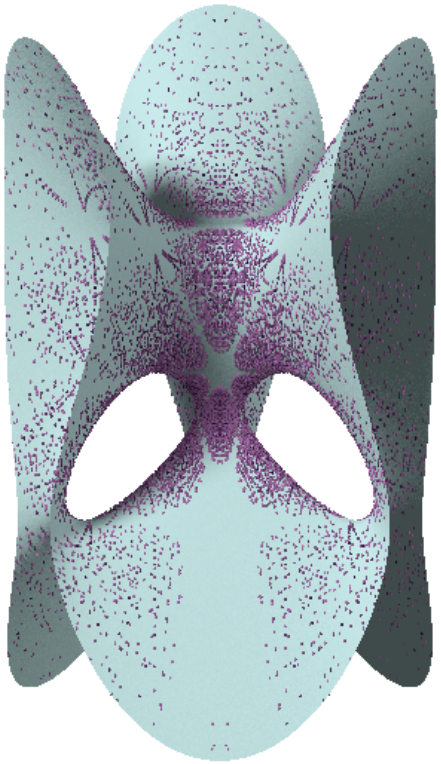


Notes: These are notes live-tex'd from a graduate course on rational points taught by Daniel Litt at the University of Georgia in Fall 2021. As such, any errors or inaccuracies are almost certainly my own.

Rational Points

Lectures by Daniel Litt. University of Georgia, Fall 2021

D. Zack Garza
University of Georgia
dzackgarza@gmail.com

Last updated: 2021-10-12

Table of Contents

Contents

Table of Contents 2

1 Preface 4

2 Thursday, August 19 4
2.1 Examples of Hasse Principles . . . 5

3 Tuesday, August 24 7
3.1 Brauer Groups . . . 8
3.1.1 The Brauer-Manin Obstruction . . . 9
3.1.2 The Hasse Principle for Severi-Brauers . . . 10
3.2 Brauer Groups and Galois Cohomology . . . 10

4 Group Cohomology (Thursday, August 26) 11
4.1 Computing Examples . . . 11
4.2 Functoriality . . . 12

5 Tuesday, August 31 14
5.1 Some Formal Properties . . . 16
5.2 Forms, Torsors, and H^1 . . . 17

6 Thursday, September 02 18
6.1 Correspondence of Forms . . . 18
6.2 Torsors . . . 20
6.3 Example: Kummer Theory . . . 20
6.4 Geometry of Brauer Groups . . . 21

7 Tuesday, September 07 23
7.1 Intro: Historical POV on Brauer Groups . . . 23
7.2 The Boundary Map and Twisted Vector Space . . . 24

8 Thursday, September 09 27
8.1 Computing Brauer Groups . . . 31

9 Tuesday, September 14 32
9.1 Cyclic Algebras . . . 32

10 Thursday, September 16 36
10.1 Computing Brauer Groups . . . 36
10.2 Proof of theorem . . . 39

11 Tuesday, September 21 42
11.1 Construction of Brauer classes over K . . . 42

11.2 The SES 44

12 Thursday, September 23 **46**
12.1 Proof of Theorem 46
12.2 Injectivity 47

13 Tuesday, September 28 **50**
13.1 Proof 53

14 Tuesday, October 05 **54**

15 Tuesday, October 12 **56**

ToDos **60**

Definitions **61**

Theorems **62**

Exercises **64**

Figures **65**

1 | Preface

Possible topics announcement from Daniel

The course will loosely follow Poonen's book on rational points, available here: https://math.mit.edu/~poonen/papers/Qpoints.pdf Planned topics include: the Hasse principle for quadratic forms, obstructions to the Hasse principle (i.e. the Brauer-Manin obstruction and beyond), finding rational points and some effective methods (e.g. Chabauty), as well as some conjectural aspects of rational points. I plan to cover topics in the second half of the semester which depend on student interest; i.e. if there's interest I can say some things about Faltings's proof of the Mordell conjecture.

2 | Thursday, August 19

Remark 2.0.1: Some useful prerequisites:

- Number theory (e.g. places)
- Class field theory
  - See Cassels-Frolich (up through ch. 5 and 6)
- AG (although we'll avoid the language of schemes)
- Galois and group cohomology
- Bjorn Poonen's book

Remark 2.0.2: On notation:

- $k^{\cdot n}$ will denote nth powers in k, and similarly for $k^\times$.
- k^{un} denotes an unramified extension.

Remark 2.0.3: Setup: let $k = \mathbb{Q}$ or more generally a number field or a function field over $\mathbb{F}_q$. Consider a system of polynomial equations over $k[x_1, \cdots, x_m]$:

$$\begin{cases} f_1(x_1, \cdots, x_m) & = 0 \\ \vdots & \vdots \\ f_n(x_1, \cdots, x_m) & = 0. \end{cases}$$

Some natural questions:

Remark 2.0.4 ***(Topic 1: Are there any common solutions?):*** More generally, does $X \coloneqq V(f_1, \cdots, f_n)$ have any rational points? How many rational points are there? Finitely many, or infinitely many?

Remark 2.0.5 ***(Topic 2: what is the distribution of points?):***

- How many points are there of height at most N, where $\mathrm{ht}(a/b) = \max(|a|, |b|)$?
- Are they Zariski dense? I.e. are there solutions outside of the ideal $\langle f_i \rangle$?
- Are they *potentially* dense, i.e. dense after some finite extension $k \hookrightarrow k'$?
- Choosing $k \hookrightarrow \mathbb{C}$ or $\mathbb{Q}_p$, are the solutions dense in the analytic topology on $X(\mathbb{C}), X(\mathbb{Q}_p)$? If not, what is the closure?

There are many conjectures around these questions, but few general results!

Remark 2.0.6 ***(Topic 3: Local to Global Principles):*** Topic 3: local to global principles. Given $X_{/\mathbb{Q}}$, if $X(\mathbb{Q}_p) \neq \emptyset$ for all p and $X(\mathbb{R}) \neq \emptyset$, does this imply that $X(\mathbb{Q}) \neq \emptyset$? More generally, for $X_{/k}$ with $X(K_v) \neq \emptyset$ for all places v of K, is this enough to imply $X(k) \neq \emptyset$ If so, we say X satisfies the **Hasse principle**. If not, are there obstructions?

Remark 2.0.7 ***(Topic 3': Weak and Strong Approximation):*** As an example,

$$X(k) \hookrightarrow \prod_{v \in P(k)} X(k_v)$$

where $p(k)$ are the places of k. Is this map dense? Note the topology is the product topology, so a basis for opens are sets with finitely factors with opens, and the remaining are the entire space. Strong approximation is an adelic version of this.

Obstructions to this principle: if this is not dense, what is the closure $X(k)$ in $\prod X(k_v)$ or $X(\mathbb{A})$ for $\mathbb{A}$ the adeles? One example we'll consider is the Brauer-Manin obstruction.

Remark 2.0.8 ***(Topic 4: effectiveness and decidability questions.):*** Given a variety $X_{/\mathbb{Q}}$, is there an actual algorithm that decides if $X(\mathbb{Q}) = \emptyset$? This is known over $\mathbb{Z}$, but open for $\mathbb{Q}$ and most (not all) number fields. Are there special classes of varieties where the answer of yes? For curves, this is only known contingent on open problems (the abc conjecture, the section conjecture, Birch-Swinnerton-Dyer, etc).

Given a special $X_{/k}$ can you find $X(k)$?

Remark 2.0.9: Other possible topics:

- The Mordell-Weil theorem for X an abelian variety, and a generalization, the Néron-Lang theorem which works over other fields.
- Falting's theorem, that curves of genus 2 have finitely many rational points.

2.1 Examples of Hasse Principles

Example 2.1.1 ***(?):*** Let $a \in \mathbb{Q}$, does $x^2 = a$ satisfy a local to global principle? This is related to Chebotarev density.

Claim: any positive number a such that $v_p(a)$ is even for all p is necessarily a square. This follows from writing $a = \pm \prod p_i^{n_i}$ where $n_i \in \mathbb{Z}$ and is equal to zero for all but finitely many i, then its square root is obtained by halving all of the n_i. Note that $a \in (\mathbb{R}^\times)^2$ implies a is positive, and $a \in ({\mathbb{Q}_p}^\times)^2$ implies that n_p is even.

Example 2.1.2 ***(?):*** Let $a \in \mathbb{Q}$ and take $x^n = a$, or more generally $f(x) = a$ for $f \in \mathbb{Q}[x]$, where $f(x) - a$ is irreducible. Corollary of Chebotarev density: the set of primes where $f - a \bmod p$ has no linear factors has positive density. This means that an even stronger theorem is true: there exists a $c < 1$ such that if $f - a$ has no roots $\bmod p$ for a set of primes of density $d > c$, then $f - a$ has no roots. So this satisfies the Hasse principle.

Example 2.1.3 ***(Conics):*** Take $X \coloneqq V(ax^2 + by^2 + cz^2) \subseteq \mathbb{P}^2$ for $a, b, c \in \mathbb{Q}$. This also satisfies the Hasse principle, but the proof is harder. Note that $x^2 + y^2 + z^2 = 0$ has no rational points (excluding zero since we're in $\mathbb{P}^2$) since it has no solutions over $\mathbb{R}$. It is potentially dense, noting that one can take $\mathbb{Q}[i]$ over $\mathbb{Q}$ and get rational points $0, 1, \infty$. Given one point, one can stereographically project to yield infinite many points by just taking lines through the fixed point and letting slopes vary.

Something about using $\mathcal{O}(1)$ to give an embedding into $\mathbb{P}^1$. Start with $\mathcal{O}(-1)$, dualize, project?

Example 2.1.4 ***(Severi-Brauer varieties):*** Taking $X_{/k}$ such that $X_{/\bar{k}} \cong \mathbb{P}^n_{/\bar{k}}$ satisfy the Hasse principle.

Example 2.1.5 ***(Quadrics):*** A theorem by Hasse-Minkowski shows that these also satisfy the Hasse principle.

Example 2.1.6 ***(Genus 1 curves):*** The **Selmer curve** $3x^3 + 4y^3 + 5z^3 = 0$ does *not* satisfy the Hasse principle, which can be understood in terms of the Tate-Shafarevich group or Brauer-Manin obstructions.

Remark 2.1.7: Note that it doesn't make sense to say a single variety satisfies the Hasse principle, but rather a class. But it makes sense to say a single variety *doesn't*.

Remark 2.1.8: A common generalization is that these are all torsors for an algebraic group, i.e. a homogeneous space, for which there are cohomological methods to understand the Hasse principle.

Remark 2.1.9: A variety $X_{/k}$ is *geometrically integral* in the affine case if when $X = V(f_1, \cdots, f_n)$, the ring $\bar{k}[x_1, \cdots, x_n]$ is an integral domain.

Theorem 2.1.10 ***(?).***
Suppose K is a number field and $X_{/K}$ is geometrically integral. Then $X(K_v) \neq \emptyset$ for all but finitely many v.

Proof (Sketch/idea).

1. Write $X = V(f_1, \cdots, f_n)$ with a nonempty smooth locus $X^{\mathsf{sm}} \subseteq X$ which is a variety (just adjoin inverses of partial derivatives appearing in minors of Jacobian matrices). So $X^{\mathsf{sm}}/\mathcal{O}_{K,S} = \mathcal{O}_K\left[\frac{1}{N}\right]$ which is smooth over $\mathcal{O}_{K,S}$
2. Use Lang-Weil to show that $X^{\mathsf{sm}}(\mathcal{O}_{K,S}/\mathfrak{p}) \neq \emptyset$ for almost all $\mathfrak{p}$.
3. Use smoothness and Hensel's lemma to get $X^{\mathsf{sm}}(\mathcal{O}_{K,S^{\widehat{\mathfrak{p}}}})$.

■

3 | Tuesday, August 24

Remark 3.0.1: Last time: if K is a number field and $X_{/K}$ is geometrically irreducible, then $X(K_v) \neq \emptyset$ for almost all v.

Proof (?).
Choose $X_{/\mathcal{O}_K[\frac{1}{N}]}$ such that X has geometrically integral fibers. It's enough to show that $X(K(v)) \neq \emptyset$ for almost all v, where $K(v)$ is the residue field at finite places v.
Now use the following theorem:

■

Theorem 3.0.2 ***(Lang-Weil Estimates).***
If X over $\mathcal{O}_K[\frac{1}{N}]$ is geometrically integral, then

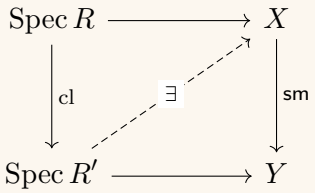
$$\#X(\mathbb{F}_{q^k}) = (1 + O(q^{\frac{1}{2}}))q^{k \dim X}.$$

Claim: If $X_{/\mathcal{O}_{K_v}}$ is smooth then

$$X(K(v)) \neq \emptyset \implies X(K_v) \neq \emptyset.$$

Proof (?).
Use

- Slice and Hensel, or the formal smoothness criterion, i.e.



Taking $R \coloneqq R'/I$ with I nilpotent.

Link to Diagram

See Hartshorne chapter 3, in the exercises!

■

Remark 3.0.3: As a black box, we'll use that this is true for $\dim_{\mathcal{O}_{K_v}} X = 1$, i.e. for curves. This follows from the Weil conjectures for curves, see Severi/Bombieri. If X is genus g, then in fact we have a finer estimate:

$$\left|\#X(\mathbb{F}_{q^k}) - q^n\right| \leq q^{\frac{1}{2}} + 1.$$

Proof (?).
We'll show this for $\dim_{\mathcal{O}_K[\frac{1}{n}]} = 2$. Idea: try to fiber with curves.

- Suppose $\operatorname{reldim} X = 1$ for $X \to S$ over $\mathcal{O}_K[\frac{1}{n}]$ where S is a curve with geometrically integral fibers.
- Without loss of generality, $X \to S$ where
  - S is smooth of genus g',
  - X/S is smooth with fibers of genus g.
  - Now take the count

$$\begin{aligned} X(\mathbb{F}_{q^k}) &= (1 + O_{g'}(q^{-\frac{k}{2}}))q \cdot (1 + O_g(q^{-\frac{k}{2}}))q \\ &= (1 + O_{g,g'}(q^{-\frac{k}{2}}))q^2. \end{aligned}$$

- Such an $X \to S$ after replacing X by an open subvariety. The proof of this follows from Bertini: for $X \subseteq \mathbb{P}^n$, take geometric projections and delete the singular locus. The fibers are slices by hyperplanes, and thus the fibers are geometrically integral.

■

3.1 Brauer Groups

Remark 3.1.1: Some upcoming topics:

- Severi-Brauer varieties (so $X_{/K}$ where $X_{/\overline{K}} \cong \mathbb{P}^n$) satisfy the Hasse principle. Implies Hasse-Minkowski!
- The Brauer-Manin obstruction to the Hasse principle.

3.1.1 The Brauer-Manin Obstruction

Remark 3.1.2: Setup:

- X is a variety,
- $\mathrm{Br}(X)$ is an abelian group
- Given $X \xrightarrow{f} Y$, there is an induced map $f^* : \mathrm{Br}(Y) \to \mathrm{Br}(X)$.

For K a number field (which we can view as a variety with a single point), we have

$$\mathrm{Br}(K_v) = \begin{cases} \mathbb{Q}/\mathbb{Z} & v \text{ finite} \\ \mathbb{Z}/2 & v \text{ real} \\ 0 & v \text{ complex,} \end{cases}$$

which fits into a SES

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0.$$

Note that most of the terms in the middle sum are $\mathbb{Q}/\mathbb{Z}$, making $\mathrm{Br}(K)$ a large group.

Remark 3.1.3: The yoga of the Hasse principle says we should try to solve things in adelic points first. Write

$$\mathbb{A}_K = \prod_v{}' (K_v, \mathcal{O}_v) \subseteq \prod_v K_v$$

where we take the restricted product. There is a map $X(K) \to X(\mathbb{A}_K)$, and taking $\alpha \in \mathrm{Br}(X)$ one gets a map $\alpha^* : X(K) \to \mathrm{Br}(K)$. This yields a diagram

$$\begin{array}{ccc} X(K) & \longrightarrow & X(\mathbb{A}_K) \\ \downarrow{\scriptstyle \alpha^*} & & \downarrow{\scriptstyle \tilde{\alpha}^*} \\ \mathrm{Br}(X) & \longrightarrow & \mathrm{Br}(\mathbb{A}_k) \cong \bigoplus_v \mathrm{Br}(K_v) \end{array}$$

Link to Diagram

Using that $\Sigma : \mathrm{Br}(\mathbb{A}_K) \to \mathbb{Q}/\mathbb{Z}$, for a fixed $\alpha \in \mathrm{Br}(K)$,

$$X(K) \subseteq (\Sigma \circ \tilde{\alpha})^{-1}(0) \subseteq X(\mathbb{A}_K),$$

and $(\Sigma \circ \tilde{\alpha})^{-1}(0) = X(\mathbb{A}_K)^\alpha$. Thus the Hasse principle is violated if $X(\mathbb{A}_K)$ is nonempty but $X(\mathbb{A}_K)^\alpha$ is empty. More generally, it's violated if

$$X(\mathbb{A}_K)^{\mathrm{Br}} := \bigcap_{\alpha \in \mathrm{Br}(X)} X(\mathbb{A}_K)^\alpha = \emptyset.$$

3.1.2 The Hasse Principle for Severi-Brauers

Remark 3.1.4: Let $X_{/K}$ be a Severi-Brauer, then $[X] \in \mathrm{Br}(K)$ and $X \cong \mathbb{P}^n_{/K} \iff [X] = 0$. Using that

$$\oplus \iota_v : \mathrm{Br}(K) \hookrightarrow \bigoplus_v \mathrm{Br}(K_v),$$

we have

$$[X] = 0 \iff \iota_v(X) = 0 \ \forall v \qquad \text{since } \iota_v(X) = [X_{K_v}] \in \mathrm{Br}(K_v).$$

Fact 3.1.5
It turns out that $X \cong \mathbb{P}^n \iff X(K) \neq \emptyset$.

3.2 Brauer Groups and Galois Cohomology

Definition 3.2.1 (Brauer Groups)
Let $K \in \mathsf{Field}$, then

$$\mathrm{Br}(K) \coloneqq H^2_{\mathsf{Gal}}(K, \overline{K}^\times) = H^2_{\mathsf{Grp}}(\mathsf{Gal}(K^s/K), (K^s)^\times).$$

Remark 3.2.2: Let $G \in \mathsf{Grp}$ be discrete, so we're not considering any topology on it. Let $M \in \mathsf{G\text{-}Mod}$, or equivalently $M \in \mathbb{Z}[\mathsf{G}]\text{-}\mathsf{Mod}$.

We can take invariants and coinvariants:

$$M^G \coloneqq \left\{ m \in M \;\middle|\; gm = m \ \forall g \in G \right\} = \hom_{\mathbb{Z}[G]}(\mathbb{Z}, M)$$
$$M_G \coloneqq M / \left\langle \left\{ gm - m \;\middle|\; g \in G \right\} \right\rangle = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M.$$

These are the largest submodules/quotient modules respectively on which G acts trivially.

Exercise 3.2.3 (?)
Why are these equal to homs and tensors respectively?

Definition 3.2.4 (Group cohomology)

$$H^i(G; M) \coloneqq \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}; M)$$
$$H_i(G; M) \coloneqq \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}; M).$$

Example 3.2.5 ***(Cyclic groups):*** For $G \coloneqq \mathbb{Z}$, we have $\mathbb{Z}[G] = \mathbb{Z}\left[x, x^{-1}\right]$. Take a projective resolution

$$0 \to \mathbb{Z}[G] \xrightarrow{\cdot(x-1)} \mathbb{Z}[G] \xrightarrow{x\mapsto 1} \mathbb{Z} \to 0.$$

Deleting the augmentation and applying $\underset{\mathbb{Z}[G]}{\mathrm{Hom}}(-, \mathbb{Z})$ yields $0 \to \mathbb{Z} \xrightarrow{f\cdot(x-1)} \mathbb{Z} \to 0$, and noting that x acts by 1, f is the zero map. This yields

$$H^*(G;\mathbb{Z}) = \begin{cases} \mathbb{Z} & * = 0, 1 \\ 0 & \text{else.} \end{cases}$$

$$H_*(G;\mathbb{Z}) = \begin{cases} \mathbb{Z} & * = 0, 1 \\ 0 & \text{else.} \end{cases}$$

4 | Group Cohomology (Thursday, August 26)

See Cassels-Frohlich, Stein, etc for group cohomology.

4.1 Computing Examples

Example 4.1.1: For $G = \mathbb{Z}$, take the resolution

$$0 \to \mathbb{Z}[x, x^{-1}] \xrightarrow{x-1} \mathbb{Z}[x, x^{-1}] \to 0.$$

Then $H_*(G;\mathbb{Z}) = H^*(G;\mathbb{Z})$ is $\mathbb{Z}$ in degrees 0 and 1, and 0 otherwise. For $M \in \mathsf{G\text{-}Mod}$, we have

$$H^*(G;M) = H^*(M \xrightarrow{x-1} M) = \begin{cases} M^G & * = 0 \\ M_G & * = 1 \\ 0 & \text{else,} \end{cases}$$

$$H_*(G;M) = H_*(M \xrightarrow{x-1} M) = \begin{cases} M_G & * = 0 \\ M^G & * = 1 \\ 0 & \text{else.} \end{cases}$$

Example 4.1.2 ***(?):*** For $G = \mathbb{Z}/n$, write σ as the generator so that $\mathbb{Z}[G] = \mathbb{Z}[\sigma]/\langle \sigma^n - 1\rangle$ We can take a resolution

$$\cdots \to \mathbb{Z}[\sigma]/\langle \sigma - 1\rangle \xrightarrow{\sigma-1} \mathbb{Z}[\sigma]/\langle \sigma - 1\rangle \xrightarrow{1+\sigma+\cdots+\sigma^{n-1}} \mathbb{Z}[\sigma]/\langle \sigma - 1\rangle \xrightarrow{\sigma-1} \mathbb{Z}[\sigma]/\langle \sigma - 1\rangle \to 0.$$

Now apply $\underset{\mathbb{Z}[G]}{\mathrm{Hom}}(-,\mathbb{Z})$, use that $\underset{\mathbb{Z}[G]}{\mathrm{Hom}}(\mathbb{Z}[G],\mathbb{Z}) = \mathbb{Z}$, and take homology of the complex

$$\mathbb{Z} \xrightarrow{\sigma-1} \mathbb{Z} \xrightarrow{\sum \sigma^i} \to \mathbb{Z} \xrightarrow{\sigma-1} \cdots \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \to \mathbb{Z} \xrightarrow{0} \cdots .$$

This yields

$$H^*(G;\mathbb{Z}) = \begin{cases} \mathbb{Z} & * = 0 \\ 0 & * \text{ odd} \\ \mathbb{Z}/n & * \text{ even.} \end{cases}$$

Remark 4.1.3: For the free abelian group $\mathbb{Z}^n$, we get $H^*(\mathbb{Z}^n;\mathbb{Z}) = \bigwedge^*(\mathbb{Z}^n)$. For the free group F_n, we get $H^*(F_n;\mathbb{Z})$ is $\mathbb{Z}$ in degree zero (always true for the trivial module, since the invariants are everything) and $\mathbb{Z}^n$ in degree 1.

Fact 4.1.4
If X is a CW complex with $\pi_0(X) = 0, \pi_1(X) = G, \pi_{>2}(X) = 0$, then $H^*_{\mathsf{Grp}}(G;\mathbb{Z}) = H^*_{\mathrm{Sing}}(X;\mathbb{Z})$. Note that $X \xrightarrow{\sim} \mathbf{B}G$ in this case, and the proof is easy: take the universal cover, then the simplicial/cellular cohomology resolves $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module.

Proposition 4.1.5 ***(?).***
Suppose G is finite and $M \in \mathsf{G\text{-}Mod}$, then $H^{>n}(G;M)$ is torsion. 1. It suffices to show this for $* = 1$ by using dimension shifting. Choose $M \hookrightarrow I$ into an injective object to get a SES

$$0 \to M \to I \to M/I \to 0$$

to get a LES in cohomology, and use that Ext into injectives vanishes to get $H^*(G;M) \cong H^*(G;M/I)[-1]$.

2. We want to show $H^1(G;M) = \mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z};M)$ is torsion, and it suffices to show $\mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z};M) \otimes \mathbb{Q} = 0$, which we can replace with $\mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Q}, M \otimes \mathbb{Q})$. So we consider SESs of the form

   $$0 \to M \otimes Q \to W \to \mathbb{Q},$$

   which we'd like to split as a SES of G-representations over $\mathbb{Q}$.

See uniquely divisible groups?
This splits by Maschke's theorem: all SESs of irreducible representations of G for G finite over $\operatorname{ch} k = 0$ split. The usual proof over $\mathbb{C}$ doesn't work for $\mathbb{Q}$, but one uses a splitting instead of an inner product.

4.2 Functoriality

Remark 4.2.1: Given $M \to N \in \mathsf{G\text{-}Mod}$ there are maps

$$H^*(G;M) \to H^*(G;N)$$
$$H_*(G;M) \to H_*(G;N).$$

Suppose $\iota : G \to T$ with $M \in \mathsf{T\text{-}Mod}$, then there are induced maps

$$\iota^* : H^*(T;M) \to H^*(G;M)$$
$$\iota_* : H_*(T;M) \to H_*(G;M)$$

coming from the functoriality of Ext and Tor under change of rings.

We'll use the following as a black box: for $G \leq T$ finite index, there is a *trace* map (or *corestriction*)

$$\mathrm{tr}_{G/T} : H^*(G;M) \to H^*(T;M).$$

It's functorial in M, and $\mathrm{tr}_{G/T} \circ \iota^*$ is multiplication by $m \coloneqq [G:T]$. This yields another proof of the previous element: take $G = 1$ to get $H^*(G;M) = 0$ and check $\mathrm{tr}_{G/T} \circ \iota_*$ is multiplication by $|T|$ and zero, making the group torsion.

Remark 4.2.2: Some interpretations:

- $H_1(G;\mathbb{Z}) = G^{\mathrm{ab}} = G/[G,G]$ is the abelianization (which can still be torsion).
- $H^1(G;\mathbb{Z}) = \underset{\mathsf{Grp}}{\mathrm{Hom}}(G;\mathbb{Z})$, which is always torsionfree.
- $H^2(G;M)$ classifies extensions of G by M in the following sense: G' occurring in a "SES" $\xi : 0 \to M \to G' \to G \to 1$ such that the action of G on M by conjugation is the given G-module structure on M. Moreover $\xi = 0$ in $H^2(G;M)$ iff ξ splits, then $G' \cong G \rtimes M$. For M a trivial G-module, these are *central extensions*.

⚠ Warning 4.2.3

Note all SESs yield semidirect products: take $0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n \to 0$, which has no sections since $\mathbb{Z}$ has no n-torsion. This in fact represents a generator $H^2(\mathbb{Z}/n;\mathbb{Z})$.

Definition 4.2.4 (Galois cohomology)
Let $L_{/k}$ be a finite Galois extension, $M \in \mathsf{G\text{-}Mod}$ for $G \coloneqq \mathsf{Gal}(L_{/k})$. Then

$$H^*_{\mathsf{Gal}}(L_{/k};M) \coloneqq H^*_{\mathsf{Grp}}(G;M).$$

If M is a discrete continuous $\mathsf{Gal}(k^s/K)$-module, then

$$H^i(k;M) \coloneqq \varinjlim_{U \trianglelefteq \mathsf{Gal}(k^s/k)} H^*(\mathsf{Gal}(k^s/k)/U;M).$$

The stabilizer of any point is open (and finite index).

Definition 4.2.5 (Brauer Groups)

$$\mathrm{Br}(k) = H^2(K;(k^s)^\times).$$

Example 4.2.6 *(?):* Consider $\mathrm{Br}(\mathbb{F}_q)$, then $\mathsf{Gal}(\mathbb{F}_q^s/\mathbb{F}_q) = \widehat{\mathbb{Z}}\left\langle \underset{q}{\mathrm{Frob}} \right\rangle$. Then

$$\begin{aligned}
\mathrm{Br}(\mathbb{F}_q) &:= H^2\left(\widehat{\mathbb{Z}}\left\langle \underset{q}{\mathrm{Frob}} \right\rangle; \bar{\mathbb{F}}_q^\times\right) \\
&= \varinjlim_{U_n \subseteq \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}} \to \mathbb{Z}/n} H^2\left(\mathbb{Z}/n; (\bar{\mathbb{F}}_q^\times)^{U_n}\right) \\
&= \varinjlim H^2\left(\mathbb{Z}/n\left\langle \underset{q}{\mathrm{Frob}} \right\rangle; \bar{\mathbb{F}}_{q^n}^\times\right) \\
&= \varinjlim H^2(\mathsf{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q); \bar{\mathbb{F}}_{q^n}^\times) \\
&= \varinjlim H^2\left(\mathbb{F}_{q^n}^\times \xrightarrow{\mathrm{Frob}-1} \mathbb{F}_{q^n}^\times \xrightarrow{\mathrm{Nm}} \mathbb{F}_{q^n}^\times \to \cdots\right) \\
&= \varinjlim \mathbb{F}_q^\times / \mathrm{Nm}(\mathbb{F}_{q^n}, \mathbb{F}_q)\mathbb{F}_{q^n}^\times \\
&= \varinjlim 0 \\
&= 0.
\end{aligned}$$

Note: we've used that

$$\ker(\mathrm{Frob} - 1 : x \mapsto x^{q-1}) = \mathbb{F}_q^\times.$$

Exercise 4.2.7 (?)
Show that the norm is surjective.

5 | Tuesday, August 31

Remark 5.0.1: Today: a systematic way to compute group cohomology by taking standard resolution. For a fixed group G, we want to resolve $\mathbb{Z}$ by free $\mathbb{Z}[G]$-modules, so take a simplicial resolution

$$\cdots \rightrightarrows G^{\times^3} \rightrightarrows G^{\times^2} \rightrightarrows G$$

Taking free $\mathbb{Z}$-modules yields

$$\cdots \rightrightarrows \mathbb{Z}[G^{\times^3}] \rightrightarrows \mathbb{Z}[G^{\times^2}] \rightrightarrows \mathbb{Z}[G]$$

Note that this is a simplicial set whose realization is EG.

Proposition 5.0.2 *(?).*
$C_\bullet(G)$ is exact, and $\mathbb{Z}[G^{\times^n}]$ is free in $\mathbb{Z}[\mathsf{G}]$-Mod where $G \curvearrowright G^{\times^n}$ diagonally and this extends linearly.

Proof (?).
$\mathbb{Z}[G^{\times^n}]$ is a free $\mathbb{Z}[G]$-module, using that $\left\{(1, g_1, \cdots, g_{n-1}) \;\middle|\; g_k \in G\right\}$ is a free basis, since these are representatives for G-orbits on $G^{\times^n}$.
That this is an exact complex will follow from a nullhomotopy $h : \mathbb{Z}[G^{\times^{n-1}}] \to \mathbb{Z}[G^{\times^n}]$ so that $hd + dh = \mathrm{id}$. Take the map $h(g_1, \cdots, g_n) = (e, g_1, \cdots, g_n)$, then

$$\begin{aligned}(hd)(g_1, \cdots, g_n) &= h \sum (-1)^i (g_1, \cdots, \widehat{g_i}, \cdots, g_n) \\ &= \sum (-1)^i (e, g_1, \cdots, \widehat{g_i}, \cdots, g_n).\end{aligned}$$

and

$$\begin{aligned}(dh)(g_1, \cdots, g_n) &= d(e, g_1, \cdots, g_n) \\ &= (g_1, \cdots, g_n) - \sum (-1)^i (e, g_1, \cdots, \widehat{g_i}, \cdots, g_n),\end{aligned}$$

and adding these two cancels the two summed terms and yields the identity.
Then just recall from homological algebra that $x \in \ker d$ implies $x = hdx + dhx = dhx$, so $x \in \operatorname{im} d$, so this makes the complex exact.

■

Corollary 5.0.3 *(?).*
For $G \in \mathsf{Grp}$ discrete and $M \in \mathsf{G}$-Mod,

$$\begin{aligned}H^*(G; M) &= H^*(\mathrm{Hom}^\bullet_{\mathbb{Z}[G]}(C_\bullet(G), M)) \\ H_*(G; M) &= H^*(M \otimes_{\mathbb{Z}[G]} C_\bullet(G)).\end{aligned}$$

Remark 5.0.4: Can we find a smaller way to represent this? Note that

$$\mathbb{Z}[G^{\times n}] = \bigoplus_{(g_1, \cdots, g_n) \in G^{n-1}} \mathbb{Z}[G](1, g_1, \cdots, g_{n-1}),$$

and there is a free/forgetful adjunction between modules and sets that yields

$$\operatorname*{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{\times^n}], M) \cong \operatorname*{Hom}_{\mathsf{Set}}(G^{\times^{n-1}}, M).$$

Definition 5.0.5 (Reduced Complex)
For $G \in \mathsf{Grp}$ discrete and $M \in \mathsf{G}$-Mod, set

$$\tilde{C}^r(G; M) \coloneqq \operatorname*{Hom}_{\mathsf{Set}}(G^{\times^r}, M).$$

The boundary maps are given by

$$\begin{aligned}\delta : \tilde{C}^0(G,M) &\to \tilde{C}^1(G,M)\\ \delta f(\sigma) &= \sigma f(-) - f(-)\end{aligned}$$

$$\begin{aligned}\delta : \tilde{C}^1(G,M) &\to \tilde{C}^2(G,M)\\ \delta f(\sigma,\tau) &= \sigma f(\tau) - f(\sigma\tau) + f(\sigma)\end{aligned}$$

$$\begin{aligned}\delta : \tilde{C}^2(G,M) &\to \tilde{C}^3(G,M)\\ \delta f(\sigma,\tau,\rho) &= \sigma f(\tau,\rho) - f(\sigma\tau,\rho) + f(\sigma,\tau\rho) - f(\sigma,\tau).\end{aligned}$$

The pattern is multiply by σ on the outside, cycle through multiplying it to each argument, and for the last term leave σ off.

Remark 5.0.6: Punchline: in principle, group cohomology is computable – however, the complex is quite large and not practical for large groups.

5.1 Some Formal Properties

Proposition 5.1.1 ***(Spectral Sequences).***
For $H \trianglelefteq G$ and $M \in \mathsf{G\text{-}Mod}$, the **Hochschild-Serre spectral sequence** reads

$$E_2^{p,q} = H^p(G/H; H^q(H;M)) \Rightarrow H^{p+q}(G;M).$$

Remark 5.1.2: This is useful for inducting on the lengths of composition series, since e.g. for solvable groups one can take G/H to be cyclic and H a smaller solvable group.

Proposition 5.1.3 ***(Inflation/Restriction Exact Sequence).***
This spectral sequence induces an **inflation/restriction exact sequence**

$$\begin{array}{ccccc} 0 & & & & \\ \downarrow & & & & \\ H^1\left(\frac{G}{H}; M^H\right) & \longrightarrow & H^1(G;M) & \longrightarrow & H^1(H;M)^{\frac{G}{H}} \\ & & & & \\ \hookrightarrow H^2\left(\frac{G}{H}; M^H\right) & \longrightarrow & H^2(G;M) & & \end{array}$$

Link to Diagram

Remark 5.1.4: This comes from the bottom-left corner of the HS spectral sequence, which is a general principle for first quadrant spectral sequences. Note that the G/H action comes from $G \curvearrowright H$ by conjugation, which yields a G-action on H^*, and since H acts trivially on $H^*(H; M)$ (since e.g. M^H has a trivial action), this action factors through G/H.

5.2 Forms, Torsors, and H^1

Definition 5.2.1 (Forms/descent, a pseudo-definition)
Let $X_{/k}$ be an object (e.g. a variety, a group scheme, a variety with extra structure), then a **form** of X over k is an object $X'_{/k}$ with an isomorphism $X'_{/k^s} \xrightarrow{\sim} X$ (i.e. a **descent** of X).

Example 5.2.2 ***(?):*** For $X \coloneqq \mathbb{P}^n_{/k^s}$ then a form of $X_{/k}$ is a Severi-Brauer variety, for example a smooth conic.

Example 5.2.3 ***(Severi Brauers):*** Let E be a genus 1 curve, then E is a form for its Jacobian $\mathrm{Jac}(E)$, i.e. it becomes isomorphic to its Jacobian if it has a rational point. Not every curve has such a point, so they only become isomorphic after base changing to a separable closure. Note that $\mathrm{Jac}(E) \curvearrowright E$ by addition of divisors (since Jacobians have degree zero, curves have divisors of degree 1, and adding them yields a degree 1 divisor). It is in fact a torsor.

Example 5.2.4 ***(?):*** If $L_{/k}$ is a finite separable extension then L is a form of $(k^s)^{\times^n}$.

Example 5.2.5 ***(?):*** The groups $\mathrm{SO}(p,q)_{/\mathbb{R}}$, the matrices preserving a quadratic form

$$h_{p,q} \coloneqq \mathrm{diag}(1, \cdots, 1, -1, \cdots, -1)$$

with p copies of 1 and q copies of -1, and these are all forms of $\mathrm{SO}(p+q)_{/\mathbb{C}}$.

Proposition 5.2.6 ***(?).***
Suppose $X_{/k}$ is some object (e.g. a variety, then forms of X_{k^s} over k are canonically in bijection with $H^1_{\mathsf{Gal}}(k; \mathrm{Aut}(X_{k^s}))$ (recalling that this was defined as a direct limit). Note that this automorphism group may be nonabelian, which we still need to define.

Proof (?).
Suppose $\mathrm{Aut}(X_{k^s})$ is abelian, then we'll show the following stronger claim:

Claim: $X'_L \xrightarrow{\sim} X_L$ since there is a bijection

$$\left\{ \begin{matrix} \text{Forms of } X_{k^s} \\ \text{split by } L_{/k} \end{matrix} \right\} \rightleftharpoons H^1_{\mathsf{Gal}}(L_{/k}; \mathrm{Aut}(X_L)).$$

Proof (?).
Recall that

$$H^1(L_{/k}; \mathrm{Aut}(X_L)) = H^1(\tilde{C}^\bullet(\mathsf{Gal}(L/k)); \mathrm{Aut}(X_L)).$$

Given $X'_{/k}$ split by L, we want a map $\mathsf{Gal}(L/k) \to \mathrm{Aut}(X_L)$. Choose an isomorphism $X'_L \xrightarrow{\sim} X_L$, noting that Galois acts on the LHS since it's defined over k, which will be different from the natural action on the right-hand side. So we can take a map

$$f : \mathsf{Gal}(L/k) \to \mathrm{Aut}(X'/L) \xrightarrow{\sim} \mathrm{Aut}(X_L),$$

although this is not generally a homomorphism.
Instead, $f(\sigma\tau) = f(\sigma)f(\tau)^\sigma$, a **crossed homomorphism** which involves acting on the coefficients of defining equations (which come from L). This says that $f \in \ker \delta$, the differential for $\tilde{C}^\bullet$. So we now have a map from forms split by L to $H^1(\mathsf{Gal}(L/k), \mathrm{Aut}(X_L))$, and we'll show it's injective and surjective.

Injectivity: Suppose X', X'' are isomorphic forms of X, so we have an isomorphism defined over k of the form $X'_L \xrightarrow{\sim} X''_L$.

> **Exercise** ***(?)***
> This changes f by an element of the form $\delta(g)$ for $g \in \mathrm{Aut}(X_L)$.

Surjectivity: Given a crossed homomorphism $f : \mathsf{Gal}(L/k) \to \mathrm{Aut}(X_L)$, we want to produce a form of $X_{/k}$ mapping to it. This is the hardest part of the argument!
Suppose $X_{/k}$ is a variety. First suppose $X \in \mathsf{AffVar}$, so $X = \operatorname{Spec} R$ and $\mathsf{Gal}(L_{/k}) \curvearrowright_f R_L = R \otimes_k L$, which is only an L-semilinear action. Then $X' = \operatorname{Spec}(R_L)^{\mathsf{Gal}(L/k)}$, and the claim is that $X'_L \cong X_L$. The proof of this is **Galois descent**, i.e. there is an equivalence of tensor categories

$$\mathsf{k\text{-}Mod}^\otimes \underset{(-)^{\mathsf{Gal}(L_{/k})}}{\overset{(-)\otimes L}{\rightleftarrows}} \mathsf{L\text{-}Mod}^\otimes + \text{ a semilinear action of } \mathsf{Gal}(L_{/k})$$

Now for general X, one reduces to the case of affines. One can alternatively prove Galois descent without reference to affine varieties.

■

■

6 | Thursday, September 02

6.1 Correspondence of Forms

Remark 6.1.1: Last time: standard/reduced complexes, forms, and H^1. A meta-definition for today: let $k, L \in \mathsf{Field}$ with $L_{/k}$ finite and separable, and $X_{/k}$ an object over k (e.g. an algebraic variety, possibly with extra structure). A **form** of $X_{/k}$ split by L is an object $X'_{/k}$ of the same class as X such that $X_L \xrightarrow{\sim} X'_L$.

Theorem 6.1.2 ***(A meta-theorem).***
The theorem was that there is a canonical bijection

$$\left\{ \begin{smallmatrix} \text{Forms of } X \\ \text{split by } L \end{smallmatrix} \right\} \rightleftharpoons H^1_{\mathsf{Gal}}(L_{/k}; \underset{k}{\mathrm{Aut}}(X_L))$$

Note that we didn't assume the coefficients formed an abelian group, so we'll explain this today. It is true that $\mathrm{Aut}(X_L) \in \mathsf{Gal}(\mathsf{L}_{/\mathsf{k}})\text{-}\mathsf{Mod}$. We'll say that X' is just **a form** of X if there exists some L' finite separable that splits k. In this case there is a correspondence

$$\{\text{Forms of } X\} \rightleftharpoons H^1_{\mathsf{Gal}}(L_{/k}; \underset{k}{\mathrm{Aut}}(X_{k^s}))$$

Proof (A meta-proof).
What is the map? Given a form X', we by definition have $F : X'_L \xrightarrow{\sim} X_L$, and we want a map $\mathsf{Gal}(L_{/k}) \to \underset{k}{\mathrm{Aut}}(X_L)$ such that $\delta f = 0$ for the differential in cohomology. Since X' is defined over k, we have an action $\mathsf{Gal}(L_{/k}) \curvearrowright X'_L$, i.e. a map $\mathsf{Gal}(L_{/k}) \to \mathrm{Aut}(X'_L)$, which we can compose with the given isomorphism to obtain

$$f : \mathsf{Gal}(L_{/k}) \to \mathrm{Aut}(X'_L) \to \mathrm{Aut}(X_L).$$

We have $f(\sigma\tau) = f(\sigma) f(\tau)^\sigma$. What happens if we change the isomorphism F to some F', changing by some $g \in \mathrm{Aut}(X_L)$

Exercise ***(?)***
Here f changes by a map of the form $\sigma \to g(g^{-1})^\sigma$.

We'll write an inverse map using Galois descent. Given $f : \mathsf{Gal}(L_{/k}) \to \underset{k}{\mathrm{Aut}}(X_L)$ with $f(\sigma\tau) = f(\sigma) f(\tau)^\sigma$, we want to construct a form of X. Assume $X \in \mathsf{AffSch}$, so $X = \mathrm{Spec}(A)$ for some $A \in \mathsf{Alg}_{/k}$, then define

$$X' \coloneqq \mathrm{Spec}(A \otimes_k L)^{\mathsf{Gal}(L_{/k})}$$

where the action is given by f.

■

Remark 6.1.4: What is $\underset{k}{\mathrm{Aut}}(X_{/L})$ is nonabelian? Then we just make this proof a definition, and set

$$H^1(L_{/k}; G) \coloneqq \left\{ f : \mathsf{Gal}(L_{/k}) \to G \;\middle|\; f(\sigma\tau) = f(\sigma) f(\tau)^\sigma \right\} / (\sigma \to g(g^{-1})^\sigma).$$

Here the maps are of finite discrete groups. This is a pointed set, using the constant map as a basepoint.

6.2 Torsors

Definition 6.2.1 (Torsor)
Recall that for $G \in \mathsf{AlgGrp}_{/k}$, a **torsor** for G (or a *principal homogeneous space*) is

1. A form of G under the left action of G on itself, i.e. a variety X with a left G-action $G \times X \to X$ where $X_L \xrightarrow{\sim} G_L$ using the left-translation action.
2. A G-variety X such that $G \times X \xrightarrow{\sigma,\pi_2} X \times X$ is an isomorphism.

Claim: Note that these are equivalent if G is smooth, which for us will always happen in characteristic zero.

Theorem 6.2.2 ***(?).***
If G is smooth, then G-torsors are canonically in bijection with $H^1(k; G(k^s))$, and G-torsors split by L biject with $H^1(L_{/k}; G(L))$.

Exercise 6.2.3 (?)
Prove this! It suffices to show that $\underset{G_L}{\mathrm{Aut}}(G_L) \cong G_L$ as a $\mathsf{GrpSch}_{/G_L}$.

6.3 Example: Kummer Theory

Example 6.3.1 ***(Kummer theory):*** Suppose $\mu_p \subseteq k$, so k contains all pth roots of unity. Then a μ_p-torsor is the same as a $\mathbb{Z}/p$ Galois extension of k, where we allow $k^p = \mu_p$ itself.

Theorem 6.3.2 ***(?).***
There is a bijection

$$\{\mathbb{Z}/p\text{-extensions}\} \rightleftharpoons H^1(k; \mu_p)$$

Proof (?).
Use the SES

$$1 \to \mu_p \to (k^s)^\times \xrightarrow{x \mapsto x^p} (k^s)^\times \to 1,$$

which yields a LES

$$1 \to H^0(k; \mu_p) \to H^0(k; (k^s)^\times) \xrightarrow{x \mapsto x^p} H^0(k; (k^s)^\times) \to H^1(k; \mu_p) \to H^1(k; (k^s)^\times),$$

and identifying terms yields

$$0 \to k^\times/(k^\times)^p \to H^1(k;\mu_p) \to H^1(k;(k^s)^\times).$$

■

Example 6.3.3 ***(?):*** What is $H^1(k;(k^s)^\times)$? Use that $L^\times = \mathrm{Aut}(V_{/L})$ where V is a 1-dimensional vector space over L. The claim is that by Galois descent, forms for a vector space split by L are precisely vector spaces over k, which makes them all trivial. This in fact implies the more general fact that $H^1(k;\mathrm{GL}_n(k^s)) = 1$.

Remark 6.3.4: Kummer theory gives us an explicit form of the map and identifying terms yields

$$0 \to k^\times/(k^\times)^p \xrightarrow{x\mapsto k[x^{\frac{1}{p}}]} H^1(k;\mu_p) \to H^1(k;(k^s)^\times).$$

This can be found by unwinding the definition of the map from the snake lemma, or noting that the kernel of a map from the absolute Galois group cuts out exactly this field.

6.4 Geometry of Brauer Groups

Example 6.4.1 ***(of H^1):*** $H^1(k;G)$ are forms of objects with automorphism groups G.

- Vector spaces are obtained by taking $G = \mathrm{GL}_n$.
- Forms of $\mathbb{P}^n$, i.e. Severi-Brauer varieties, come from taking $G \coloneqq \mathrm{PGL}_{n+1}$.
- For G finite, a form of G is an étale k-algebra (product of separable extensions of k with total Galois group G).
  - For G simple, these are Galois extensions with Galois group G. For $G \coloneqq \mathbb{Z}/p$, this is Kummer theory.
- For E an elliptic curve, all genus 1 curves are torsors for their Jacobian. So genus 1 curves C with $\mathrm{Jac}(C) \cong E$ biject with $H^1(k;E(k^s))$.

Remark 6.4.2: We'll now look at H^2, and there is a correspondence

$$H^2(G;A) \xrightarrow{\sim} \left\{ \xi : \ 0 \longrightarrow A \longrightarrow G' \overset{s}{\longleftarrow} G \longrightarrow 1 \right\}$$

Given a set-theoretic section $s : G \to G'$, we get a map

$$\begin{aligned} f_s : G^{\times^2} &\to A \\ (g_1, g_2) &\mapsto s(g_1)s(g_2)s(g_1g_2)^{-1}. \end{aligned}$$

Note that if s is a group morphism, this is just the constant map.

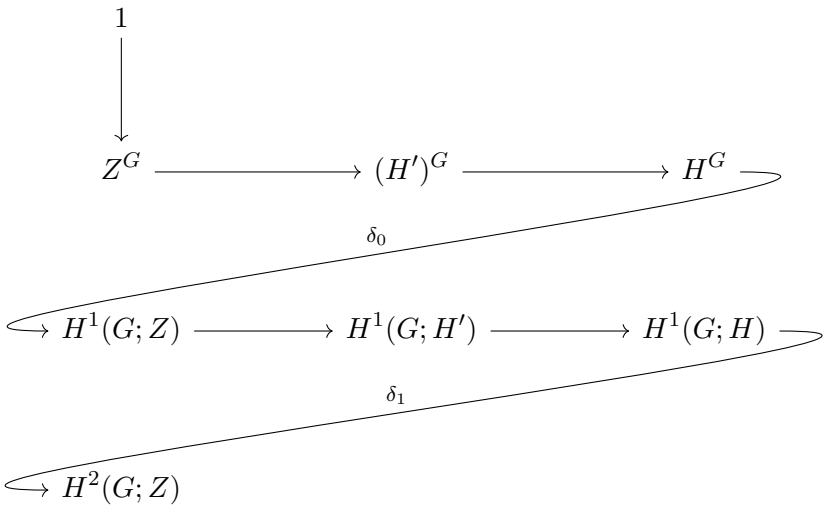
Claim: One needs to show the following:

1. $\delta f_s = 0$, so one gets a cocycle.
2. Changing s changes f_s by a coboundary.
3. Make the inverse.

The group operation here is $G' \cdot G'' \coloneqq G' \underset{G}{\times} G''/A$, and the multiplication map is

$$(a_1, g_1) \cdot (a_2, g_2) \coloneqq (a_1 a_2 f_s(g_1, g_2),\ g_1 g_2).$$

Remark 6.4.3: Suppose $1 \to Z \to H' \to H \to 1$ is a SES of groups with a G-action such that Z is in the center of H'. Then there is a "LES"



Link to Diagram

Note that some terms here are only sets, so exactness means that differentials surject onto kernels, and $H^1(G;Z) \curvearrowright H^1(G;H')$ and $H^1(G;H)$ is the quotient by this action.

Remark 6.4.4:

Definition 6.4.5 (Brauer group)
Take $1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1$, then we get a map

$$H^1(k; \mathrm{PGL}_n(k^s)) \xrightarrow{\iota_n} H^2(k, (k^s)^\times).$$

Then define the **Brauer group** of k to be

$$\mathrm{Br}(k) \coloneqq \bigcup_n \mathrm{im}(\iota_n).$$

Remark 6.4.6: Studying H^2 is hard in general, so this fact is the reason we can actually study Brauer groups.

Something about Hilbert 90

This surjection gives us geometric objects to work with. We'll show this is a group next time, along with the following theorem:

Theorem 6.4.7 *(?).*

$$\bigcup_n \mathrm{im}(\iota_n) = H^2(k; (k^s)^\times).$$

7 | Tuesday, September 07

7.1 Intro: Historical POV on Brauer Groups

Remark 7.1.1: Last time we defined $\mathrm{Br}(k) \coloneqq H^2(k; k^\times)$ and had a SES

$$1 \to (k^s)^\times \to \mathrm{GL}_n(k^s) \to \mathrm{PGL}_n \to 1.$$

We identified a subset of PGL_n-torsors in $H^1(k; \mathrm{PGL}_n(k^s)) \xrightarrow{\iota_n} H^2(k; (k^s)^\times)$, and alternatively defined $\mathrm{Br}(k) = \cup_n \mathrm{im}(\iota_n)$. We'll now look at geometric interpretations of elements of H^1.

Example 7.1.2 *(?):* $\mathrm{Aut}(X) = \mathrm{PGL}_n$ for the following:

- $\mathbb{P}^{n-1}$
- GL_n
- $\mathrm{Mat}(n \times n)$, by the Skolem-Noether theorem.

Corollary 7.1.3 *(?).*
For any of the X above, there is an isomorphism:

$$H^1(k; \mathrm{PGL}_n(k^s)) \xrightarrow{\sim} \{\text{Forms of } X\}_{/\sim} \xrightarrow{\sim} \{\mathrm{PGL}_n\text{-torsors}\}_{/\sim}.$$

Definition 7.1.4 (Severi-Brauers)
A **Severi-Brauer** variety over k is a form of $\mathbb{P}^n_{/k}$ for some n.

Example 7.1.5 *(?):*

- C a conic with no rational points, e.g. $x^2 + y^2 + z^2 = 0$ over $\mathbb{R}$.

- $\mathrm{Sym}^n C$ is a nontrivial Severi-Brauer if n is odd. It's difficult to write any down for even n, e.g. there are no Severi-Brauer surfaces over $\mathbb{R}$.

Definition 7.1.6 (CSAs/Azumaya Algebras)
A finite dimensional **central simple algebra** or **Azumaya algebra** over k is a associative algebra over k with no nontrivial 2-sided ideals with center k which is finite-dimensional as a k-vector space.

Theorem 7.1.7 ***(Classification of CSAs).***
Let $A \in \mathsf{Alg}_{/k}$, then TFAE:

- $\exists$ a finite separable extension $L_{/k}$ where after base-changing to L one obtains $A \otimes_k L \cong \mathrm{Mat}(n \times n, L)$.
- $A \otimes_k k^s \cong \mathrm{Mat}(n \times n, k^s)$.
- $\exists$ a finite (not necessarily separable) extension $L_{/k}$ such that $A \otimes_k L \cong \mathrm{Mat}(n \times n, L)$.
- A is a finite dimensional central simple algebra / Azumaya algebra.
- A is a matrix algebra over a finite-dimensional central k-division algebra.

This is essentially a classification theorem: they're all forms of matrix algebras over division algebras. Moreover there is a bijection

$$\{\text{Central simple } k\text{-algebras }\} \to H^2(k; (k^s)^\times).$$

Definition 7.1.8 (Opposite algebra)
If $A \in \mathsf{CSA}_{/k}$, then $A^{\mathrm{op}} \in \mathsf{CSA}_{/k}$ is an algebra with the same underlying vector space as A with $a \cdot_{\mathrm{op}} b \coloneqq ba$.

Definition 7.1.9 (Morita equivalence)
A, B are Morita equivalent if $A \otimes_k B^{\mathrm{op}}$ is isomorphic to a matrix algebra.

Theorem 7.1.10 ***(?).***
Given $A, B \in \mathsf{CSA}_{/k}$ which correspond to elements $[A], [B] \in H^2$, then

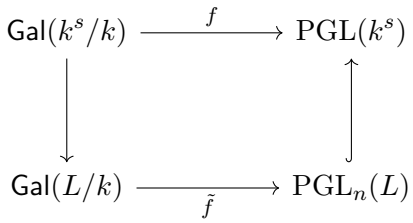
- $[A] = [B] \iff A, B$ are Morita equivalent.
- $[A]^{-1} = [A^{\mathrm{op}}]$.
- $[A] \cdot [B] = [A \otimes_k B]$.

7.2 The Boundary Map and Twisted Vector Space

Remark 7.2.1: We'd now like to make the boundary map explicit:

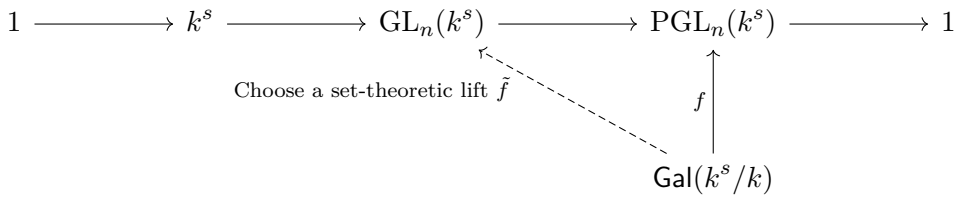
$$H^1(k; \mathrm{PGL}_n(k^s)) \to H^2(k; (k^s)^\times).$$

Given $[f] \in H^1$, choose a representable cocycle f:



Link to Diagram

To compute this boundary, we use the original SES:



Link to Diagram

So $\tilde{f} : \mathsf{Gal}(k^s/k) \to \mathrm{GL}_n(k^s)$ is a lieft of f, and δf measures the failure of $\tilde{f}$ to be a cocycle. We have

$$\delta\tilde{f}(\sigma,\tau) = \tilde{f}(\sigma\tau)\left(\tilde{f}(\sigma)\tilde{f}(\tau)^{\sigma}\right)^{-1} \in (k^s)^{\times},$$

using exactness since for f it lands in PGL_n and is trivial.

Definition 7.2.2 (Twisted vector spaces)
For $L_{/k}$ a separable extension and $\alpha : G^{\times^2} \to L^{\times}$ a 2-cocycle, so $[\alpha] \in H^2(L_{/k}; L^{\times})$, a **twisted vector space** is a twisted semilinear action of $\mathsf{Gal}(L_{/k})$ on L^n. I.e. it is a map

$$\tilde{f} : \mathsf{Gal}(L_{/k}) \to \mathrm{Aut}(L^n) = \mathrm{GL}_n(L)$$
$$\text{such that } \tilde{f}(\sigma\tau) = \tilde{f}(\sigma)\tilde{g}(\tau)^{\sigma}\alpha(\sigma,\tau).$$

Remark 7.2.3: For each $\sigma \in \mathsf{Gal}(L_{/k})$ we get a σ-semilinear automorphism of L^n, i.e. a map

$$f_\sigma : L^n \to L^n$$
$$\text{where } f_\sigma(s \cdot v) = \sigma(s) \cdot f_\sigma(v),$$

which is just the definition of semilinearity, and moreover $f_{\sigma\tau} = f_\sigma f_\tau \alpha(\sigma,\tau)$.

Remark 7.2.4: If $\alpha = \mathrm{id}$, an α-twisted vector space is the same as a k-vector space by Galois descent.

Proposition 7.2.5 ***(Properties of categories of twisted vector spaces).***

1. $\alpha \in \operatorname{im}\left(H^1(k;\mathrm{PGL}_n(k^s)) \to H^2(k;(k^s)^\times)\right) \iff$ there exists an n-dimensional α-twisted vector space.

   The proof of this is just unwinding definitions, it's literally the same data!

2. The category Tw_α of α-twisted vector spaces is abelian – the only nontrivial thing to check is that there are enough injectives.

3. There are natural functors

$$\begin{aligned}(-)\otimes(-) &: \mathsf{Tw}_\alpha \times \mathsf{Tw}_{\alpha'} \to \mathsf{Tw}_{\alpha\alpha'}\\ \mathrm{Hom}(-,-) &: (\mathsf{Tw}_\alpha)^{\mathrm{op}} \times \mathsf{Tw}_{\alpha'} \to \mathsf{Tw}_{\alpha'\alpha^{-1}}\\ \mathrm{Sym}^n, \bigwedge^n &: \mathsf{Tw}_\alpha \to \mathsf{Tw}_{\alpha^n}.\end{aligned}$$

4. If $F_{/k}$ is a separable field extension, then

$$(-)\otimes F : \mathsf{Tw}_{\alpha/k} \to \mathsf{Tw}_{\alpha/F}.$$

5. There is an equivalence of categories

$$\mathsf{Tw}_{\mathrm{id}/k} \xrightarrow{\sim} \mathsf{k\text{-}Mod}.$$

Proposition 7.2.6 ***(?).***
There is a 1-dimensional α-twisted vector space iff $[\alpha] = 1 \in H^1(k;(k^s)^\times)$.

Proof (?).
$\Longleftarrow$: First suppose $\alpha \equiv 1$, then $\mathsf{Tw}_\alpha \xrightarrow{\sim} \mathsf{Vect}_{/k}$, so just take the vector space k. If $\alpha = \delta g$ for some $g : \mathsf{Gal}(k^s/k) \to (k^s)^\times$. Then the action $\mathsf{Gal}(k^s/k) \curvearrowright k^s$ where $f_\sigma = g(\sigma)$ is a 1-dimensional α-twisted vector space by sending $1 \to g(\sigma)$ and extending semilinearly.
$\Longrightarrow$: Let V be a 1-dimensional α-twisted vector space. Choose an isomorphism $V \xrightarrow{\sim} k^s$ For each $\sigma \in \mathsf{Gal}(k^s/k)$ set $g(\sigma) = g(1)$ and $g(\sigma\tau) = g(\sigma)g(\tau)^\sigma\alpha(\sigma,\tau)$, then

$$\alpha = \delta g = g(\sigma\tau)\left(g(\sigma)g(\tau)^\sigma\right)^{-1}.$$

■

Theorem 7.2.7 ***(?).***
Suppose $\alpha \in H^2(k;(k^s)^\times)$ is in $\operatorname{im}\left(H^1(k;\mathrm{PGL}_n) \to H^2(k;(k^s)^\times)\right)$, then $\alpha^n = 1$.

Proof (?).
If α is in the image, there exists an n-dimensional α-twisted vector space $V \in \mathsf{Tw}_\alpha$, and so $\bigwedge^n V \in \mathsf{Tw}_{\alpha^n}$.

■

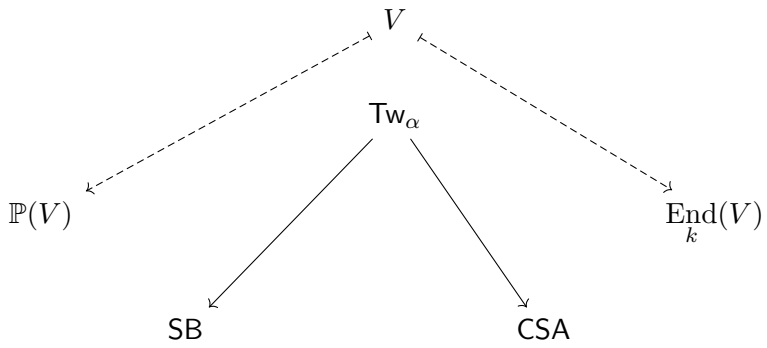
Definition 7.2.8 (Index and period)
Given $H^2(k;(k^s)^\times) = \mathrm{Br}(k)$ (which we'll prove soon), the **period** of α is the order of α, and the **index** is defined the minimal n such that α is in the above image. I.e.,

$$\begin{aligned}\mathrm{period}(\alpha) &:= \mathrm{Ord}(\alpha)\\ \mathrm{index}(\alpha) &:= \min\left\{n \;\middle|\; \alpha \in \mathrm{im}(H^1 \to H^2)\right\}.\end{aligned}$$

Corollary 7.2.9 *(?).*
Period divides index.

Question 7.2.10
An open question: how different are the period and index? See the period-index problem.

Remark 7.2.11: There are some maps between the categories Tw_α, SB (Severi-Brauers), and CSA:



Link to Diagram

An analogy is that in vector spaces, $\mathbb{P}^n$ is to $\mathrm{End}(V)$ as SB is to CSA in twisted vector spaces. Note that $\mathsf{Gal}(L/k)$" $\curvearrowright$ "V, which isn't a true action but only fails to be one up to a scalar. Thus projectivizing yields a semilinear action $\mathsf{Gal}(L/k) \curvearrowright \mathbb{P}(V)$, and Galois descent yields forms of $\mathbb{P}(V)_{/k}$.

Remark 7.2.12: Why is $\mathrm{End}(V)$ a form of $\mathrm{Mat}(n\times n)$? Since $V \in \mathsf{Tw}_\alpha$, split it: choose an L such that $\alpha|_L$ is trivial. Then $\mathsf{Tw}_{\alpha|_L} = \mathsf{Vect}_{/L}$.

8 | Thursday, September 09

Remark 8.0.1: Last time: 3 geometric avatars of elements α of a Brauer group:

- α-twisted vector spaces Tw_α

- After projectivizing: Severi-Brauer varieties
- Taking endomorphisms: central simple algebras.

Here we set $G \coloneqq \mathsf{Gal}(L_{/k})$ and $\alpha : G^{\times^2} \to L^\times$ representing $[\alpha] \in H^2(G; L^\times)$, and defined an α-twisted vector space as a $V \in \mathsf{Vect}_{/L}$ with a semilinear map $f_\sigma : V \to V$ for each $\sigma \in G$ where $\sigma(\ell v) = \sigma(\ell)\sigma(v)$ such that $f_{\sigma\tau} = f_\sigma \circ f_\tau \alpha(\sigma\tau)$. Last time we used this to show that

$$\operatorname{im}\left(H^1(k; \mathrm{PGL}_n) \to H^2(k; (k^s)^\times)\right)$$

is n-torsion.

Theorem 8.0.2 *(?).*
The category Tw_α is **semisimple**, i.e. every SES splits, and every object is a direct sum of simple objects.

Proof (?).
Note that in vector spaces, $\underset{k}{\mathrm{Hom}}(A, B) \cong B \otimes_k A^\vee$, so $\underset{k}{\mathrm{Hom}}(-, B) = (-) \otimes_k B^\vee$ as functors. Take a SES

$$0 \to V_2 \to W \to V_1 \to 0 \in \mathsf{Tw}_\alpha.$$

We want to split this, a good trick to try every time: apply $\underset{\mathsf{Tw}_\alpha}{\mathrm{Mor}}(V_1, \cdot)$:

$$0 \to \underset{\mathsf{Tw}_\alpha}{\mathrm{Mor}}(V_1, V_2) \to \underset{\mathsf{Tw}_\alpha}{\mathrm{Mor}}(V_1, W) \to \underset{\mathsf{Tw}_\alpha}{\mathrm{Mor}}(V_1, V_1) \to 0.$$

This sequence is exact since we can write

$$\underset{\mathsf{Tw}_\alpha}{\mathrm{Mor}}(-, V_1) = (-) \otimes_k V_1{}^\vee.$$

It's enough to split this SES, since any splitting $s : \underset{\mathsf{Tw}_\alpha}{\mathrm{Mor}}(V_1, V_2) \to \mathrm{Mor}(V_1, W)$ would allow taking $s(\mathrm{id}_{V_1})$ to split the original. But this sequence does split, since $\underset{\mathsf{Tw}_\alpha}{\mathrm{Mor}}(V_1, V_1)$ is free, thus projective.

■

Theorem 8.0.3 *(?).*
Any two simple objects $D_1, D_2 \in \mathsf{Tw}_\alpha$ are isomorphic.

Remark 8.0.4: This is an analog of showing that every vector space is a sum of 1-dimensional sub-vector spaces, i.e. every vector space has a basis. In this situation, it's essentially Schur's lemma.

Proof (?).
$\underset{\mathsf{Tw}_\alpha}{\mathrm{Mor}}(D_1, D_2) \in \mathsf{Vect}_{/L}$ is of dimension $d = \dim_L(d_1) \dim_L(d_2) > 0$, so there exists a nonzero map $f : D_1 \to D_2$. The claim is that f is an isomorphism: since both objects are simple, just use that $\ker D_1 \leq D_1$ and $\operatorname{im} f \leq D_2$ are sub-objects.

■

Corollary 8.0.5 *(?).*
There exists a unique simple object D of Tw_α, and every other object is of the form $D^{\oplus I}$.

Corollary 8.0.6 *(?).*
Any CSA is a matrix algebra over a division algebra.

Proof (?).
$\mathrm{End}(D^{\oplus n}) = \mathrm{Mat}(n \times n, \mathrm{End}(D))$, so it's enough to show $\mathrm{End}(D)$ is a division algebra. This follows by the previous argument, again using Schur's lemma.

■

Corollary 8.0.7 *(?).*
For $X_{/k}$ a Severi Brauer, $X \cong \mathbb{P}^n_{/k} \iff X(k) \neq \emptyset$.

Proof (?).
$\implies$: Clear, since $\mathbb{P}^n$ has rational points!
$\impliedby$: We'll do a variant of the proof that uses Tw_α. Let $X = \mathbb{P}(V)$ for $V \in \mathsf{Tw}_\alpha$, then any point $x \in X$ yields a 1-dimensional (twisted!) subspace $R \subseteq V$. Then $[\alpha] = 0 \in H^2(k; (k^s)^\times)$, and by Hilbert 90 this comes from a point in the following composition:

$$H^1(k; \mathrm{GL}_n) \longrightarrow H^1(k; \mathrm{PGL}_n) \longrightarrow 0 \in H^2(k; (k^s)^\times)$$

$$[\alpha] \longmapsto [X] \longmapsto 0$$

Link to Diagram

This forces $X = \mathbb{P}^n$.

■

Proof ($\impliedby$, classical proof).
Let $X \in \mathsf{SB}$ with $X(k) \neq \emptyset$, then Artin defines $X^\vee$, a dual Severi Brauer variety. This is constructed using that $X_{k^s} = \mathbb{P}^n$ and sets ${X_{k^s}}^\vee = (\mathbb{P}^n)^\vee$, which comes with descent data to k. A rigorous construction is that if $X = \mathbb{P}(V)$, we set $X^\vee = \mathbb{P}(V^\vee)$. If X has a k-point, then $X^\vee$ has a rational hyperplane H. The claim is that $X^\vee = \mathbb{P}^n$: this follows from the fact that $\mathcal{O}(H)$ is a line bundle on $X^\vee$ which is isomorphic to $\mathcal{O}(1)$ on $(\mathbb{P}^n)^\vee$ after base changing to k^s. This follows from cohomology of base change, since

$$\Gamma\left(X^\vee, \mathcal{O}(H)_{/k^s}\right) = \Gamma\left({X_{k^s}}^\vee, \mathcal{O}(H)_{/k^s}\right) = \Gamma\left(\mathbb{P}^n_{/Y}, \mathcal{O}(1)\right).$$

So $\mathcal{O}(H)$ yields a map $X^\vee \to \mathbb{P}^n$ which is an isomorphism after passing to k^s. Now we can write $X = (X^\vee)^\vee$ and $X^\vee = \mathbb{P}^n$, so

$$X = (X^\vee)^\vee = (\mathbb{P}^n)^\vee \cong \mathbb{P}^n.$$

■

Definition 8.0.8 (Reduced norm and trace)
Let $A \in \mathsf{CSA}_{/k}$, then there are maps

$$\begin{aligned} \mathrm{Nm}_{A_{/k}} &: A \to k && \text{multiplicative} \\ \mathrm{Tr}_{A_{/k}} &: A \to k && \text{additive.} \end{aligned}$$

How they're constructed: let $A \in \mathrm{End}(V) = V \otimes V^\vee$, then since $\bigwedge^*(-)$ is a functor, there is a map

$$\mathrm{Nm}_{A_{/k}} : \mathrm{End}(V) \to \mathrm{End}\left(\bigwedge^{\dim V} V\right) = k$$

$$\mathrm{Tr}_{A_{/k}} : \mathrm{End}(V) \xrightarrow{\sim} V \otimes V^\vee \xrightarrow{\langle -,\, - \rangle} k.$$

Proposition 8.0.9 ***(?).***
For $A \in \mathsf{CSA}_{/k}$, then if there exists a nonzero $f \in A$ with $\mathrm{Nm}_{A_{/k}}(f) = 0$, then A is not a division algebra.

Algebra: nontrivial matrix algebra over a field implies existence of matrices with determinant zero.

Proof (?).
The norm is multiplicative, so if f is a unit then $\mathrm{Nm}(ff^{-1}) = 1 \neq 0$.

■

Theorem 8.0.10 ***(?).***
There is a surjection

$$\bigcup_n H^1(k; \mathrm{PGL}_n) \twoheadrightarrow H^2(k; (k^s)^\times).$$

Proof (sketch).
It's enough to show the following surjection:

$$\bigcup_n H^1(L_{/k}; \mathrm{PGL}_n) \to H^2(L_{/k}; L^\times).$$

Given α in the codomain, interpret it as a central extension:

$$1 \to L^\times \to M_\alpha \to \mathsf{Gal}(L_{/k}) \to 1.$$

Definition ***(Semilinear group rings)***
Define $L[M_\alpha]$ to be the **semilinear group ring** of M_α:

$$L[M_\alpha] \bigoplus_{\lambda \in M_\lambda} L[e_\lambda]$$

where $e_{\lambda_1} e_{\lambda_2} = e_{\lambda_1 \lambda_2}$ and $\ell e_\lambda = e_\lambda \lambda(\ell)$.

Claim: $A_\alpha \coloneqq L[M_\alpha] / \langle \lambda e_1 - 1 e_\lambda \rangle$ is a CSA mapping to $[\alpha]$. See Serre's *Local Fields*.

■

Question 8.0.12
Can this construction be done in SB or Tw_α?

8.1 Computing Brauer Groups

Remark 8.1.1:

Claim: $\mathrm{Br}(\mathbb{F}_q) = 0$.

Theorem 8.1.2 ***(?).***
Let k be a C_1-field, so any homogeneous polynomial in k with degree $d < n$ has a nonzero solution. Then $\mathrm{Br}(k) = 0$.

Remark 8.1.3: Note that Chevalley–Warning exactly says that finite fields are C_1.

Proof (of theorem).

Claim: Let $A \in \mathsf{CSA}_{/k}$, then $\mathrm{Nm}_{A_{/k}} : A \to k$ is a polynomial function on n^2 variables of degree n.

Proof (?).
This is true for the actual determinant, and this is a claim that can be checked after passing to k^s since the norm is a *form* of the determinant.

■

Corollary 8.1.4 ***(?).***
If k is C_1 and $\operatorname{rank} A > 1$, there exists a nonzero $f \in A$ such that $\mathrm{Nm}_{A_{/k}}(f) = 0$.

But all k-division algebras are isomorphic to k, here all CSAs are of the form $\mathrm{Mat}(n \times n, k)$, so the Brauer group is trivial.

■

Theorem 8.1.5 ***(Tsem).***
If $k = \bar{k}$ and $C_{/k}$ is a smooth proper curve, then the function field $k(C)$ is C_1.

Proof (?).
Let f be a homogeneous polynomial, $\deg f = d$, in n variables over $k(C)$ with $d < n$. Then regard $f : k(C)^n \to k(C)$, we want to show $f^{-1}(0)$ is big. Let $p \in C$, and now f as a map

$$f : \Gamma\left(C; \mathcal{O}(r \cdot p)^n\right) \to \Gamma\left(C; \mathcal{O}(rd \cdot p)\right),$$

which is a polynomial map of finite dimensional vector spaces that are subspaces of the previous domain/codomain. Using Riemann-Roch, the dimension of the left-hand side grows like $r \cdot n$ and the right-hand side grows like $r \cdot d$, and for r large enough, $rn > rd$. Since f is homogeneous, $f^{-1}(0)$ contains 0, so $\dim f^{-1}(0) > 0$. But a positive-dimensional variety over

an algebraically closed field has lots of rational points!

■

9 | Tuesday, September 14

Remark 9.0.1: Goal: Severi-Brauer varieties satisfy the Hasse principle, and develop the Brauer-Manin obstruction. We have the following theorem: if $X \in \mathsf{SB}_{/k}$, then TFAE:

- X has a rational point,
- $X \cong \mathbb{P}^n$ for some n,
- $[X] \in \mathrm{Br}(k)$ is the trivial class.

We'll soon prove the following theorem:

Theorem 9.0.2 ***(Hasse principle for Severi Brauers).***
For K a number field, there is an injective map

$$\mathrm{Br}(k) \hookrightarrow \bigoplus_{v \in \mathrm{Pl}(k)} \mathrm{Br}(k_v),$$

which is a statement of the Hasse principle, since the previous theorem shows that if $\mathrm{Br}(k_v)$ is empty for all k_v, it will have to come from a zero class in $\mathrm{Br}(k)$

Remark 9.0.3: Note that the cokernel of this map is prominent in class field theory! Today we'll compute $\mathrm{Br}(k_v)$, or more generally $\mathrm{Br}(F)$ for F a local field.

9.1 Cyclic Algebras

Remark 9.1.1: Setup: take $k \in \mathsf{Field}$, $L_{/k}$ a C_n-Galois extension, which is the data of

$$\chi_L : \mathsf{Gal}(k^s_{/k}) \to C_n.$$

For $a \in K^s$, we'll consider pairs $(\chi, a) = L[x]^\chi / \langle x^n - a \rangle$ where commutation in $L[x]^\chi$ is given by $lx = x\sigma(\ell)$ for $l \in L$ where $C_n = \langle \sigma \rangle$. This is a k-vector space of dimension n^2, and the claim is that $(\chi, a) \in \mathsf{CSA}$.

Example 9.1.2 ***(?):*** Take $\chi : \mathsf{Gal}(\mathbb{C}_{/\mathbb{R}}) \to C_2$ with $a = -1$, then $(\chi, a) = \mathbb{H} = \mathbb{R}[i,j] / \left\langle i^2, j^2, [ij] \right\rangle$ is the (Hamilton) quaternions.

Fact 9.1.3
One can view $\chi \in H^1_{\mathsf{Gal}}(k; C_n)$ and

$$a \in H^1_{\mathsf{Gal}}(k; \mu_n) = k^\times / (k^\times)^{\cdot 2}.$$

In this case

$$(\chi, a) \coloneqq \chi \smile [a] \in H^2(k; \mu_n) \subseteq H^2(k; (k^{\text{sep}})^\times).$$

Note that this cup product can be computed explicitly from the product on Ext or using the standard resolution.

Remark 9.1.4: Now to compute more Brauer groups! So far, we've only done relatively trivial examples. We'll start with local fields: for algebraically closed fields, Galois cohomology vanishes, so

- $\mathrm{Br}(\mathbb{C}) = 0$
- To compute $\mathrm{Br}(\mathbb{R}) = H^2(\mathsf{Gal}(\mathbb{C}_{/\mathbb{R}}); \mathbb{C}^\times)$, take the resolution

$$P^\bullet: \quad \begin{array}{cc} \vdots & \\ \mathbb{Z}[x]/\left\langle x^2-1\right\rangle & \\ \downarrow{\scriptstyle x-1} & \\ \mathbb{Z}[x]/\left\langle x^2-1\right\rangle & \\ \updownarrow{\scriptstyle x+1} & \\ \mathbb{Z}[x]/\left\langle x^2-1\right\rangle & \\ \downarrow{\scriptstyle x-1} & \\ \mathbb{Z}[x]/\left\langle x^2-1\right\rangle & 1 \\ \downarrow & \downarrow \\ \mathbb{Z} & 1 \end{array}$$

Link to Diagram

Then we can take $H^*(\underset{\mathsf{Gal\text{-}Mod}}{\mathrm{Hom}}(P^\bullet, \mathbb{C}^\times))$:

$$1 \longrightarrow z\bar{z}$$

$$\mathbb{C}^\times \longrightarrow \mathbb{C}^\times \longrightarrow \mathbb{C}^\times \longrightarrow \mathbb{C}^\times$$

$$z \longrightarrow \bar{z}z^{-1} \qquad\qquad z \longrightarrow \bar{z}z^{-1}$$

Link to Diagram

Check that $\bar{z}z^{-1} = 1$ then $z = \bar{z}$ so $z \in \mathbb{R}^\times$ and $\ker d = \mathbb{R}^\times$. Similarly, $\operatorname{im} d = \mathbb{R}^\times_{>0}$, so

$$\mathrm{Br}(\mathbb{R}) = \mathbb{R}^\times/\mathbb{R}^\times_{>0} = \{\pm 1\}.$$

Example 9.1.5 *(?):* $\mathbb{H}$ represents -1 in $\mathrm{Br}(\mathbb{R})$, as does the corresponding Severi Brauer

$$\left\{x^2 + y^2 + z^2 = 0\right\} \subseteq \mathbb{P}^2_{/\mathbb{R}}.$$

Note that $+1$ is represented by the field itself, regarded as a 1×1 matrix algebra, or projective space.

Remark 9.1.6: Write k^{un} for the maximal unramified extensions, where an extension is *ramified* if the degree of the residue field changes (or the valuation remains an integer?) For example, for $k = \mathbb{Q}_p$, we have $k^{\mathrm{un}} = \mathrm{ff}(W(\overline{\mathbb{F}_p}))$ (i.e. the Witt vectors). In general, $k^{\mathrm{un}} = k(\mu'_\infty)$ where μ'_∞ is the set of roots of unity of order prime to the characteristic. As a corollary, $\mathsf{Gal}(k^{\mathrm{un}}_{/k}) = \overline{\mathbb{F}_q}/\mathbb{F}_1 = \widehat{\mathbb{Z}}$.

Theorem 9.1.7 *(?).*
For k a nonarchimedean local field (a finite extension of $\mathbb{Q}_p$), then $\mathrm{Br}(k) = \mathbb{Q}/\mathbb{Z}$

- $H^2(k^{\mathrm{un}}_{/k}; (k^{\mathrm{un}})^\times) = \mathbb{Q}/\mathbb{Z}$
- $H^2(k^{\mathrm{un}}_{/k}, (k^{\mathrm{un}})^\times) \xrightarrow{\sim} H^2(k; (k^s)^\times) = \mathrm{Br}(k)$ is an isomorphism.

Remark 9.1.8: Many proofs of this are delicate! We'll follow a mix of Cassels-Frolich and Milne for this proof.

Proof (of 1).
Take the SES coming from the valuation map:

$$1 \longrightarrow U_{k^{\mathrm{un}}} \longrightarrow (k^{\mathrm{un}})^\times \xrightarrow{\mathrm{val}} \mathbb{Z} \longrightarrow 0$$

Link to Diagram

Claim:
- $H^2(k^{\mathrm{un}}_{/k}; \mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.
- $H^*(k^{\mathrm{un}}_{/k}; U_{k^{\mathrm{un}}}) = 0$

Remark 9.1.9: Why this implies the theorem: take the LES in cohomology to get the following:

$$H^2(k^{\mathrm{un}}_{/k}; U_{k^{\mathrm{un}}}) = 0 \longrightarrow H^2(k^{\mathrm{un}}_{/k}; (k^{\mathrm{un}})^\times) \longrightarrow H^2(k^{\mathrm{un}}_{/k}; \mathbb{Z})$$
$$H^3(k^{\mathrm{un}}_{/k}; U_{k^{\mathrm{un}}}) = 0$$

Link to Diagram

A claim is that $H^2(k^{\text{un}}_{/k}; \mathbb{Z}) = H^2(\widehat{\mathbb{Z}}; \mathbb{Z})$. One can compute this colimit explicitly, but there is a SES

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Now note that $H^{>0}(G; \mathbb{Q}) = 0$ for profinite groups, since this is necessarily a torsion $\mathbb{Q}$-vector space. For a full proof, use that multiplication by n is an isomorphism the annihilates it. As a corollary, taking the LES above yields $H^i(G; \mathbb{Z}) = H^{i-1}(G; \mathbb{Q}/Z)$ for $i \geq 2$. Thus

$$H^2(\widehat{\mathbb{Z}}; \mathbb{Z}) = H^1(\widehat{\mathbb{Z}}; \mathbb{Q}/\mathbb{Z}) = \underset{\mathsf{Top}}{\mathrm{Hom}}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z},$$

and in fact

$$H^1(\widehat{\mathbb{Z}}; \mathbb{Q}/\mathbb{Z}) = \varinjlim_n \mathrm{Hom}(C_n; \mathbb{Q}/\mathbb{Z}).$$

■

Proof (of b).
Here we'll have to use the structure of $U_{k^{\text{un}}}$. It's enough to show

$$H^{>0}(k_{n/k}; U_{k_n}) = 0$$

for $k_{n/k}$ unramified of finite degree n, using that these are unique. We'll use the following:

Definition *(?)*
There is a filtration $\mathrm{Fil}_r U_{k_n} = \left\{ u \in U_{k_n} \;\middle|\; u = 1 \bmod \pi^r \right\}$ for π a uniformizer.

Fact
We can identify

$$\mathrm{Fil}_r / \mathrm{Fil}_{r+1} = \begin{cases} \kappa_n^\times & r = 0 \\ \kappa_n^+ & r > 0. \end{cases},$$

where κ denotes residue fields, $\kappa_{n/\kappa}$ is the unique degree n extension, and κ^+ is the additive group. Why: use that these look like power series, and the associated graded picks off the rth coefficient. Moreover, things like $1 + \pi^2$ can be units by formally inverting using geometric series.

Thus it's enough to show for residue fields that

$$H^{>0}(\kappa_{n/\kappa}; \kappa_n^\times) = 0$$
$$H^{>0}(\kappa_{n/\kappa}; \kappa_n^+) = 0,$$

since each graded piece of the associated grading having zero cohomology implies the entire thing has zero cohomology.
For the first,

- $i = 1$ is Hilbert 90,
- $i = 2$ follows from $\mathrm{Br}(\kappa_{n/\kappa}) = 0$,
- $i \geq 3$ uses that $H^* = H^*[-2]$, since the resolution used for cohomology of a cyclic group was 2-periodic.

For the second, to compute the cohomology of a cyclic group we take the 2-periodic resolution:

$$x \xrightarrow{\text{Frob}-1} x^q - x$$

$$k_n \longrightarrow k_n \longrightarrow k_n \longrightarrow \cdots$$

$$x \xrightarrow{\mathrm{tr}_{\kappa_n/\kappa}} \sum x^{q^i}$$

Link to Diagram

Then

- $H^2 = \ker / \operatorname{im}$, and $\ker = k$ since Frobenius fixes everything, and use that
$$\sum x^{q^i} = x + x^q + x^{q^2} + \cdots = \mathrm{tr}_{\kappa_n/\kappa}(x).$$
- If n is invertible, so $p \nmid n$, writing $\mathrm{Tr}(1) = n$ we can take $\mathrm{Tr}(a/n) = a$.
- It suffices to show this polynomial isn't identically zero, but it's a polynomial of degree q^{n-1} but $\#\kappa_n = q^n$.
- Now use that $a = \mathrm{tr}(x)$ for some $a^\bullet$, then take $b = \mathrm{tr}(bx/a)$.

■

10 Thursday, September 16

10.1 Computing Brauer Groups

Remark 10.1.1: Let k be a p-adic field, our goal is to show $\mathrm{Br}(k) = \mathbb{Q}/\mathbb{Z}$. We were trying to show

1. $H^2(k^{\mathrm{un}}_{/k}; (k^{\mathrm{un}})^\times) = \mathbb{Q}/\mathbb{Z}$,
2. Any Brauer class is split by an *unramified* extension

This says that we can split the computation of $\mathrm{Br}(k)$ into an interesting part (the ramified case) and a trivial part (the unramified case).

Check 2!

To prove 1, we used

$$1 \to U_{k^{\mathrm{un}}} \to (k^{\mathrm{un}})^\times \to \mathbb{Z} \to 0,$$

and

a. $H^2(k^{\mathrm{un}}_{/k}; \mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$,
b. $H^{>0}(k^{\mathrm{un}}_{/k}; U_{k^{\mathrm{un}}}) = 0$,

where we used a filtration

$$\mathrm{Fil}_r U_{k^{\mathrm{un}}} = \begin{cases} U_{k^{\mathrm{un}}} & r = 0 \\ \left\{ x \;\middle|\; x \equiv 1 \bmod \pi^r \right\} & r \geq 1. \end{cases}$$

and

$$\mathsf{gr}^r(\mathrm{Fil}_\bullet U_{k^{\mathrm{un}}}) = \begin{cases} \kappa^\times & r = 0 \\ \kappa & r \geq 1. \end{cases}.$$

We now want to show

- $H^{>0}(k^{\mathrm{un}}_{/k}; \bar{\kappa}^\times) = H^{>0}(\kappa; \bar{\kappa}^\times)$
- $H^*(k^{\mathrm{un}}_{/k}; \bar{\kappa}^\times) = H^*(\kappa; \bar{\kappa}^\times) = 0$, and we were working on $* = 2$.

Proposition 10.1.2 *(?).*
For k any field, $H^1(k; (k^{\mathrm{sep}})^+) = 0$, where k^+ denotes taking the additive group.

Proof (?).
H^1 here classifies forms of SESs

$$0 \to k \to V \to k \to 0,$$

since automorphisms of this SES correspond to matrices $\left\{ \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \;\middle|\; * \in k^+ \right\} \cong k^+$. But any form of this splits, since any SES of vector spaces splits.

■

Theorem 10.1.3 *(?).*
For k any field, $H^{>0}(k; (k^{\mathrm{sep}})^+) = 0$.

Proof (?).
It's enough to show this for finite extensions, so consider $H^{>0}(L_{/k}; L^+) = 0$. The normal basis theorem implies that $L^+ \cong k[G]$ as a G-module, since this is the regular representation. We'll

use the following common lemma:

Lemma 10.1.4 ***(Shapiro's Lemma).***
If $H \leq G$ are finite groups and $M \in \mathsf{H\text{-}Mod}$ then

$$H^*(G; \operatorname*{Ind}_H^G M) \cong H^*(H; M), \qquad \operatorname*{Ind}_H^G M = M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G].$$

Now use that

$$H^*(\mathsf{Gal}(L_{/k}); k[\mathsf{Gal}(L_{/k})]) = H^*(1; k) = 0 \qquad * > 0.$$

■

Proof (of Shapiro's lemma).
Let $P^\bullet \rightrightarrows \mathbb{Z} \in \mathbb{Z}[\mathsf{G}]\text{-}\mathsf{Mod}$ be a free resolution and use Frobenius reciprocity to write

$$\begin{aligned} H^*(G; \operatorname*{Ind}_H^G M) &= H^*(\mathrm{Hom}(P^\bullet, \operatorname*{Ind}_H^G M)) \\ &= H^*(\mathrm{Hom}(\operatorname*{Res}_H^G P^\bullet, M)) \\ &= H^*(H; M), \end{aligned}$$

where $\operatorname*{Res}_H^G P^\bullet \rightrightarrows \mathbb{Z} \in \mathbb{Z}[\mathsf{H}]\text{-}\mathsf{Mod}$ is a free resolution, since $P^\bullet = \mathbb{Z}[G]^{\oplus I}$ (using that it's free) and thus $\operatorname*{Res}_H^G P^\bullet = \mathbb{Z}[H]^{\oplus I'}$.

■

Proof (of theorem, part b).
We now want to prove (3),

$$H^*(k^{\mathrm{un}}_{/k}; U_{k^{\mathrm{un}}}/\mathrm{Fil}^r) = 0 \qquad * > 0.$$

By induction on r, since we have a SES

$$0 \to \mathrm{Fil}^{r-1}/\mathrm{Fil}^r \to U_{k^{\mathrm{un}}}/\mathrm{Fil}^r \to U_{k^{\mathrm{un}}}/\mathrm{Fil}_{r-1} \to 1,$$

where H^* of the two outer terms vanishes and thus so does H^* of the middle by the LES in cohomology.
For (4), we want to show $H^*(k^{\mathrm{un}}_{/k}; U_{k^{\mathrm{un}}}) \to \varprojlim_r H^*(k^{\mathrm{un}}_{/k}; U_{k^{\mathrm{un}}}/\mathrm{Fil}_r)$. We can move an inverse limit in:

$$\begin{aligned} \varprojlim_r \varprojlim_n H^*(k_{n/k}; U_{k^{\mathrm{un}}}/\mathrm{Fil}^r) &= \varprojlim_r \varprojlim_n H^*(\mathrm{Hom}(P^\bullet, U_{k^{\mathrm{un}}}/\mathrm{Fil}^r)) \\ &= H^*(k^{\mathrm{un}}_{/k}; \varprojlim_r U_{k^{\mathrm{un}}}/\mathrm{Fil}^r). \end{aligned}$$

This uses the Mittag-Leffler condition to show that $\varprojlim_1$ vanishes, which applies because we actually have surjectivity.

■

Theorem 10.1.5 ***(Hasse).***
If $D_{/k}$ is a division algebra over k a p-adic field (or any local field) with $\dim_k D = n^2$ (using that it's a form of a matrix algebra), then D is split by the unique **unramified** extension of k of degree n.

Remark 10.1.6: That there is a unique such extensions follows from the fact that $\widehat{\mathbb{Z}}$ has a unique subgroup of every index.

10.2 Proof of theorem

Remark 10.2.1: Write k_n for the unique unramified extension of degree n. We'll want to show

1. Show that it's enough to show $K_n \subseteq D$,
2. Actually show $k_n \subseteq D$.

Lemma 10.2.2 ***(?).***
For k any field and $D_{/k}$ any division algebra of $\dim_k D = n^2$, then if $L_{/k} \subseteq D$ is a Galois extension of degree n, then D splits over L.

This is true without the extension being Galois.

Proof (of lemma, using Tw*).*
Write $D = \mathrm{End}(V) \in \mathsf{Tw}_{/k}$ for some $V \in \mathsf{Tw}$ of dimension n, then

$$D \underset{k}{\times} L = \mathrm{End}(V \underset{k}{\times} L) \in \mathsf{Tw}_{/L}.$$

Then since $L \subseteq D$, we have $L \curvearrowright V$ so $L \otimes_k L \curvearrowright V_L$, then use that $L \otimes_k L \xrightarrow{\sim} L^n$ for $n := \#\mathsf{Gal}(L_{/k})$.

Why: write $L \otimes_k L = k[x]/I$ and use the Chinese remainder theorem!

We can write $L^n = \oplus L e_i$, so $V_L = \oplus e_i V_L$ which is dimension 1 and thus its Brauer class is trivial.

■

Remark 10.2.3: Other proofs of this seem much more difficult!

So now let's show k_n splits D. We'll need to develop some valuation theory for division algebras.

Definition 10.2.4 (Valuations on division algebras)
Define a valuation $v : D \to \mathbb{Z} \cup \{\infty\}$ extending the valuation on $K \subseteq D$ given by $1/n\mathrm{val}(\mathrm{Nm}_{D_{/k}}(x))$. Equivalently, for $x \in D$, use that $k(x) \subseteq D$ is a finitely generated k-algebra in which every nonzero element is a unit, so it's a field and carries a natural valuation.

Definition 10.2.5 (Valuation ring)
Define

$$\begin{aligned}\mathcal{O}_D &\coloneqq \left\{x \;\middle|\; v(x) \geq 0\right\} \subseteq D \\ \mathfrak{m}_D &\coloneqq \left\{x \;\middle|\; v(x) > 0\right\} \subseteq D \\ \mathcal{I} &\coloneqq \mathcal{O}_D/\mathfrak{m}_D,\end{aligned}$$

where $\mathfrak{m}_D \in \operatorname{mSpec} D$, and set

$f \coloneqq [\mathcal{I} : k]$	Degree of field extensions
$e \coloneqq [\operatorname{val}(k) : \operatorname{val}(D)]$	Ramification index.

Remark 10.2.6: Note that $\mathcal{I}$ is a field, since all division algebras over finite fields are field extensions (using our computation of the Brauer groups of fields).

Fact 10.2.7
$ef = n^2$, where the same proof for extensions of p-adic fields goes through.

Claim:

$$e = f = n.$$

Remark 10.2.8: We'll show

1. $e \leq n$,
2. $f \leq n$,

Then since $ef = n^2$ this forces $e = f = n$.

Lemma 10.2.9*(?).*
Any commutative $L \in \mathsf{Alg}_{/k}$ with $L \subseteq D$ satisfies $\dim_k L \leq n$.

Proof (?).
It's enough to prove this for $\operatorname{Mat}(n \times n; k)$, since the dimension won't change after passing to a finite extension, and proving here is classical.

Exercise *(?)*
Prove this!

■

Proof (of claim).
For (1): chose $\pi \in \mathcal{O}_D$ with $v(\pi) = 1/e$, i.e. something with minimal positive valuation. Then $k(\pi) \subseteq D$ is an extension over k of degree at most n, by the lemma.
For (2): Write $\mathcal{I} = \kappa(\alpha)$ for α a primitive element, and let $\tilde{\alpha} \in D$ be a lift. Then $k(\tilde{\alpha}) \subseteq D$ is a field extension of degree $\leq n$ by the lemma, and its residue field is $\mathcal{I}$.
■

Corollary 10.2.11 *(?).*
We have an exact equality

$$[k(\tilde{\alpha}) : k] = n,$$

so $k(\tilde{\alpha})_{/k}$ is unramified, and there's a unique such extension, and since $\kappa(\tilde{\alpha}) \subseteq D$.

Remark 10.2.12: A proof of this theorem using Tw or SB would be clarifying.

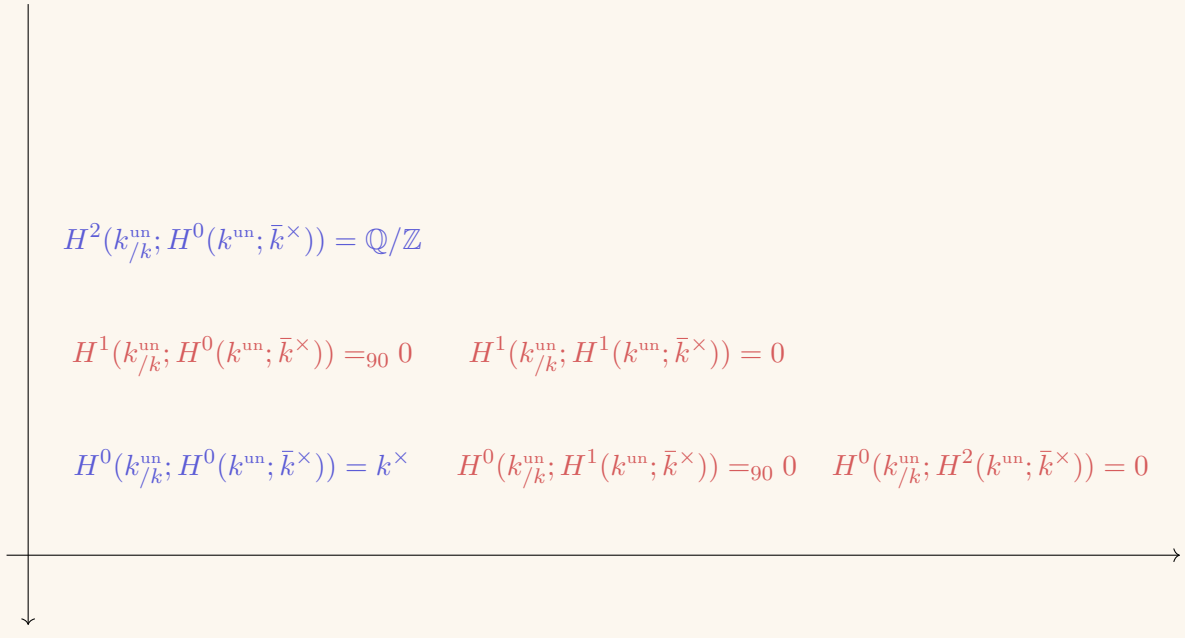
Claim: The following map is an isomorphism:

$$\mathbb{Q}/\mathbb{Z} \cong H^2(k^{\mathrm{un}}_{/k}; (k^{\mathrm{un}})^\times) \xrightarrow{\sim} H^2(k; \bar{k}^\times).$$

Proof (of claim).
Use that the LHS is isomorphic to $H^2(k^{\mathrm{un}}_{/k}; H^0(k^{\mathrm{un}}; \bar{k}^\times))$, and consider the Hochschild-Serre spectral sequence

$$H^p(k^{\mathrm{un}}_{/k}; H^q(k^{\mathrm{un}}; \bar{k}^\times)) \Rightarrow H^{p+q}(k; \bar{k}^\times).$$

The spectral sequence reads:



Link to Diagram

Then for degree reasons, there are no nontrivial differentials to kill the two nonzero terms. One can alternatively use the SES

$$0 \to \mathrm{Br}(k^{\mathrm{un}}_{/k}) \to \mathrm{Br}(k) \to \mathrm{Br}(k^{\mathrm{un}}).$$

■

11 | Tuesday, September 21

Remark 11.0.1: Last time: for k a p-adic field, we have $\mathrm{Br}(k) = \mathbb{Q}/\mathbb{Z}$. The plan for today:

- Examples
- A SES for L a number field:

$$0 \to \mathrm{Br}(L) \to \bigoplus_{v \in \mathrm{Pl}(k)} L_{\widehat{v}} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

- Possibly the Hasse-Minkowski theorem
- The Brauer-Manin obstruction.

11.1 Construction of Brauer classes over K

Remark 11.1.1: Fix a character to a cyclic group

$$\chi : \mathsf{Gal}(k^{\mathrm{sep}}{}_{/k}) \to C_n = \langle \sigma \rangle$$

and set k_χ to be the fixed field.

Definition 11.1.2 (Cyclic Algebra)
For $a \in k^\times/(k^\times)^{\cdot n}$, write

$$(\chi, a) = k_\chi \langle \sigma \rangle / \langle \sigma s = s^\sigma \sigma, \sigma^n - a \rangle \qquad s \in k_\chi.$$

Remark 11.1.3: We have

$$[(\chi, a)] \coloneqq [X] \smile [a] \in H^1(K; C_n) \cup H^1(K; \mu_n) = \mathrm{Br}(k).$$

There are cases where it's not known if these types of algebras are generators of certain Brauer groups.

Remark 11.1.4: For k a p-adic field and k_n the unique unramified degree n extension, we can construct a character

$$\chi_n : \mathsf{Gal}(k^{\mathrm{sep}}/k) \to \mathsf{Gal}(k_n/k) \xrightarrow[\text{can}]{\sim} C_n,$$

where the isomorphism is canonical, sending the Galois group to the Frobenius.

Theorem 11.1.5 ***(?).***
Let π be a uniformizer of $\mathcal{O}_K$. Every CSA is equivalent to one of the form

$$(\chi_n, \pi^m) \to \frac{m}{n} \in \mathbb{Q}/\mathbb{Z} = \mathrm{Br}(k).$$

Remark 11.1.6: If m, n are coprime one gets a division algebra.

Proof (Sketch).
This is mostly a computation that involves unwinding the isomorphism $\mathrm{Br}(k) \to \mathbb{Q}/\mathbb{Z}$. A sketch:

- The class $[(\chi_n, \pi)]$ has order n,
- The class $[(\chi_n, \pi)]^m = [(\chi_n, \pi^m)]$, which is given by a cup product.

■

Remark 11.1.7 ***(An algorithm to compute):*** Let D/k be a division algebra.

- Find a copy of k_n in D, which can be done since this is a division algebra of dimension n^2.
- There exists a $\sigma \in D$ such that $\sigma \curvearrowright K_n$ by conjugation is the canonical generator of $\mathsf{Gal}(k_n/k) \xrightarrow[\text{can}]{\sim} C_n$ (where we take Frob as the canonical generator).
- Then $[D] \mapsto \dfrac{v(\sigma)}{n} \in \mathbb{Q}/\mathbb{Z} = \mathrm{Br}(k)$, where v is the normalized valuation on D we constructed previously. Note that this is well defined since changing D changes the output by an integer.

Example 11.1.8 ***(The simplest case: $n = 2$):*** Using that there is in fact a canonical isomorphism $\mu_2 \cong C_2$ since there's only one nontrivial element in each group, we have

$$H^1(k; C_2) = H^1(k; \mu_2) = k^\times/(k^\times)^{\cdot 2}.$$

Hence any character

$$\chi : \mathsf{Gal}(k^{\mathrm{sep}}/k) \to C_2 = \mu_2$$

is represented by some $b_\chi \in k^\times/(k^\times)^{\cdot 2}$. So we have an identification

$$(\chi, a) \rightsquigarrow (b_\chi, a)_2 = (a, b_\chi)_2 = \begin{cases} 0 & v(a) \equiv v(b) \bmod 2 \\ \frac{1}{2} & \text{else.} \end{cases}$$

For the corresponding extension to be unramified, one needs the valuation to be zero. So for example taking $k(\pi)/k$ yields a ramified extension since $v(\pi) = 1$.

Note that here $(-,-)_n$ is generally a Hilbert or norm-residue symbol.

Exercise 11.1.9 (?)
Prove that these cyclic algebras are CSAs.

11.2 The SES

Remark 11.2.1: Our goal for today: for k a number field, show the following sequence is exact

$$0 \to \mathrm{Br}(k) \to \bigoplus_{v \in \mathrm{Pl}(k)} k_{\widehat{v}} \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \to 0.$$

Proposition 11.2.2 *(?).*
For $\alpha \in \mathrm{Br}(k)$, using the pullback of i_v,

$$\mathrm{Br}(K) \xrightarrow{\prod_{i_v^*}} \prod_v \mathrm{Br}(k_{\widehat{v}})$$

factors through $\bigoplus_v \mathrm{Br}(k_{\widehat{v}})$, i.e. $i_v^*(\alpha) = 0$ for almost all v.

Proof (of prop, proof 1).
First represent α by $X \in \mathsf{SB}$, so $X(k_{\widehat{v}}) \neq \emptyset$ for almost all v. This implies $X_{k_{\widehat{v}}} \cong \mathbb{P}^n_{/k}$ for almost all v.

■

Definition 11.2.3 (Ideles)

$$\mathbb{I}_k \coloneqq \prod_v{}' (k_{\widehat{v}}^\times, \mathcal{O}_{k_{\widehat{v}}}^\times) = \left\{ (x_v) \in \prod_v k_{\widehat{v}}^\times \;\middle|\; x_v \in \mathcal{O}_{k_{\widehat{v}}}^\times \text{ for almost all } v \right\}.$$

A basis of open sets is given by $(x) \cdot \prod_v \mathcal{O}_{k_{\widehat{v}}}^\times$.

⚠ Warning 11.2.4
There is a map

$$\begin{aligned} \mathbb{I}_k &\hookrightarrow \mathbb{A}_k^2 \\ x &\mapsto (x, x^{-1}), \end{aligned}$$

and there is a subspace topology – but this is not equivalent to the topology above, and is in fact a source of an infamous error!

Definition 11.2.5 (S-ideles)
If S is a finite set of places of K containing all infinite places, then define

$$\mathbb{I}_{k,S} = \prod_{v\in S} \widehat{k_v}^\times \times \prod_{v\notin S} \mathcal{O}^\times_{\widehat{k_v}} \subseteq \mathbb{I}_K.$$

Fact 11.2.6

$$\mathbb{I}_k = \varinjlim_S \mathbb{I}_{k,s}.$$

Remark 11.2.7: The idea will be to study the following SES of Galois modules:

$$1 \to L^\times \to \mathbb{I}_L \to C_L \to 1,$$

where C_L is the idele class group.

Proposition 11.2.8 *(?).*

$$H^2(L_{/k}; \mathbb{I}_L) = \bigoplus_{v\in \mathrm{Pl}(k)} \mathrm{Br}(L_{\widehat{v}/\widehat{k_v}})$$
$$H^2(k; \mathbb{I}_{k^{\mathrm{sep}}}) = \bigoplus_{v\in \mathrm{Pl}(k)} \mathrm{Br}(\widehat{k_v}),$$

Theorem 11.2.9 *(?).*

$$H^1(L_{/k}; C_L) = 0$$
$$H^2(L_{/k}; C_L) = [d] \in \mathbb{Q}/\mathbb{Z}, \quad d \coloneqq \frac{1}{[L:k]}.$$

This will imply

$$H^1(k; C_{k^{\mathrm{sep}}}) = 0$$
$$H^2(k; C_{k^{\mathrm{sep}}}) = \mathbb{Q}/\mathbb{Z}.$$

Proof (sketch).
We can write

$$\begin{aligned} H^2(L_{/k}; \mathbb{I}_L) &= H^2(L_{/k}; \varinjlim_T \mathbb{I}_{L,T}) \\ &= \varinjlim_T H^2(L_{/k}; \mathbb{I}_{L,T}), \end{aligned}$$

so it's enough to show that for S a finite set of places of K and T a set of places over S that

we have

$$H^2(L_{/k}; \mathbb{I}_{L,T}) = \bigoplus_{v \in S} \mathrm{Br}(L_{\widehat{v}/k_{\widehat{v}}}).$$

■

Exercise 11.2.10 (?)
Try to prove this, it uses Shapiro's lemma and isn't too difficult.

12 | Thursday, September 23

Remark 12.0.1: Let $k \in \mathsf{Field}$, we have a SES $1 \to k^\times \to \mathbb{I}_k \to C_k \to 1$. An exercise from last time: for $\mathrm{Pl}(k)$ the places of k, prove that

$$H^2(L_{/k}; \mathbb{I}_L) = \bigoplus_{v \in \mathrm{Pl}(k)} \mathrm{Br}(L_{\widehat{v}}/k_{\widehat{v}}),$$

where $L_{\widehat{v}}$ was obtained by choosing any place above v in L and completing.

12.1 Proof of Theorem

Remark 12.1.1: For $S \subseteq \mathrm{Pl}(k)$ a finite set of places containing all of the infinite places and T a set of places of L above S, we have

$$\mathbb{I}_{L,T} = \prod_{w \in T} L_w^\times \times \prod_{w \notin T} \mathcal{O}_{L_{\widehat{v}}}^\times.$$

We can also write $H^2(L_{/k}; \mathbb{I}_L) = \varinjlim_T H^2(L_{/k}; \mathbb{I}_{L,T})$, so it's enough to show the following:

$$H^2(L_{/k}; \mathbb{I}_{L,T}) = \bigoplus_{v \in S} \mathrm{Br}(L_{\widehat{v}}/k_{\widehat{v}})$$
$$H^2(L_{/k}; \mathbb{I}_{\bar{k},T}) = \bigoplus_{v \in S} \mathrm{Br}(k_{\widehat{v}}).$$

We have

$$H^2(L_{/k}; \mathbb{I}_{L,T}) = \prod_{v \in S} H^2(L_{/k}; \prod_{w_{/v}} L_w^\times) \times \prod_{v \in S} H^2(L_{/k}; \prod_{w_{/v}} \mathcal{O}_{L_w}^\times),$$

noting that we need to take the entire product to actually get a Galois module.

Claim:

$$H^2(L_{/k}; \prod_{w_{/v}} L_{\widehat{v}}^{\times}) = \mathrm{Br}(L_{\widehat{v}/k_{\widehat{v}}})$$
$$H^2(L_{/k}; \prod_{w_{/v}} L_{\widehat{v}}^{\times}) = 0.$$

Proof (of 1).

$$\begin{aligned} H^2(L_{/k}; \prod_{w_{/v}} L_w^{\times}) &= H^2(L_{/k}; \operatorname*{Ind}_{\mathsf{Gal}(L/k)}^{\mathsf{Gal}(L_{\widehat{v}}/k_{\widehat{v}})} L_{\widehat{v}}^{\times}) \\ &= H^2(L_{\widehat{v}/k_{\widehat{v}}}; L_{\widehat{v}}^{\times}) \\ &:= \mathrm{Br}(L_{\widehat{v}/k_{\widehat{v}}}). \end{aligned}$$

■

Proof (of 2).
Write

$$\begin{aligned} H^2(L_{/k}; \prod_{w_{/v}} L_w^{\times}) &= H^2(L_{/k}; \operatorname*{Ind}_{\mathsf{Gal}(L/k)}^{\mathsf{Gal}(L_{\widehat{v}}/k_{\widehat{v}})} \mathcal{O}_{L_{\widehat{v}}}^{\times}) \\ &= H^2(L_{\widehat{v}/k_{\widehat{v}}}; \mathcal{O}_{L_{\widehat{v}}}^{\times}) \\ &= 0. \end{aligned}$$

■

Corollary 12.1.2 ***(?).***

$$\begin{array}{ccc} \mathrm{Br}(k) & \longrightarrow & \bigoplus_v \mathrm{Br}(k_{\widehat{v}}) \\ \| & & \| \\ H^2(k; \bar{k}^{\times}) & \longrightarrow & H^2(k; \mathbb{I}_{\bar{k}}) \end{array}$$

Link to Diagram

12.2 Injectivity

Theorem 12.2.1 ***(Injectivity).***
$\mathrm{Br}(k) \hookrightarrow \bigoplus_v \mathrm{Br}(k_{\widehat{v}})$ is injective, since $H^1(L_{/k}; C_L) = 0$.

Theorem 12.2.2 ***(Actual IRL application of Sylow theorems).***
If G is a finite group and $M \in \mathsf{G\text{-}Mod}$ then $H^i(G; M) = 0$ if $H^i(G_p; M|_{G_p}) = 0$ for all p where G_p is a p-Sylow subgroup of G.

Proof (?).
There's a map

$$\left(H^1(G; M) \xrightarrow{\text{res}} H^1(G_p; M|_{G_p}) \xrightarrow{\text{coRes}} H^1(G; M)\right) = \text{mult}_d, d \coloneqq [G : G_p].$$

Since d is prime to p, res is injective on p-power torsion, making $H^1(G; M)$ torsionfree. Then since G is finite, $H^i(G; M)$ is torsion, and the only torsion torsionfree group is zero.

■

Remark 12.2.3: There will be multiple steps:

- It's enough to prove this for $\mathsf{Gal}(L_{/k})$ a p-group, using theorem on applications of Sylow. We know enough about the structure of p-groups to make induction arguments!
- It's enough to show that $H^i(L_{/k}; C_L) = 0$ for $L_{/k}$ cyclic. Letting $L_{/k}$ be Galois with $G \coloneqq H^i(L_{/k})$ a p-group, then let $H \leq G$ be a nontrivial normal cyclic subgroup. Then the inflation-restriction exact sequence yields

  $$0 \to H^1(G/H; C_L^H) \to H^1(G; C_L) \to H^1(H; C_L),$$

  using idele class groups and writing C_L^H for the class group of the fixed field by H, and recalling that this comes from the Hochschild-Serre spectral sequence. By induction on the size of G, we'll know the right-hand side is 0, and the left-hand side is 0 by induction on $\#G$. However, note that we have to show this for *all* cyclic extensions!
- Prove the following theorem;

Remark 12.2.4: Note that C_L will not even be finitely generated!

Theorem 12.2.5 ***(?).***
If $L_{/k}$ is cyclic, then $H^1(L_{/k}; C_L) = 0$, and $\#H^2(L_{/k}; C_L) = [L : k]$.

⚠ **Warning 12.2.6**
Note that $\#H^1 = 1$ in this case!

Definition 12.2.7 (Herbrand Quotient)
If G is finite cyclic and $M \in \mathsf{G\text{-}Mod}$, define the **Herbrand quotient** as

$$q(M) \coloneqq \frac{\#H^2(G; M)}{\#H^1(G; M)},$$

whenever this ratio is defined.

Remark 12.2.8: Taking logs makes this look like an Euler characteristic.

Lemma 12.2.9 ***(Herbrand quotients are multiplicative).***
Suppose $0 \to A \to B \to C \to 0$ is a SES of G-modules for G cyclic. Then

$$q(A)q(C) = q(B).$$

Exercise 12.2.10 (A fun one)
Prove this! It's the same proof that $\chi(A) + \chi(C) = \chi(B)$.

Lemma 12.2.11 ***(?).***
If M is finite, then $q(M) = 1$, so this invariant for infinite modules.

Proof (?).
We first claim that $\#M^G = \#M_G$, recalling that $M_G = M/\langle g-1\rangle = M/IM$ for I the augmentation ideal. Note that in finite groups, for a SES $0 \to A \to B \to C \to 0$ yields $\#B = (\#A)\cdot(\#C)$, or equivalently $(\#A)\cdot(\#B)^{-1}\cdot(\#C) = 1$ and this extends to longer exact sequences.
Now use the exact sequence

$$0 \to M^G \to M \xrightarrow{g-1} M \to M_G \to 0,$$

and so

$$(\#M^G)\cdot(\#M)^{-1}\cdot(\#M)\cdot(\#M_G)^{-1} = 1.$$

Now to show that the sizes are equal, Recall that

$$H^*(G;M) = H^*\left(M \xrightarrow{g-1} M \xrightarrow{\sum g^i} M \to \cdots\right).$$

Thus we get

$$0 \to H^1(G;M) \to \operatorname{coker}(M \xrightarrow{g-1} M) \xrightarrow{\sum g^i} \ker(M \xrightarrow{g-1} M) \twoheadrightarrow H^2(G;M) \to 0$$
$$\implies 0 \to H^1(G;M) \to M_G \xrightarrow{\sum g^i} M^G \twoheadrightarrow H^2(G;M) \to 0,$$

so

$$\#H^1(G;M)\cdot(\#M_G)^{-1}\cdot(\#M^G)\cdot(\#H^2(G;M))^{-1} = 1 = q(M)^{-1}.$$

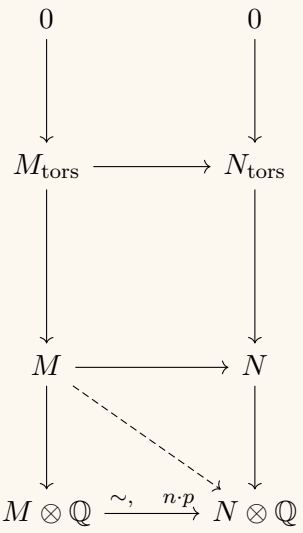
■

Lemma 12.2.12 ***(?).***
If M, N are finitely generated in $\mathsf{G\text{-}Mod}$ and $M \otimes \mathbb{R} \cong N \otimes \mathbb{R} \in \mathsf{G\text{-}Mod}$, then $q(M) = q(N)$.

Remark 12.2.13: Analogy: Reidemeister torsion! Tensoring up to $\mathbb{R}$ somehow doesn't lose all torsion information.

Proof (of lemma).
We'll first show $M \otimes \mathbb{Q} \xrightarrow{\sim} N \otimes \mathbb{Q}$ implies $q(M) = q(N)$.

Claim: There is a map $M/\text{tors} \to N/\text{tors}$ with finite kernel and cokernel.



$$0 \longrightarrow M_{\text{tors}} \longrightarrow M \longrightarrow N/N_{\text{tors}} \longrightarrow \text{torsion!} \longrightarrow 0$$

Link to Diagram

Claim:

$$M \otimes \mathbb{R} \cong N \otimes \mathbb{R} \iff M \otimes \mathbb{Q} \cong N \otimes \mathbb{Q}.$$

Exercise ***(?)***
Prove this!

■

13 | Tuesday, September 28

See fppf cohomology. Note: statements of the form $A \otimes C \cong B \otimes C \implies A \cong B$ aren't quite descent! There's no descent data or e.g. Galois equivariance, and the downstairs maps may not be related to the original map at all.

Theorem 13.0.1 ***(?).***
For $L_{/k}$ cyclic of degree n,

$$q(C_L) = n.$$

Remark 13.0.2: Recall that q is multiplicative in exact sequences, equals 1 for finite G-modules,

and if $M \otimes R \cong N \otimes R$ then $q(M) = q(N)$.

Proof (of 3rd property).
It's enough to show this for M, N torsionfree, since $q(M) = q(M/M_{\text{tors}})$. The claim is that for R sufficiently divisible, letting $M \otimes \mathbb{Q} \xrightarrow{\varphi} N \otimes \mathbb{Q}$, $\varphi|_M$ factors through N with torsion kernel. Use that $M \otimes \mathbb{R} \xrightarrow{\sim} N \otimes \mathbb{R}$ implies $M \otimes \mathbb{Q} \xrightarrow{\sim} N \otimes \mathbb{Q}$ Now we claim that if $G \in \mathsf{Grp}$ and $V_1, V_2 \in \mathsf{G\text{-}Mod}$ over a field k and $L_{/k}$ is any extension, then $V_1 \otimes L \xrightarrow{\sim} V_2 \otimes L$ implies $V_1 \xrightarrow{\sim} V_2$. ■

Proof (of claim).
1: Use that Hom commutes with tensor products in the following way:

$$\operatorname*{Hom}_G(V_1 \otimes L, V_2 \otimes L) = \operatorname*{Hom}_G(V_1, V_2) \otimes L.$$

We can write the LHS as $({V_1}^\vee \otimes V_2 \otimes_k L)^G$, and the right-hand side as $({V_1}^\vee \otimes V_2)^G \otimes_k L$. It's enough to show that for any G-representation V, since $V^G \otimes L \cong (V \otimes L)^G$ where $V^G \coloneqq \ker(V^{\oplus q} \xrightarrow{q} \bigoplus_{g \in G} V)$. But now we're done since $L_{/k}$ is flat.
2: If both V_i are irreducible over L, this follows from Schur. For V_i irreducible over k an infinite field, then being an isomorphism is a Zariski open condition, and any Zariski open subset of $\mathbb{A}^n_{/k}$ has infinitely many rational points. ■

Theorem 13.0.3 ***(?).***
If $L_{/k}$ is cyclic and S is a set of primes of K including all infinite primes, all primes that ramify, and all primues under a set of generators of the class group of L, letting T be the set of primes of L over S, we have

- $q(\mathbb{I}_{L,T}) = \prod_{v \in S} [L_{\widehat{v}} : k_{\widehat{v}}]$
- $[L : k] q(\mathcal{O}^\times_{L,T}) = \prod_v [L_{\widehat{v}} : k_{\widehat{v}}]$
- $q(C_L) = [L : k]$

Proof (1 and 2 imply 3).
There is a SES

$$0 \to \mathcal{O}^\times_{L,T} \to \mathbb{I}_{L,T} \to C_L \to 1,$$

where $\mathcal{O}^\times_{L,T}$ allows denominators in T. Then using (1) and (2),

$$q(C_L) = q(\mathbb{I}_{L,T}) / q(\mathcal{O}^\times_{L,T}) = [L : k].$$

■

Proof (of 1).

Write $\mathbb{I}_{L,T} = \prod_{v\in T} L_{\widehat{v}}^\times \times \prod_{v\notin T} \mathcal{O}_{L_{\widehat{v}}}^\times$, so

$$\begin{aligned} q(\mathbb{I}_{L,T}) &= \prod_{v\in S} q\Big(\prod_{w\in \mathrm{Pl}(/L)} L_w^\times\Big) \\ &= \prod_{v\in S} \frac{\#H^2(L_{\widehat{v}/k_{\widehat{v}}}; L_{\widehat{v}}^\times)}{\#H^2(L_{\widehat{v}/k_{\widehat{v}}}; L_{\widehat{v}}^\times)} \\ &= \prod_{v\in S} \#\operatorname{Br}(L_{\widehat{v}/k_{\widehat{v}}}) \\ &= \prod_{v\in S} [L_{\widehat{v}} : k_{\widehat{v}}]. \end{aligned}$$

■

Proof (of 2).
Write $L_1 \coloneqq \underset{\mathsf{Set}}{\mathrm{Hom}}(T, \mathbb{Z})$ and

$$L_2 \coloneqq m(\lambda : \mathcal{O}_{L,T}^\times \to L_1 \otimes \mathbb{R})\alpha \qquad \mapsto (\log |\alpha|_w)_{w\in T}.$$

Dirichlet's unit theorem implies $L_2 \hookrightarrow L_1^0 \otimes \mathbb{R} \coloneqq \left\{\mathbf{x} \;\middle|\; \sum x_i = 0\right\}$ is a lattice. We can write

$$\begin{aligned} L_1 &= \bigoplus_{v\in S} \bigoplus_{w_{/v}} \mathbb{Z} \\ &= \bigoplus_{v\in S} \operatorname*{Ind}_{\mathsf{Gal}(L_{\widehat{v}/k_{\widehat{v}}})}^{\mathsf{Gal}(L_{/k})} \mathbb{Z}, \end{aligned}$$

Thus

$$\begin{aligned} q(L_1) &= \prod_{v\in S} q\left(\operatorname*{Ind}_{\mathsf{Gal}(L_{\widehat{v}/k_{\widehat{v}}})}^{\mathsf{Gal}(L_{/k})} \mathbb{Z}\right) \\ &= \prod_{v\in S} q(L_{\widehat{v}/k_{\widehat{v}}}, \mathbb{Z}) \\ &= \prod_{v\in S} [L_{\widehat{v}} : k_{\widehat{v}}]. \end{aligned}$$

To compute the other side, use that there is a SES $0 \to L_1^0 \to L_1 \xrightarrow{\Sigma} \mathbb{Z} \to 0$. So

$$q(L_1^0) = q(L_1)/q(L_{/k}; \mathbb{Z}) = \frac{\prod [L_{\widehat{v}} : k_{\widehat{v}}]}{[L : k]}.$$

Now note $q(L_k) = q(\mathcal{O}_{L,T}^\times)$ and there is a SES

$$0 \to \mu(L) \to \mathcal{O}_{L,T}^\times \to L_k \to 0 \implies q(\mathcal{O}_{L,T}^\times) = q(L_k),$$

where $\mu(L)$ are the roots of unity in L, which form a finite group. Then

$$q(\mathcal{O}_{L,T}^\times) = q(L_1^0) = \frac{\prod [L_{\widehat{v}} : k_{\widehat{v}}]}{[L : k]}.$$

■

Fact 13.0.4 (from class field theory)

$$\#\left(\frac{\mathbb{I}_K}{k^\times \operatorname{Nm}_{L/k} \mathbb{I}_L}\right) = [L:k].$$

How to prove: reduce to Kummer extensions, adjoin pth roots of unity, etc.

Remark 13.0.5: This fact implies $H^1(L/k; C_L) = 1$. The proof is that $\#\left(H^2/H^1\right) = [L:k]$, which implies $\#H^1 = 1$.

Theorem 13.0.6 ***(?).***
Severi-Brauer varieties over k satisfy the Hasse principle, i.e. the following sequence is exact:

$$0 \to \operatorname{Br}(k) \to \bigoplus_{v \in \operatorname{Pl}(k)} \operatorname{Br}(k_{\widehat{v}}).$$

13.1 Proof

Theorem 13.1.1 ***(Hasse-Minkowski).***
Let q be a quadratic form over a number field k, then the projective quadric $X \coloneqq \{q = 0\} \subseteq \mathbb{P}^n_{/k}$ satisfies the Hasse principle: X has rational points over k iff X has rational points over $k_{\widehat{v}}$ for all $v \in \operatorname{Pl}(k)$.

Definition 13.1.2 (Quadratic forms representing elements)
Given q a quadratic form over k a field (e.g. a number field or a local field), then for $a \in k$, we say q **represents** a if there exist elements $\mathbf{x} \in k^n \setminus \{0\}$ such that $q(\mathbf{x}) = 0$.

Theorem 13.1.3 ***(a stronger one).***
Given $a \in k$, q represents a iff over k iff q represents a over $k_{\widehat{v}}$ for all $v \in \operatorname{Pl}(k)$. Moreover, rational points are Zariski dense on $q(x) = a$.

Remark 13.1.4: That this implies the first theorem is easy, setting $a = 0$. Conversely, consider $q'(\mathbf{x}, z) \coloneqq q(\mathbf{x}) - az^2$. Then q represents a iff q' represents 0 – however, this can go wrong if $z = 0$! Exercise: find a good proof.

Proof (?).
Let n be the number of variables.

- For $n = 1$, we saw that $x^2 = a$ satisfies the Hasse principle in the first class. Moreover rational points are Zariski dense on the projective variety $x^2 = ay^2$.
- For $n = 2$, consider $q(x_1, x_2) = a$. We'll pick this up next time!

■

14 | Tuesday, October 05

Remark 14.0.1: Goal: prove the Hasse-Minkowski theorem. We looked at $n \leq 3$, so today we'll look at $n = 4$.

Theorem 14.0.2 *(?).*
Let $Q \subseteq \mathbb{P}^3_{/k}$ be a smooth quadric, then

$$Q(k) \neq \emptyset \iff Q(k_{\widehat{v}}) \neq \emptyset$$

for all places $v \in \mathrm{Pl}\,(k)$.

Proof ($n = 4$ case).
Let $X \subseteq \mathrm{Gr}_1(\mathbb{P}^3)$ be the variety of lines in Q, and consider $\mathcal{I} \to X$ the universal family. Then $X_{\bar{k}} = \mathbb{P}^1 \cup \mathbb{P}^1$ since $Q_{\bar{k}} = \mathbb{P}^1 \times \mathbb{P}^1 \xhookrightarrow{\mathcal{O}(1,1)} \mathbb{P}^3$. Consider the case when X is not connected. Then

- $\mathcal{U}_c \to Q$ is an isomorphism, which can be checked over $\bar{k}$.
- $Q(k_{\widehat{v}}) \neq \emptyset$ implies $\mathcal{U}_c(k_{\widehat{v}}) \neq \emptyset$ and thus $C(k_{\widehat{v}}) \neq \emptyset$ for all v.
- By the Hasse principle for Severi-Brauers, if $C = \mathbb{P}^1$ implies $C(k) \neq \emptyset$.
- Then $\mathcal{U}_c \to C$ is Zariski trivial, so $\mathcal{U}_c \cong Q$ has rational points.

$$\begin{array}{ccccc} \mathcal{U}_c & \longrightarrow & \mathcal{U} & \longrightarrow & Q \\ \downarrow & & \downarrow & & \\ C & \hookrightarrow & X & & \end{array}$$

Link to Diagram

Now consider the case when X is connected. The claim is that there exists a quadratic extensions k'/k where $X_{k'}$ is not connected:

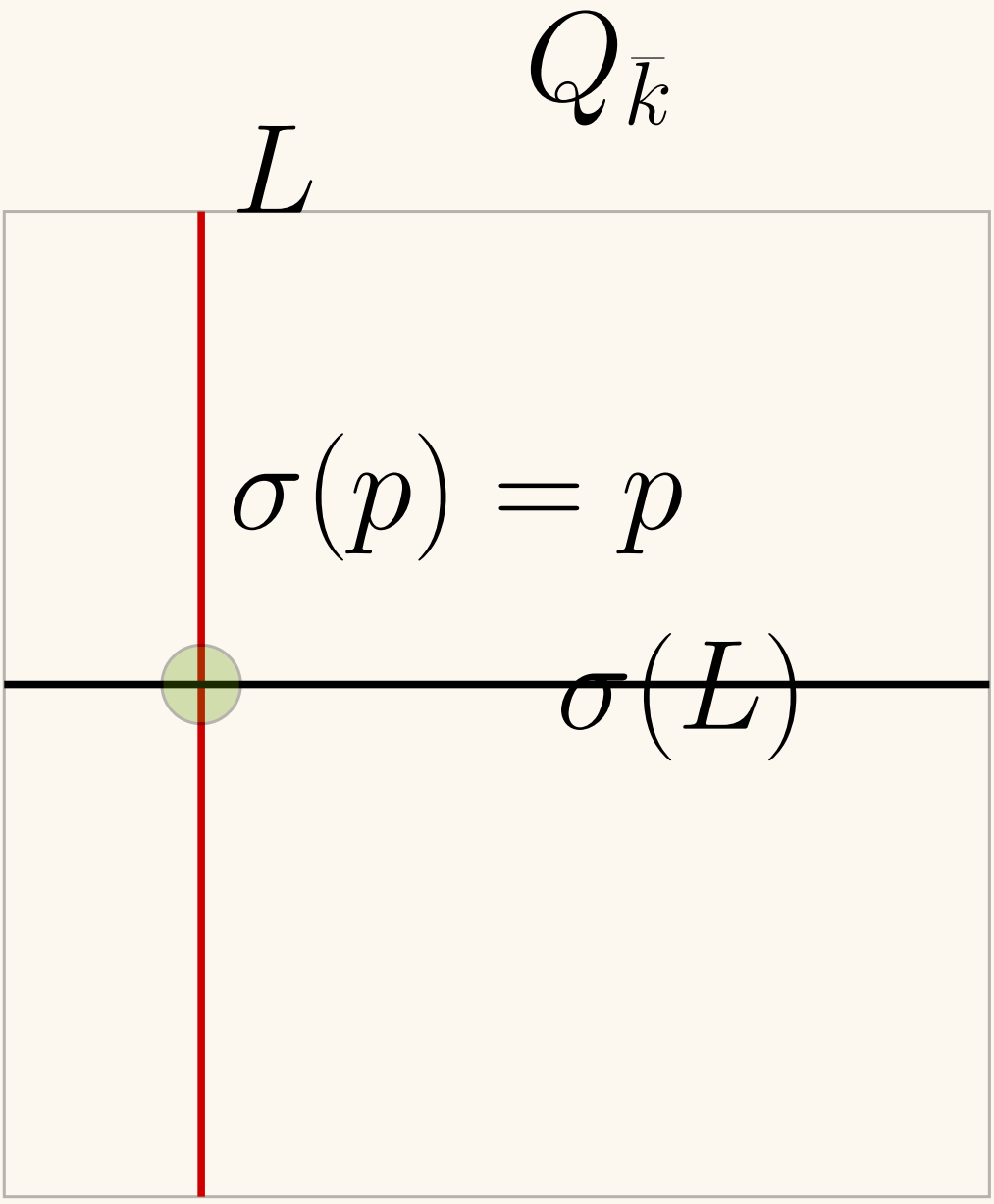
- $k' = \Gamma\left(X; \mathcal{O}_X\right)$, which is a rank 2 vector bundle (which can be checked over $\bar{k}$). So

  $$\Gamma\left(X_{k'}; \mathcal{O}_{X_{k'}}\right) = \Gamma\left(X; \mathcal{O}_X\right)_{k'} = k' \otimes_k k' \cong k' \oplus k',$$

  so $X_{k'}$ is disconnected.
- We can take $[Q] \in H^1(k; \mathrm{O}_n) \xrightarrow{\det} H^1(k; \mu_2)$, and it maps to $[k']$.
- $\mathsf{Gal}(\bar{k}_{/k})$ acts on $\mathrm{Pic}(Q) \cong \mathbb{Z}^{\times^2}$, and this action factors through $\{\pm 1\}$. Here $\mathrm{O}_n = \mathrm{Aut}(\sum x_i^2)$.
  - Why: this action preserves the *effective cone* in $\mathrm{Pic}(Q_{\bar{k}})$ spanned by $\pi_1^*\mathcal{O}(1)$ and $\pi_2^*\mathcal{O}(1)$, which are those bundles with global sections (which is preserved by Galois).

⚠ Warning 14.0.3
Even if $[L] \in \mathrm{Pic}Q$ is Galois-invariant, this does not imply that L is defined over k! This can be a common source of errors.

By case 1, $X(k') \neq \emptyset$, so there exists a rational line $L \subseteq Q$ contained in one connected component of $X_{k'}$. There is an action $\mathsf{Gal}(k'_{/k}) \curvearrowright L$, so take $\sigma \in \mathsf{Gal}(k'_{/k})$. Then $\sigma(L)$ is in the other component $X_{k'}$, since Galois interchanges its components pointwise. Then considering the two rulings of the quadric yields the following picture, where they intersect at a point:



But then $\sigma(p) = p$ is Galois fixed, and is thus a k-rational point.

■

Theorem 14.0.4 *(?).*
Let $n \geq 5$ and $Q = \sum_{l \leq i \leq n} a_i x_i^2$ be a nondegenerate quadratic form over a number field k. Then

Q satisfies the Hasse principle.

Proof (General case).
We'll proceed by induction on $n \geq 5$. Write $Q = a_1x_1^2 + a_2x_2^2 + G(x_3, \cdots, x_n)$.

Claim: G represents $k_{\widehat{v}}$ for almost all $v \in \mathrm{Pl}\,(k)$.
It's enough to show that $G'(x_3, \cdots, x_{n+1}) \coloneqq G(x_3, \cdots, x_n) + ax_{n+1}^2$ represents 0 for all $a \in k_{\widehat{v}}$ and almost all v. Without loss of generality, we can assume G is nondegenerate over the residue field $\kappa(v)$, by throwing out finitely many things. Then G' has rank at least $n-2$ over $\kappa(v)$ for almost all v.

Claim: G' has a smooth rational point for for all
Using the Lang-Weil estimates (using absolute irreducibility), $G'(\kappa(v))$ has about $(\#\kappa(v))^{n-3}$ rational points, where the error term is uniform in v. The singular locus is a dimension smaller, so about $(\#\kappa(v))^{n-4}$, and for n large enough for this to hold, the former is larger.
Now use Hensel's lemma, any smooth rational point on the special fiber lifts to the generic fiber (i.e. the infinitesimal smoothness criteria). This proves the first claim that G represents $k_{\widehat{v}}$ for almost all v.
Fact
For almost all v, $G(x_3, \cdots, x_n)$ represents *every* element of k.

Let $U \subseteq (\prod k_{\widehat{v}})^{\times^{n-2}} k[v]$ be the set $\{(x_3, v), \cdots, (x_n, v)\}$ such that there exists an $(x_1, v), (x_2, v)$ with $Q(x_1, \cdots, x_n) = 0$. Some claims:

- U is open, which follows from the fact above,
- U is nonempty since Q represents 0 locally by hypothesis,
- The set $U' \subseteq (\prod k_{\widehat{v}})^{\times^2}$ of pairs $(x_1, v), (x_2, v)$ such that there exist $(x_3, v), \cdots, (x_n, v)$ with $Q(x_1, \cdots, x_n) = 0$ is also open.

Then by weak approximation, there exist $x_1, x_2 \in k$ such that $(x_1, x_2) \in U$. So write $c = a_1x_1^2 + a_2x_2^2 \in k$ and define $Q'(z, x_3, \cdots, x_n) = -cz^2 + G(x_3, \cdots, x_n)$. This is a quadratic form in $n-1$ variables that represents 0 locally. Now by induction, Q' represents zero globally.
■

15 | Tuesday, October 12

Reference: FGA Explained.

Proposition 15.0.1 *(?).*
For R a complete local ring with residue field κ, there is an isomorphism $\mathrm{Br}(R) \xrightarrow{\sim} \mathrm{Br}(\kappa)$.

Remark 15.0.2: We'll prove a stronger claim that there is a bijection $\mathsf{SBSch}_{/R}/\sim \to \mathsf{SBSch}_{/k}/\sim$, which requires some deformation theory. A summary of obstruction theory for schemes:

Let $A \in \mathsf{CRing}$, $I \trianglelefteq A$ is square zero ideal, and $X_{/A/I}$ a smooth scheme. Then there exists a functorial class $\mathrm{obs}(X) \in H^2(X; \mathbf{T}_X \otimes_{A/I} I)$ such that X admits a flat lift to A iff $\mathrm{obs}(X) = 0$. If the obstruction vanishes, the set of lifts is a torsor for H^1, and the automorphisms of the lift are given by H^0. Here $\mathbf{T}_X$ is the tangent sheaf, and a *flat lift* is a flat scheme $\tilde{X}_{/A}$ equipped with an isomorphism $\tilde{X} \otimes (A/I) \xrightarrow{\sim} X$.

A word on this deformation-theoretic result is proved:

- Show affine schemes lift, e.g. using Cohen structure theorem. Alternatively, something about being étale?
- Try to glue, which may not satisfy the cocycle condition – failure to glue will show up in this cohomology. Why the tangent sheaf: the difference between two gluing data is a derivation.

Note that for vector bundles $E \to X$, the cohomology would be in $\mathrm{End}(E)$.

See also tangent/cotangent complex.

Proof (?).
We'll try to lift a Severi-Brauer over k to one over R. Claim: letting $R_n \coloneqq R/\mathfrak{m}^n$, given a lift to R_n, there exists a unique lift to $S_n \coloneqq R_{n+1}$. We have

$$\mathrm{obs}(S_n) \in H^2(S^n; \mathbf{T}_{S_n} \otimes \mathfrak{m}^n/\mathfrak{m}^{n+1}) = H^2(S_n; \mathbf{T}_{S_n}) \otimes_k \mathfrak{m}^n/\mathfrak{m}^{n+1},$$

which follows from base change in cohomology using $\mathbf{T}_{S_n} \otimes_{R_n} k \otimes_k \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Here $\mathrm{obs}(S_n) = 0$, since

$$H^2(S; \mathbf{T}_S) \otimes_k \bar{k} = H^2(S_{\bar{k}}; \mathbf{T}_{S,\bar{k}}) = H^2(\mathbb{P}^n_{/\bar{k}}; \mathbf{T}_{\mathbb{P}^n_{/k}}) = 0.$$

See Hartshorne, this uses the Euler exact sequence.
So a lift exists for each R_n.
This lift is unique since lifts are torsors for $H^1(S_n; \mathbf{T}_{S_n} \otimes \mathfrak{m}^n/\mathfrak{m}^{n+1})$.
Why this lifts to R: formal GAGA, which gives a way of going from formal schemes to actual schemes. See "FGA Explained", Ch. 8. This is because giving a scheme over R^n for all n amounts to giving a formal scheme, since the underlying topological spaces are the same. The input is an ample line bundle: here for $\mathbb{P}^n$ we can take the dual of the dualizing sheaf ${\mathcal{O}_{S_n}}^\vee$. ∎

Remark 15.0.3: Formal GAGA: one of the most useful techniques!

Proposition 15.0.4*(?).*
Suppose $X \in \mathsf{Var}_{/k}$ and let $A \in \mathrm{Br}(X)$ (e.g. represented by an Azumaya algebra), then

- If k is a p-adic field, then there is a map

$$\begin{aligned} X(k) &\to \mathrm{Br}(X) \\ x &\mapsto x^*(A). \end{aligned}$$

- For $k = \mathbb{R}$, the map $X(\mathbb{R}) \to \mathrm{Br}(k) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is locally constant, i.e. constant on connected components.

Proof (?).
For $x \in X(k)$, $\widehat{\mathcal{O}_{X,x}}$ is a complete local k-algebra with residue field k. Then for $A \in \mathrm{Br}(X)$, we have a map $\psi : A|_{\widehat{\mathcal{O}_{X,x}}} \xrightarrow{\sim} (A_x) \otimes_k \widehat{\mathcal{O}_{X,x}}$. We want to spread ψ out to a p-adic neighborhood of x. In the analytic setting, this can be done using **Artin approximation**, which will imply there exists an étale neighborhood U of x and a map

$$\begin{aligned} U &\to X \\ y &\mapsto x, \end{aligned}$$

which extends (?) and induces an isomorphism on complete local rings. Now applying the implicit function theorem, there exists a p-adic neighborhood of x in any $U(k)$.

■

Corollary 15.0.5 *(?).*
Let $X_{/k}$ for k a number field and $A \in \mathrm{Br}(X)$. Then

a. The following map on adeles is locally constant:

$$\begin{aligned} A^* : X(\mathbb{A}_k) &\to \mathbb{Q}/\mathbb{Z} \\ x &\mapsto \sum_{v \in \mathrm{Pl}(k)} m_{v_x}(x^* A). \end{aligned}$$

b. $X(\mathbb{A})^{\mathbb{A}} := (A^*)^{-1}(0)$ is closed and open.

c. $X(\mathbb{A})^{\mathrm{Br}} = \bigcap_{A \in \mathrm{Br}(X)} X(\mathbb{A})^{\mathbb{A}}$ is closed.

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

e. If X is proper, then $X(\mathbb{A})^{\mathrm{Br}} \neq X(\mathbb{A})$ and weak approximation does not hold.

Proof (?).

a. Use the same Lang-Weil argument used previously, and that this is a sum of locally constant maps.
b. 0 is closed and open in $\mathbb{Q}/\mathbb{Z}$ and A^* is continuous.
c. This is an intersection of closed sets.
d. We already know $X(k)$ is contained in the RHS, and by (c) we know it's closed, so the RHS contains its closure.
e. Immediate from (d).

■

⚠ **Warning 15.0.6**
The adelic topology is not the product topology.

Definition 15.0.7 (Symbol Algebra)
For $k \in \mathsf{Field}$ and let $\chi : \mathsf{Gal}(\bar{k}_{/k}) \to C_n$ and $a \in k^\times/(k^\times)^n$, then recall that $(\chi, a) \coloneqq L_\chi \langle x \rangle_\sigma / \langle x^n - a \rangle$ where L_χ is the fixed field of χ and $L_\chi \langle x \rangle_\sigma$ is the twisted polynomial ring where $\ell x = x\sigma(\ell)$.

Example 15.0.8 ***(?):*** Take a smooth proper model of $U = \left\{ y^2 + z^2 = (3 - x^2)(x^2 - 2) \right\}$ and the *symbol algebra* $A = (3 - x^2, -1)$.

Exercise 15.0.9 ***(Homework)***
Check that this has points locally!

Our goal is to show that $X(\mathbb{A})^A = \emptyset$. By Kummer theory, choosing an isomorphism $\mu_n(k) \to C_n$ induces a bijection

$$\begin{aligned} k^\times/(k^\times)^n &\xrightarrow{\sim} \left\{ \chi : \mathsf{Gal}(\bar{k}_{/k}) \to C_n \right\} \\ a &\mapsto k[x]/\langle x^n - a \rangle . \end{aligned}$$

For $n = 2$ and $\operatorname{ch} k \neq 2$, there is a canonical isomorphism $\{\pm 1\} \xrightarrow{\sim} \mu_2(k) \xrightarrow{\sim} C_2$. View $(\chi, a) \in H^2(k, \mu_n)$, and there is a cup product

$$\begin{aligned} H^1(k; C_n) \times H^1(k; \mu_n) &\to H^2(l; \mu_n) \\ \chi &\mapsto [\chi] \smile [a]. \end{aligned}$$

Another point of view: if $L_{/k}$ is Galois with Galois group C_n, it comes with a choice of generator σ and thus a canonical element in $[\sigma] \in H^2(L_{/k}; \mathbb{Z}) \xrightarrow{\sim} C_n$. Then there is another cup product

$$k^\times = H^0(L_{/k}; L^\times) \xrightarrow{(-)\smile[\sigma]} H^2(L_{/k}; L^\times) = \operatorname{Br}(L_{/k}) = k^\times / \operatorname{Nm}_{L_{/k}} k^\times,$$

in which case $(\chi, a) = a \smile [\sigma]$.

Corollary 15.0.10 ***(?).***
$(\chi, a) = 0 \iff a \in \operatorname{Nm}_{L_{/k}} L^\times$.

Remark 15.0.11: For $n = 2$, one has $(a, b) = k\left[\sqrt{b}\right] \langle x \rangle_\sigma / \langle x^n - a \rangle$, and this splits iff a is a norm from $k(\sqrt{b})$ when this is a field.

Exercise 15.0.12 (?)
What are the equations for the Severi-Brauer arising from (a, b).

ToDos

List of Todos

Something about using $\mathcal{O}(1)$ to give an embedding into $\mathbb{P}^1$. Start with $\mathcal{O}(-1)$, dualize, project? 6

Something about Hilbert 90 23

Check 2! 36

Definitions

3.2.1 Definition – Brauer Groups . . . 10
3.2.4 Definition – Group cohomology . . . 10
4.2.4 Definition – Galois cohomology . . . 13
4.2.5 Definition – Brauer Groups . . . 13
5.0.5 Definition – Reduced Complex . . . 15
5.2.1 Definition – Forms/descent, a pseudo-definition . . . 17
6.2.1 Definition – Torsor . . . 20
6.4.5 Definition – Brauer group . . . 22
7.1.4 Definition – Severi-Brauers . . . 23
7.1.6 Definition – CSAs/Azumaya Algebras . . . 24
7.1.8 Definition – Opposite algebra . . . 24
7.1.9 Definition – Morita equivalence . . . 24
7.2.2 Definition – Twisted vector spaces . . . 25
7.2.8 Definition – Index and period . . . 27
8.0.8 Definition – Reduced norm and trace . . . 30
8.0.11 Definition – Semilinear group rings . . . 30
9.1.10 Definition – ? . . . 35
10.2.4 Definition – Valuations on division algebras . . . 39
10.2.5 Definition – Valuation ring . . . 40
11.1.2 Definition – Cyclic Algebra . . . 42
11.2.3 Definition – Ideles . . . 44
11.2.5 Definition – S-ideles . . . 45
12.2.7 Definition – Herbrand Quotient . . . 48
13.1.2 Definition – Quadratic forms representing elements . . . 53
15.0.7 Definition – Symbol Algebra . . . 59

Theorems

2.1.10 Theorem – ? . . . 6
3.0.2 Theorem – Lang-Weil Estimates . . . 7
4.1.5 Proposition – ? . . . 12
5.0.2 Proposition – ? . . . 15
5.1.1 Proposition – Spectral Sequences . . . 16
5.1.3 Proposition – Inflation/Restriction Exact Sequence . . . 16
5.2.6 Proposition – ? . . . 17
6.1.2 Theorem – A meta-theorem . . . 19
6.2.2 Theorem – ? . . . 20
6.3.2 Theorem – ? . . . 20
6.4.7 Theorem – ? . . . 23
7.1.7 Theorem – Classification of CSAs . . . 24
7.1.10 Theorem – ? . . . 24
7.2.5 Proposition – Properties of categories of twisted vector spaces . . . 26
7.2.6 Proposition – ? . . . 26
7.2.7 Theorem – ? . . . 26
8.0.2 Theorem – ? . . . 28
8.0.3 Theorem – ? . . . 28
8.0.9 Proposition – ? . . . 30
8.0.10 Theorem – ? . . . 30
8.1.2 Theorem – ? . . . 31
8.1.5 Theorem – Tsem . . . 31
9.0.2 Theorem – Hasse principle for Severi Brauers . . . 32
9.1.7 Theorem – ? . . . 34
10.1.2 Proposition – ? . . . 37
10.1.3 Theorem – ? . . . 37
10.1.5 Theorem – Hasse . . . 39
11.1.5 Theorem – ? . . . 43
11.2.2 Proposition – ? . . . 44
11.2.8 Proposition – ? . . . 45
11.2.9 Theorem – ? . . . 45
12.2.1 Theorem – Injectivity . . . 47
12.2.2 Theorem – Actual IRL application of Sylow theorems . . . 48
12.2.5 Theorem – ? . . . 48
13.0.1 Theorem – ? . . . 50
13.0.3 Theorem – ? . . . 51
13.0.6 Theorem – ? . . . 53
13.1.1 Theorem – Hasse-Minkowski . . . 53
13.1.3 Theorem – a stronger one . . . 53
14.0.2 Theorem – ? . . . 54
14.0.4 Theorem – ? . . . 55

15.0.1 Proposition – ? 56
15.0.4 Proposition – ? 57

Exercises

3.2.3 Exercise – ? . . . 10
4.2.7 Exercise – ? . . . 14
5.2.7 Exercise – ? . . . 18
6.1.3 Exercise – ? . . . 19
6.2.3 Exercise – ? . . . 20
10.2.10 Exercise – ? . . . 40
11.1.9 Exercise – ? . . . 44
11.2.10 Exercise – ? . . . 46
12.2.10 Exercise – A fun one . . . 49
12.2.14 Exercise – ? . . . 50
15.0.9 Exercise – Homework . . . 59
15.0.12 Exercise – ? . . . 59

Figures

List of Figures