G$.

Cohomology of profinite groups

Since G-Mod has enough injectives, we could simply define the right derived functors of $M \mapsto M^G$. But we would lose the explicit description.

Cohomology of profinite groups

Since G-Mod has enough injectives, we could simply define the right derived functors of $M \mapsto M^G$. But we would lose the explicit description. So, we make the following def:

Definition

Let G be a profinite group and M a G-module. We define

$$H^i(G, M) := \operatorname*{colim}_U H^i(G/U, A^U),$$

where U runs through the open normal subgroups of G. (Which are all of finite index.)

Cohomology of profinite groups

Since G-Mod has enough injectives, we could simply define the right derived functors of $M \mapsto M^G$. But we would lose the explicit description. So, we make the following def:

Definition

Let G be a profinite group and M a G-module. We define

$$H^i(G, M) := \operatorname*{colim}_U H^i(G/U, A^U),$$

where U runs through the open normal subgroups of G. (Which are all of finite index.)

With this definition, the explicit description still works (the only change is that we consider continuous cochains).

Cohomology of profinite groups

Since G-Mod has enough injectives, we could simply define the right derived functors of $M \mapsto M^G$. But we would lose the explicit description. So, we make the following def:

Definition

Let G be a profinite group and M a G-module. We define

$$H^i(G, M) := \operatorname*{colim}_U H^i(G/U, A^U),$$

where U runs through the open normal subgroups of G. (Which are all of finite index.)

With this definition, the explicit description still works (the only change is that we consider continuous cochains). Basically all the theory of finite groups keeps working in this context.

Cohomology of the additive group

Proposition

Let K/k be a finite Galois extension. Then $H^i(\mathrm{Gal}(K/k), K) = 0$ for all $i > 0$. In particular, $H^i(G_k, k_{\mathrm{sep}}) = 0$ for all $i > 0$.

Cohomology of the additive group

Proposition

Let K/k be a finite Galois extension. Then $H^i(\mathrm{Gal}(K/k), K) = 0$ for all $i > 0$. In particular, $H^i(G_k, k_{\mathrm{sep}}) = 0$ for all $i > 0$.

We won't prove this since it's going to follow from our theory.

Cohomology of the additive group

Proposition

Let K/k be a finite Galois extension. Then $H^i(\mathrm{Gal}(K/k), K) = 0$ for all $i > 0$. In particular, $H^i(G_k, k_{\mathrm{sep}}) = 0$ for all $i > 0$.

We won't prove this since it's going to follow from our theory. But if you know a little about group cohomology, this is obvious:

Cohomology of the additive group

Proposition

Let K/k be a finite Galois extension. Then $H^i(\mathrm{Gal}(K/k), K) = 0$ for all $i > 0$. In particular, $H^i(G_k, k_{\mathrm{sep}}) = 0$ for all $i > 0$.

We won't prove this since it's going to follow from our theory. But if you know a little about group cohomology, this is obvious: the normal basis theorem says that $K \cong \mathbb{Z}[\mathrm{Gal}(K/k)] \otimes_{\mathbb{Z}} k$. So K is induced and its cohomology vanishes by Shapiro's lemma.

Cohomology of the multiplicative group

Proposition - Hilberts 90 Satz

Let K/k be a finite Galois extension. Then $H^1(\mathrm{Gal}(K/k), K^\times) = 0$. In particular, $H^1(G_k, k_{\mathrm{sep}}^\times) = 0$.

Cohomology of the multiplicative group

Proposition - Hilberts 90 Satz

Let K/k be a finite Galois extension. Then $H^1(\mathrm{Gal}(K/k), K^\times) = 0$. In particular, $H^1(G_k, k_{\mathrm{sep}}^\times) = 0$.

Let $G = \mathrm{Gal}(K/k)$.

Cohomology of the multiplicative group

Proposition - Hilberts 90 Satz

Let K/k be a finite Galois extension. Then $H^1(\mathrm{Gal}(K/k), K^\times) = 0$. In particular, $H^1(G_k, k_{\mathrm{sep}}^\times) = 0$.

Let $G = \mathrm{Gal}(K/k)$. We have to show that every element of $Z^1(G, K^\times)$ (that is, a function $\varphi : G \to K^\times$ satisfying $\varphi(gh) = \varphi(g)\, h(\varphi(g))$) and show that it's in $B^1(G, K^\times)$ (that is, it's of the form $g \mapsto g(x)/x$ for some $x \in K^\times$).

Cohomology of the multiplicative group

Proposition - Hilberts 90 Satz

Let K/k be a finite Galois extension. Then $H^1(\mathrm{Gal}(K/k), K^\times) = 0$. In particular, $H^1(G_k, k_{\mathrm{sep}}^\times) = 0$.

Let $G = \mathrm{Gal}(K/k)$. We have to show that every element of $Z^1(G, K^\times)$ (that is, a function $\varphi : G \to K^\times$ satisfying $\varphi(gh) = \varphi(g)\, h(\varphi(g))$) and show that it's in $B^1(G, K^\times)$ (that is, it's of the form $g \mapsto g(x)/x$ for some $x \in K^\times$).

Dedekind's theorem on the independence of characters gives an element $x \in K^\times$ such that

$$z := \sum_{h \in G} \varphi(h) h(x)$$

is non-zero.

Then, for all $g \in G$,

$$g(z) = \sum_{h \in G} h(\varphi(g))g(h(x)) = \sum_{h \in G} \varphi(g)^{-1}\varphi(gh)g(h(x)) = \varphi(g)^{-1}z.$$

Then, for all $g \in G$,

$$g(z) = \sum_{h \in G} h(\varphi(g))g(h(x)) = \sum_{h \in G} \varphi(g)^{-1}\varphi(gh)g(h(x)) = \varphi(g)^{-1}z.$$

Proving that $\varphi(g) = g(z^{-1})/z^{-1}$. I.e., $\varphi \in B^1(G, K^\times)$.

Guess what!

The next cohomology group of the multiplicative group is an old friend!

Guess what!

The next cohomology group of the multiplicative group is an old friend!

Theorem

Let K/k be a finite Galois extension. Then $\mathrm{Br}(K/k) \cong H^2(\mathrm{Gal}(K/k), K^\times)$ and so $\mathrm{Br}(k) \cong H^2(G_k, k_{\mathrm{sep}}^\times)$.

Guess what!

The next cohomology group of the multiplicative group is an old friend!

Theorem

Let K/k be a finite Galois extension. Then $\mathrm{Br}(K/k) \cong H^2(\mathrm{Gal}(K/k), K^\times)$ and so $\mathrm{Br}(k) \cong H^2(G_k, k_{\mathrm{sep}}^\times)$.

As a corollary, we obtain that $H^i(G_k, k^\times) = 0$ for all $i > 0$ if k is algebraically closed.

Calculating étale cohomology

Cohomology of points [LM, Theorem 17.1]

Besides being an incredible number-theoretic tool, Galois cohomology will allow us to calculate some étale cohomology groups.

Cohomology of points [LM, Theorem 17.1]

Besides being an incredible number-theoretic tool, Galois cohomology will allow us to calculate some étale cohomology groups.

Theorem

Let $X = \operatorname{Spec} k$. Then the functor $\mathscr{F} \mapsto \mathscr{F}(X)$ defines an equivalence of categories between the étale sheaves on X and the G_k-modules.

Cohomology of points [LM, Theorem 17.1]

Besides being an incredible number-theoretic tool, Galois cohomology will allow us to calculate some étale cohomology groups.

Theorem

Let $X = \operatorname{Spec} k$. Then the functor $\mathscr{F} \mapsto \mathscr{F}(X)$ defines an equivalence of categories between the étale sheaves on X and the G_k-modules. In particular, $H^i_{\text{ét}}(X, \mathscr{F}) = H^i(G_k, \mathscr{F}(X))$ for all i.

Cohomology of points [LM, Theorem 17.1]

Besides being an incredible number-theoretic tool, Galois cohomology will allow us to calculate some étale cohomology groups.

Theorem

Let $X = \operatorname{Spec} k$. Then the functor $\mathscr{F} \mapsto \mathscr{F}(X)$ defines an equivalence of categories between the étale sheaves on X and the G_k-modules. In particular, $H^i_{\text{ét}}(X, \mathscr{F}) = H^i(G_k, \mathscr{F}(X))$ for all i.

This proof basically amounts to verifying that things identify as expected.

Cohomology of curves

We're finally in position to calculate the cohomology of an algebraic curve!

Theorem

Let X be a smooth projective connected curve over an algebraically closed field k.

We're finally in position to calculate the cohomology of an algebraic curve!

Theorem

Let X be a smooth projective connected curve over an algebraically closed field k. Then

$$H^0(X, \mathbb{G}_m) = k^\times, \quad H^1(X, \mathbb{G}_m) = \mathrm{Pic}(X), \qquad H^p(X, \mathbb{G}_m) = 0 \text{ for p} \geq 2.$$

Cohomology of curves

We're finally in position to calculate the cohomology of an algebraic curve!

Theorem

Let X be a smooth projective connected curve over an algebraically closed field k. Then

$$H^0(X, \mathbb{G}_m) = k^\times, \quad H^1(X, \mathbb{G}_m) = \mathrm{Pic}(X), \qquad H^p(X, \mathbb{G}_m) = 0 \text{ for p} \geq 2.$$

The only thing left to prove is the last part.

Cohomology of curves

We're finally in position to calculate the cohomology of an algebraic curve!

Theorem

Let X be a smooth projective connected curve over an algebraically closed field k. Then

$$H^0(X,\mathbb{G}_m) = k^\times, \quad H^1(X,\mathbb{G}_m) = \mathrm{Pic}(X), \qquad H^p(X,\mathbb{G}_m) = 0 \text{ for p} \geq 2.$$

The only thing left to prove is the last part. For that we're going to use the divisor exact sequence:

$$0 \to \mathbb{G}_{m,X} \to j_*\mathbb{G}_{m,K} \to \bigoplus_{x\in X \text{ closed}} i_{x,*}\underline{\mathbb{Z}} \to 0,$$

where K is the function field of X, $j : \mathrm{Spec}\, K \to X$ the inclusion of the generic point, and $i_x : \{x\} \to X$ the inclusion of a closed point $x \in X$.

Cohomology of curves

We split the proof in parts.

Cohomology of curves

We split the proof in parts. By the long exact sequence, it suffices to prove that both $H^p(X, j_*\mathbb{G}_{m,K})$ and $H^p(X, i_{x,*}\underline{\mathbb{Z}})$ vanish, for $p > 0$ and $x \in X$ closed.

Lemma A

We have $H^p(\operatorname{Spec} K, \mathbb{G}_m) = 0$ and so $H^p(X, j_*\mathbb{G}_{m,K}) = 0$ for all $p > 0$.

We split the proof in parts. By the long exact sequence, it suffices to prove that both $H^p(X, j_*\mathbb{G}_{m,K})$ and $H^p(X, i_{x,*}\underline{\mathbb{Z}})$ vanish, for $p > 0$ and $x \in X$ closed.

Lemma A

We have $H^p(\operatorname{Spec} K, \mathbb{G}_m) = 0$ and so $H^p(X, j_*\mathbb{G}_{m,K}) = 0$ for all $p > 0$.

The first part follows from Tsen's theorem and our characterization of Galois cohomology as a Brauer group.

We split the proof in parts. By the long exact sequence, it suffices to prove that both $H^p(X, j_*\mathbb{G}_{m,K})$ and $H^p(X, i_{x,*}\mathbb{Z})$ vanish, for $p > 0$ and $x \in X$ closed.

Lemma A

We have $H^p(\operatorname{Spec} K, \mathbb{G}_m) = 0$ and so $H^p(X, j_*\mathbb{G}_{m,K}) = 0$ for all $p > 0$.

The first part follows from Tsen's theorem and our characterization of Galois cohomology as a Brauer group. Since j_* is exact, $\mathrm{R}^p j_*\mathbb{G}_{m,K} = 0$

Cohomology of curves

We split the proof in parts. By the long exact sequence, it suffices to prove that both $H^p(X, j_*\mathbb{G}_{m,K})$ and $H^p(X, i_{x,*}\underline{\mathbb{Z}})$ vanish, for $p > 0$ and $x \in X$ closed.

Lemma A

We have $H^p(\operatorname{Spec} K, \mathbb{G}_m) = 0$ and so $H^p(X, j_*\mathbb{G}_{m,K}) = 0$ for all $p > 0$.

The first part follows from Tsen's theorem and our characterization of Galois cohomology as a Brauer group. Since j_* is exact, $\mathrm{R}^p j_*\mathbb{G}_{m,K} = 0$ and so the Leray spectral sequence degenerates on the second page, proving that $H^p(X, j_*\mathbb{G}_{m,K}) = H^p(\operatorname{Spec} K, \mathbb{G}_m)$.

Cohomology of curves

Lemma B

We have $H^p(X, i_{x,*}\underline{\mathbb{Z}}) = 0$ for all $p > 0$.

Lemma B

We have $H^p(X, i_{x,*}\underline{\mathbb{Z}}) = 0$ for all $p > 0$.

As before, the exactness of $i_{x,*}$ implies that $\mathrm{R}^p i_{x,*}\underline{\mathbb{Z}} = 0$ for all $p > 0$.

Lemma B

We have $H^p(X, i_{x,*}\underline{\mathbb{Z}}) = 0$ for all $p > 0$.

As before, the exactness of $i_{x,*}$ implies that $\mathrm{R}^p i_{x,*}\underline{\mathbb{Z}} = 0$ for all $p > 0$. Then the Leray spectral sequence gives that

$$H^p(X, i_{x,*}\underline{\mathbb{Z}}) = H^p(\{x\}, \underline{\mathbb{Z}}),$$

which vanishes since $\{x\} = \operatorname{Spec} k$ and k is algebraically closed.

Questions?