

*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](mailto:dzackgarza@gmail.com)

*Last updated: 2021-12-02*

# Table of Contents

## Contents

<b>Table of Contents</b>	<b>2</b>
<b>1 Preface</b>	<b>5</b>
<b>2 Thursday, August 19</b>	<b>5</b>
2.1 Examples of Hasse Principles . . . . .	6
<b>3 Tuesday, August 24</b>	<b>8</b>
3.1 Brauer Groups . . . . .	9
3.1.1 The Brauer-Manin Obstruction . . . . .	10
3.1.2 The Hasse Principle for Severi-Brauers . . . . .	11
3.2 Brauer Groups and Galois Cohomology . . . . .	11
<b>4 Group Cohomology (Thursday, August 26)</b>	<b>12</b>
4.1 Computing Examples . . . . .	12
4.2 Functoriality . . . . .	13
<b>5 Tuesday, August 31</b>	<b>15</b>
5.1 Some Formal Properties . . . . .	17
5.2 Forms, Torsors, and $H^1$ . . . . .	18
<b>6 Thursday, September 02</b>	<b>19</b>
6.1 Correspondence of Forms . . . . .	19
6.2 Torsors . . . . .	21
6.3 Example: Kummer Theory . . . . .	21
6.4 Geometry of Brauer Groups . . . . .	22
<b>7 Tuesday, September 07</b>	<b>24</b>
7.1 Intro: Historical POV on Brauer Groups . . . . .	24
7.2 The Boundary Map and Twisted Vector Space . . . . .	25
<b>8 Thursday, September 09</b>	<b>28</b>
8.1 Computing Brauer Groups . . . . .	32
<b>9 Tuesday, September 14</b>	<b>33</b>
9.1 Cyclic Algebras . . . . .	33
<b>10 Thursday, September 16</b>	<b>37</b>
10.1 Computing Brauer Groups . . . . .	37
10.2 Proof of theorem . . . . .	40
<b>11 Tuesday, September 21</b>	<b>43</b>
11.1 Construction of Brauer classes over $K$ . . . . .	43

11.2 The SES . . . . .	45
<b>12 Thursday, September 23</b>	<b>47</b>
12.1 Proof of Theorem . . . . .	47
12.2 Injectivity . . . . .	48
<b>13 Tuesday, September 28</b>	<b>51</b>
13.1 Proof . . . . .	54
<b>14 Tuesday, October 05</b>	<b>55</b>
<b>15 Tuesday, October 12</b>	<b>57</b>
<b>16 Tuesday, October 19</b>	<b>61</b>
16.1 Descent Obstruction . . . . .	62
<b>17 Descent (Tuesday, October 26)</b>	<b>64</b>
17.1 Selmer Sets . . . . .	66
<b>18 Thursday, October 28</b>	<b>66</b>
18.1 Proof of finiteness of Selmer Sets . . . . .	67
<b>19 Tuesday, November 02</b>	<b>69</b>
19.1 Proof . . . . .	70
19.1.1 Proof of a . . . . .	70
19.1.2 Proof of b . . . . .	71
19.2 Misc . . . . .	72
<b>20 Tuesday, November 09</b>	<b>72</b>
20.1 Proof . . . . .	72
20.2 Showing $X(\mathbb{A})^{\text{ét}, \text{Br}}$ . . . . .	74
20.3 Étale-Brauer-Manin Set . . . . .	75
<b>21 Chabauty-Coleman (Thursday, November 11)</b>	<b>76</b>
21.1 Proofs . . . . .	77
<b>22 The Mordell Conjecture (Tuesday, November 23)</b>	<b>78</b>
<b>23 Tuesday, November 30</b>	<b>82</b>
23.1 Faltings Theorem . . . . .	82
23.1.1 Proof . . . . .	82
23.2 The Kodaira-Parshin Trick . . . . .	83
<b>24 Thursday, December 02</b>	<b>85</b>
24.1 Setup . . . . .	85
24.2 Proof: Finiteness implies the Tate conjecture . . . . .	86
24.3 Faltings Heights . . . . .	88
<b>ToDoS</b>	<b>89</b>

<b>Definitions</b>	<b>91</b>
<b>Theorems</b>	<b>92</b>
<b>Exercises</b>	<b>94</b>
<b>Figures</b>	<b>95</b>

# 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:

- $k^n$  will denote  $n$ th powers in  $k$ , and similarly for  $k^\times$ .
- $k^{\text{un}}$  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  $k[x_1, \dots, x_m]$ :

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

Some natural questions:

**Remark 2.0.4 (Topic 1: Are there any common solutions?):** More generally, does  $X := V(f_1, \dots, f_n)$  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  $\text{ht}(a/b) = \max(|a|, |b|)$ ?
- 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 adèles? 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 is 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  $f - a \pmod{p}$  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 mod  $p$  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  $X := V(ax^2 + by^2 + cz^2) \subseteq \mathbb{P}^2$  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  $X_{/\bar{k}} \cong \mathbb{P}_{/\bar{k}}^n$  satisfy the Hasse principle.

**Example 2.1.5(Quadratics)**: 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  $X = V(f_1, \dots, f_n)$ , the ring  $\bar{k}[x_1, \dots, x_n]$  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  $X = V(f_1, \dots, f_n)$  with a nonempty smooth locus  $X^{\text{sm}} \subseteq X$  which is a variety (just adjoin inverses of partial derivatives appearing in minors of Jacobian matrices). So  $X^{\text{sm}}/\mathcal{O}_{K,S} = \mathcal{O}_K \left[ \frac{1}{N} \right]$  which is smooth over  $\mathcal{O}_{K,S}$
2. Use Lang-Weil to show that  $X^{\text{sm}}(\mathcal{O}_{K,S}/\mathfrak{p}) \neq \emptyset$  for almost all  $\mathfrak{p}$ .
3. Use smoothness and Hensel's lemma to get  $X^{\text{sm}}(\mathcal{O}_{K,S}^{\widehat{\mathfrak{p}}})$ .

■

## 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.

$$\begin{array}{ccc} \text{Spec } R & \longrightarrow & X \\ \downarrow \text{cl} & \nearrow \exists & \downarrow \text{sm} \\ \text{Spec } R' & \longrightarrow & Y \end{array}$$

Taking  $R := R'/I$  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  $\text{reldim } X = 1$  for  $X \rightarrow S$  over  $\mathcal{O}_K[\frac{1}{n}]$  where  $S$  is a curve with geometrically integral fibers.
- Without loss of generality,  $X \rightarrow S$  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  $X \rightarrow S$  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  $X/\bar{K} \cong \mathbb{P}^n$ ) 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,
- $\text{Br}(X)$  is an abelian group
- Given  $X \xrightarrow{f} Y$ , there is an induced map  $f^* : \text{Br}(Y) \rightarrow \text{Br}(X)$ .

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

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

which fits into a SES

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

Note that most of the terms in the middle sum are  $\mathbb{Q}/\mathbb{Z}$ , making  $\text{Br}(K)$  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  $X(K) \rightarrow X(\mathbb{A}_K)$ , and taking  $\alpha \in \text{Br}(X)$  one gets a map  $\alpha^* : X(K) \rightarrow \text{Br}(K)$ . This yields a diagram


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

[Link to Diagram](#)

Using that  $\Sigma : \text{Br}(\mathbb{A}_K) \rightarrow \mathbb{Q}/\mathbb{Z}$ , for a fixed  $\alpha \in \text{Br}(X)$ ,

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

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

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


### 3.1.2 The Hasse Principle for Severi-Brauers

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

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

we have

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

#### 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  $K \in \text{Field}$ , then

$$\text{Br}(K) := H_{\text{Gal}}^2(K, \bar{K}^\times) = H_{\text{Grp}}^2(\text{Gal}(K^s/K), (K^s)^\times).$$

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

We can take invariants and coinvariants:

$$M^G := \left\{ m \in M \mid gm = m \quad \forall g \in G \right\} = \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

$$M_G := M / \left\langle \{ gm - m \mid g \in G \} \right\rangle = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M.$$

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)

$$H^i(G; M) := \text{Ext}_{\mathbb{Z}[G]}^i(\mathbb{Z}; M)$$

$$H_i(G; M) := \text{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}; M).$$

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

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

Deleting the augmentation and applying  $\text{Hom}_{\mathbb{Z}[G]}(-, \mathbb{Z})$  yields  $0 \rightarrow \mathbb{Z} \xrightarrow{f \cdot (x-1)} \mathbb{Z} \rightarrow 0$ , 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

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

Then  $H_*(G; \mathbb{Z}) = H^*(G; \mathbb{Z})$  is  $\mathbb{Z}$  in degrees 0 and 1, and 0 otherwise. For  $M \in \mathbb{G}\text{-Mod}$ , 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  $\sigma$  as the generator so that  $\mathbb{Z}[G] = \mathbb{Z}[\sigma]/\langle \sigma^n - 1 \rangle$ . We can take a resolution

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

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

$$\mathbb{Z} \xrightarrow{\sigma-1} \mathbb{Z} \xrightarrow{\sum \sigma^i} \mathbb{Z} \xrightarrow{\sigma-1} \dots \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \dots$$

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  $H_{\text{Grp}}^*(G; \mathbb{Z}) = H_{\text{Sing}}^*(X; \mathbb{Z})$ . 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  $M \in \mathbf{G}\text{-Mod}$ , 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

$$0 \rightarrow M \rightarrow I \rightarrow M/I \rightarrow 0$$

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

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

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

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  $\text{ch } k = 0$  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  $M \rightarrow N \in \mathbf{G}\text{-Mod}$  there are maps

$$\begin{aligned} H^*(G; M) &\rightarrow H^*(G; N) \\ H_*(G; M) &\rightarrow H_*(G; N). \end{aligned}$$

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

$$\begin{aligned} \iota^* : H^*(T; M) &\rightarrow H^*(G; M) \\ \iota_* : H_*(T; M) &\rightarrow H_*(G; M) \end{aligned}$$

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*)

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

It's functorial in  $M$ , and  $\mathrm{tr}_{G/T} \circ \iota^*$  is multiplication by  $m := [G : T]$ . 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).
- $H^1(G; \mathbb{Z}) = \mathrm{Hom}_{\mathrm{Grp}}(G; \mathbb{Z})$ , which is always torsionfree.
- $H^2(G; M)$  classifies extensions of  $G$  by  $M$  in the following sense:  $G'$  occurring in a “SES”  $\xi : 0 \rightarrow M \rightarrow G' \rightarrow G \rightarrow 1$  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  $\xi$  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  $0 \rightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \rightarrow \mathbb{Z}/n \rightarrow 0$ , 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,  $M \in \mathbf{G}\text{-Mod}$  for  $G := \mathrm{Gal}(L/k)$ . Then

$$H_{\mathrm{Gal}}^*(L/k; M) := H_{\mathrm{Grp}}^*(G; M).$$

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

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

*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  $\text{Br}(\mathbb{F}_q)$ , then  $\text{Gal}(\mathbb{F}_q^s/\mathbb{F}_q) = \widehat{\mathbb{Z}} \langle \text{Frob}_q \rangle$ . Then

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

Note: we've used that

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

#### 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

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

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

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

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  $\mathbb{Z}[G]$ -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  $\{(1, g_1, \dots, g_{n-1}) \mid g_k \in G\}$  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  $h : \mathbb{Z}[G^{\times n-1}] \rightarrow \mathbb{Z}[G^{\times n}]$  so that  $hd + dh = \text{id}$ . Take the map  $h(g_1, \dots, g_n) = (e, g_1, \dots, g_n)$ , then

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

and

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

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  $x \in \text{im } d$ , so this makes the complex exact. ■

**Corollary 5.0.3 (?)**

For  $G \in \text{Grp discrete}$  and  $M \in \text{G-Mod}$ ,

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

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

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

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

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

**Definition 5.0.5 (Reduced Complex)**

For  $G \in \text{Grp discrete}$  and  $M \in \text{G-Mod}$ , set

$$\tilde{C}^r(G; M) := \text{Hom}_{\text{Set}}(G^{\times r}, M).$$



The boundary maps are given by

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

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

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

The pattern is multiply by  $\sigma$  on the outside, cycle through multiplying it to each argument, and for the last term leave  $\sigma$  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  $M \in \mathbf{G}\text{-Mod}$ , 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**

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

[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  $X := \mathbb{P}^n_{/k^s}$  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  $\text{Jac}(E)$ , 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  $\text{Jac}(E) \curvearrowright E$  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  $\text{SO}(p, q)_{/\mathbb{R}}$ , the matrices preserving a quadratic form

$$h_{p,q} := \text{diag}(1, \dots, 1, -1, \dots, -1)$$

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

**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  $H^1_{\text{Gal}}(k; \text{Aut}(X_{k^s}))$  (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  $\text{Aut}(X_{k^s})$  is abelian, then we'll show the following stronger claim:

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

$$\left\{ \begin{array}{l} \text{Forms of } X_{k^s} \\ \text{split by } L/k \end{array} \right\} \cong H^1_{\text{Gal}}(L/k; \text{Aut}(X_L)).$$

*Proof (?)*.

Recall that

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

Given  $X'_{/k}$  split by  $L$ , we want a map  $\text{Gal}(L/k) \rightarrow \text{Aut}(X_L)$ . 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

$$f : \text{Gal}(L/k) \rightarrow \text{Aut}(X'/L) \xrightarrow{\sim} \text{Aut}(X_L),$$

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  $H^1(\text{Gal}(L/k), \text{Aut}(X_L))$ , 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  $g \in \text{Aut}(X_L)$ .

**Surjectivity:** Given a crossed homomorphism  $f : \text{Gal}(L/k) \rightarrow \text{Aut}(X_L)$ , 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  $X \in \text{AffVar}$ , so  $X = \text{Spec } R$  and  $\text{Gal}(L/k) \curvearrowright_f R_L = R \otimes_k L$ , which is only an  $L$ -semilinear action. Then  $X' = \text{Spec}(R_L)^{\text{Gal}(L/k)}$ , 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

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

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  $k, L \in \text{Field}$  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

$$\{\text{Forms of } X \text{ split by } L\} \cong H^1_{\text{Gal}}(L/k; \text{Aut}(X_L))$$

Note that we didn't assume the coefficients formed an abelian group, so we'll explain this today. It is true that  $\text{Aut}(X_L) \in \text{Gal}(L/k)\text{-Mod}$ . 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

$$\{\text{Forms of } X\} \cong H^1_{\text{Gal}}(L/k; \text{Aut}(X_{k^s}))$$

*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  $\text{Gal}(L/k) \rightarrow \text{Aut}(X_L)$  such that  $\delta f = 0$  for the differential in cohomology. Since  $X'$  is defined over  $k$ , we have an action  $\text{Gal}(L/k) \curvearrowright X'_L$ , i.e. a map  $\text{Gal}(L/k) \rightarrow \text{Aut}(X'_L)$ , which we can compose with the given isomorphism to obtain

$$f : \text{Gal}(L/k) \rightarrow \text{Aut}(X'_L) \rightarrow \text{Aut}(X_L).$$

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

**Exercise (?)**

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

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

$$X' := \text{Spec}(A \otimes_k L)^{\text{Gal}(L/k)}$$

where the action is given by  $f$ . ■

**Remark 6.1.4:** What is  $\text{Aut}(X_L)$  is nonabelian? Then we just make this proof a definition, and set

$$H^1(L/k; G) := \left\{ f : \text{Gal}(L/k) \rightarrow G \mid f(\sigma\tau) = f(\sigma)f(\tau)^\sigma \right\} / (\sigma \rightarrow g(g^{-1})^\sigma).$$

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  $G \in \text{AlgGrp}/k$ , 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  $G \times X \rightarrow X$  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  $\text{Aut}_{G_L}(G_L) \cong G_L$  as a  $\text{GrpSch}/G_L$ .

## 6.3 Example: Kummer Theory

**Example 6.3.1 (Kummer theory):** Suppose  $\mu_p \subseteq k$ , so  $k$  contains all  $p$ th roots of unity. Then a  $\mu_p$ -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

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

*Proof* (?).

Use the SES

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

which yields a LES

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

and identifying terms yields

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

■

**Example 6.3.3(?)**: What is  $H^1(k; (k^s)^\times)$ ? Use that  $L^\times = \text{Aut}(V/L)$  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  $H^1(k; \text{GL}_n(k^s)) = 1$ .

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

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

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  $G = \text{GL}_n$ .
- Forms of  $\mathbb{P}^n$ , i.e. Severi-Brauer varieties, come from taking  $G := \text{PGL}_{n+1}$ .
- 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  $G := \mathbb{Z}/p$ , this is Kummer theory.
- For  $E$  an elliptic curve, all genus 1 curves are torsors for their Jacobian. So genus 1 curves  $C$  with  $\text{Jac}(C) \cong E$  biject with  $H^1(k; E(k^s))$ .

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

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

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

$$f_s : G^{\times 2} \rightarrow A$$

$$(g_1, g_2) \mapsto s(g_1)s(g_2)s(g_1g_2)^{-1}.$$

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  $G' \cdot G'' := G' \times_G G'' / A$ , and the multiplication map is

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

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

$$\begin{array}{ccccccc}
 & & 1 & & & & \\
 & & \downarrow & & & & \\
 & & Z^G & \longrightarrow & (H')^G & \longrightarrow & H^G \\
 & & & & \delta_0 & & \\
 & \hookrightarrow & H^1(G; Z) & \longrightarrow & H^1(G; H') & \longrightarrow & H^1(G; H) \\
 & & & & \delta_1 & & \\
 & \hookrightarrow & H^2(G; Z) & & & & 
 \end{array}$$

[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  $1 \rightarrow \mathbb{G}_m \rightarrow \mathrm{GL}_n \rightarrow \mathrm{PGL}_n \rightarrow 1$ , 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

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

**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(?)**.

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

## 7 | Tuesday, September 07

### 7.1 Intro: Historical POV on Brauer Groups

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

$$1 \rightarrow (k^s)^\times \rightarrow \text{GL}_n(k^s) \rightarrow \text{PGL}_n \rightarrow 1.$$

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

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

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

**Corollary 7.1.3(?)**.

For any of the  $X$  above, there is an isomorphism:

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

**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  $\mathbb{R}$ .



- $\text{Sym}^n C$  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  $A \in \text{Alg}/_k$ , then TFAE:

- $\exists$  a finite separable extension  $L/k$  where after base-changing to  $L$  one obtains  $A \otimes_k L \cong \text{Mat}(n \times n, L)$ .
- $A \otimes_k k^s \cong \text{Mat}(n \times n, k^s)$ .
- $\exists$  a finite (not necessarily separable) extension  $L/k$  such that  $A \otimes_k L \cong \text{Mat}(n \times n, L)$ .
- $A$  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

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

**Definition 7.1.8** (Opposite algebra)

If  $A \in \text{CSA}/_k$ , then  $A^{\text{op}} \in \text{CSA}/_k$  is an algebra with the same underlying vector space as  $A$  with  $a \cdot_{\text{op}} b := ba$ .

**Definition 7.1.9** (Morita equivalence)

$A, B$  are Morita equivalent if  $A \otimes_k B^{\text{op}}$  is isomorphic to a matrix algebra.

**Theorem 7.1.10** (?).

Given  $A, B \in \text{CSA}/_k$  which correspond to elements  $[A], [B] \in H^2$ , then

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

## 7.2 The Boundary Map and Twisted Vector Space

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

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

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

$$\begin{array}{ccc}
 \mathrm{Gal}(k^s/k) & \xrightarrow{f} & \mathrm{PGL}(k^s) \\
 \downarrow & & \uparrow \\
 \mathrm{Gal}(L/k) & \xrightarrow{\tilde{f}} & \mathrm{PGL}_n(L)
 \end{array}$$

[Link to Diagram](#)

To compute this boundary, we use the original SES:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & k^s & \longrightarrow & \mathrm{GL}_n(k^s) & \longrightarrow & \mathrm{PGL}_n(k^s) & \longrightarrow & 1 \\
 & & & & \nwarrow \tilde{f} & & \uparrow f & & \\
 & & & & & & \mathrm{Gal}(k^s/k) & & 
 \end{array}$$

Choose a set-theoretic lift  $\tilde{f}$

[Link to Diagram](#)

So  $\tilde{f} : \mathrm{Gal}(k^s/k) \rightarrow \mathrm{GL}_n(k^s)$  is a lift of  $f$ , and  $\delta f$  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  $\mathrm{PGL}_n$  and is trivial.

**Definition 7.2.2** (Twisted vector spaces)

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

$$\begin{aligned}
 \tilde{f} : \mathrm{Gal}(L/k) &\rightarrow \mathrm{Aut}(L^n) = \mathrm{GL}_n(L) \\
 \text{such that } \tilde{f}(\sigma\tau) &= \tilde{f}(\sigma) \tilde{f}(\tau)^\sigma \alpha(\sigma, \tau).
 \end{aligned}$$

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

$$\begin{aligned}
 f_\sigma : L^n &\rightarrow L^n \\
 \text{where } f_\sigma(s \cdot v) &= \sigma(s) \cdot f_\sigma(v),
 \end{aligned}$$

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

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

2. The category  $\text{Tw}_\alpha$  of  $\alpha$ -twisted vector spaces is abelian – the only nontrivial thing to check is that there are enough injectives.
3. There are natural functors

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

4. If  $F/k$  is a separable field extension, then

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

5. There is an equivalence of categories

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

**Proposition 7.2.6 (?).**

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

*Proof (?).*

$\Leftarrow$  : First suppose  $\alpha \equiv 1$ , then  $\text{Tw}_\alpha \xrightarrow{\sim} \text{Vect}_k$ , so just take the vector space  $k$ . If  $\alpha = \delta g$  for some  $g : \text{Gal}(k^s/k) \rightarrow (k^s)^\times$ . Then the action  $\text{Gal}(k^s/k) \curvearrowright k^s$  where  $f_\sigma = g(\sigma)$  is a 1-dimensional  $\alpha$ -twisted vector space by sending  $1 \rightarrow g(\sigma)$  and extending semilinearly.

$\Rightarrow$  : Let  $V$  be a 1-dimensional  $\alpha$ -twisted vector space. Choose an isomorphism  $V \xrightarrow{\sim} k^s$ . For each  $\sigma \in \text{Gal}(k^s/k)$  set  $g(\sigma) = g(1)$  and  $g(\sigma\tau) = g(\sigma)g(\tau)^\sigma \alpha(\sigma, \tau)$ , then

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

■

**Theorem 7.2.7 (?).**

Suppose  $\alpha \in H^2(k; (k^s)^\times)$  is in  $\text{im} \left( H^1(k; \text{PGL}_n) \rightarrow H^2(k; (k^s)^\times) \right)$ , then  $\alpha^n = 1$ .

*Proof (?).*

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

■

**Definition 7.2.8** (Index and period)

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

$$\begin{aligned} \text{period}(\alpha) &:= \text{Ord}(\alpha) \\ \text{index}(\alpha) &:= \min \left\{ n \mid \alpha \in \text{im}(H^1 \rightarrow H^2) \right\}. \end{aligned}$$

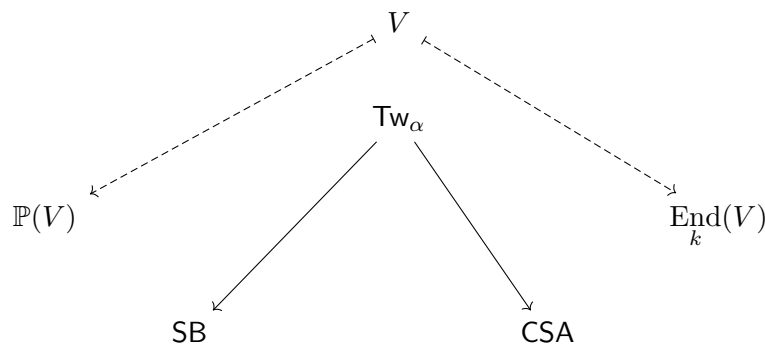
**Corollary 7.2.9(?)**.

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  $\text{Tw}_\alpha$ , SB (Severi-Brauers), and CSA:



[Link to Diagram](#)

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

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

## 8 | Thursday, September 09

**Remark 8.0.1:** Last time: 3 geometric avatars of elements  $\alpha$  of a Brauer group:

- $\alpha$ -twisted vector spaces  $\text{Tw}_\alpha$

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

Here we set  $G := \text{Gal}(L/k)$  and  $\alpha : G^{\times 2} \rightarrow L^\times$  representing  $[\alpha] \in H^2(G; L^\times)$ , and defined an  $\alpha$ -twisted vector space as a  $V \in \text{Vect}/L$  with a semilinear map  $f_\sigma : V \rightarrow V$  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

$$\text{im} \left( H^1(k; \text{PGL}_n) \rightarrow H^2(k; (k^s)^\times) \right)$$

is  $n$ -torsion.

**Theorem 8.0.2(?)**.

The category  $\text{Tw}_\alpha$  is **semisimple**, i.e. every SES splits, and every object is a direct sum of simple objects.

*Proof (?)*.

Note that in vector spaces,  $\text{Hom}_k(A, B) \cong B \otimes_k A^\vee$ , so  $\text{Hom}_k(-, B) = (-) \otimes_k B^\vee$  as functors.

Take a SES

$$0 \rightarrow V_2 \rightarrow W \rightarrow V_1 \rightarrow 0 \in \text{Tw}_\alpha.$$

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

$$0 \rightarrow \text{Mor}_{\text{Tw}_\alpha}(V_1, V_2) \rightarrow \text{Mor}_{\text{Tw}_\alpha}(V_1, W) \rightarrow \text{Mor}_{\text{Tw}_\alpha}(V_1, V_1) \rightarrow 0.$$

This sequence is exact since we can write

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

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

**Theorem 8.0.3(?)**.

Any two simple objects  $D_1, D_2 \in \text{Tw}_\alpha$  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 (?)*.

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

**Corollary 8.0.5(?)**

There exists a unique simple object  $D$  of  $\mathrm{Tw}_\alpha$ , 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  $\mathrm{Tw}_\alpha$ . Let  $X = \mathbb{P}(V)$  for  $V \in \mathrm{Tw}_\alpha$ , 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  $X \in \mathrm{SB}$  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

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

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

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

**Definition 8.0.8** (Reduced norm and trace)

Let  $A \in \text{CSA}_{/k}$ , then there are maps

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

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

$$\begin{aligned} \text{Nm}_{A/k} : \text{End}(V) &\rightarrow \text{End}\left(\bigwedge^{\dim V} V\right) = k \\ \text{Tr}_{A/k} : \text{End}(V) &\xrightarrow{\sim} V \otimes V^\vee \xrightarrow{\langle -, - \rangle} k. \end{aligned}$$

**Proposition 8.0.9** (?).

For  $A \in \text{CSA}_{/k}$ , then if there exists a nonzero  $f \in A$  with  $\text{Nm}_{A/k}(f) = 0$ , 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  $\text{Nm}(ff^{-1}) = 1 \neq 0$ . ■

**Theorem 8.0.10** (?).

There is a surjection

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

*Proof* (sketch).

It's enough to show the following surjection:

$$\bigcup_n H^1(L/k; \text{PGL}_n) \rightarrow H^2(L/k; L^\times).$$

Given  $\alpha$  in the codomain, interpret it as a central extension:

$$1 \rightarrow L^\times \rightarrow M_\alpha \rightarrow \text{Gal}(L/k) \rightarrow 1.$$

**Definition (Semilinear group rings)**

Define  $L[M_\alpha]$  to be the **semilinear group ring** of  $M_\alpha$ :

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

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

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

**Question 8.0.12**

Can this construction be done in SB or  $\text{Tw}_\alpha$ ?

## 8.1 Computing Brauer Groups

**Remark 8.1.1:**

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

**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  $\text{Br}(k) = 0$ .

**Remark 8.1.3:** Note that [Chevalley-Waring](#) exactly says that finite fields are  $C_1$ .

*Proof (of theorem).*

**Claim:** Let  $A \in \text{CSA}_{/k}$ , then  $\text{Nm}_{A/k} : A \rightarrow k$  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  $\text{rank } A > 1$ , there exists a nonzero  $f \in A$  such that  $\text{Nm}_{A/k}(f) = 0$ .

But all  $k$ -division algebras are isomorphic to  $k$ , here all CSAs are of the form  $\text{Mat}(n \times n, k)$ , 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  $f : k(C)^n \rightarrow k(C)$ , we want to show  $f^{-1}(0)$  is big. Let  $p \in C$ , and now  $f$  as a map

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

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  $X \in \text{SB}/k$ , then TFAE:

- $X$  has a rational point,
- $X \cong \mathbb{P}^n$  for some  $n$ ,
- $[X] \in \text{Br}(k)$  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

$$\text{Br}(k) \hookrightarrow \bigoplus_{v \in \text{PI}(k)} \text{Br}(k_v),$$

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

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

### 9.1 Cyclic Algebras

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

$$\chi_L : \text{Gal}(k^s/k) \rightarrow C_n.$$

For  $a \in K^s$ , we'll consider pairs  $(\chi, a) = L[x]^X / \langle x^n - a \rangle$  where commutation in  $L[x]^X$  is given by  $lx = x\sigma(l)$  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  $(\chi, a) \in \text{CSA}$ .

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

**Fact 9.1.3**

One can view  $\chi \in H_{\text{Gal}}^1(k; C_n)$  and

$$a \in H_{\text{Gal}}^1(k; \mu_n) = k^\times / (k^\times)^2.$$

In this case

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

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

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

$$\begin{array}{ccc}
 & & \vdots \\
 P^\bullet : & & \\
 & \mathbb{Z}[x]/\langle x^2 - 1 \rangle & \\
 & \downarrow x-1 & \\
 & \mathbb{Z}[x]/\langle x^2 - 1 \rangle & \\
 & \uparrow x+1 & \\
 & \mathbb{Z}[x]/\langle x^2 - 1 \rangle & \\
 & \downarrow x-1 & \\
 & \mathbb{Z}[x]/\langle x^2 - 1 \rangle & 1 \\
 & \downarrow & \downarrow \\
 & \mathbb{Z} & 1
 \end{array}$$

[Link to Diagram](#)

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

$$\begin{array}{ccccccc}
 1 & \longrightarrow & z\bar{z} & & & & \\
 & & & & & & \\
 \mathbb{C}^\times & \longrightarrow & \mathbb{C}^\times & \longrightarrow & \mathbb{C}^\times & \longrightarrow & \mathbb{C}^\times \\
 & & & & & & \\
 z & \longrightarrow & \bar{z}z^{-1} & & z & \longrightarrow & \bar{z}z^{-1}
 \end{array}$$

[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,  $\text{im } d = \mathbb{R}_{>0}^\times$ , so

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

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

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

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

**Remark 9.1.6**: Write  $k^{\text{un}}$  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  $k^{\text{un}} = \text{ff}(W(\overline{\mathbb{F}}_p))$  (i.e. the Witt vectors). In general,  $k^{\text{un}} = k(\mu'_{\infty})$  where  $\mu'_{\infty}$  is the set of roots of unity of order prime to the characteristic. As a corollary,  $\text{Gal}(k^{\text{un}}/k) = \overline{\mathbb{F}}_q / \mathbb{F}_1 = \hat{\mathbb{Z}}$ .

**Theorem 9.1.7 (?)**.

For  $k$  a nonarchimedean local field (a finite extension of  $\mathbb{Q}_p$ ), then  $\text{Br}(k) = \mathbb{Q}/\mathbb{Z}$

- $H^2(k^{\text{un}}/k; (k^{\text{un}})^\times) = \mathbb{Q}/\mathbb{Z}$
- $H^2(k^{\text{un}}/k; (k^{\text{un}})^\times) \xrightarrow{\sim} H^2(k; (k^s)^\times) = \text{Br}(k)$  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:

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

[Link to Diagram](#)

**Claim:**

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

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

$$\begin{array}{ccccc} H^2(k^{\text{un}}/k; U_{k^{\text{un}}}) = 0 & \longrightarrow & H^2(k^{\text{un}}/k; (k^{\text{un}})^\times) & \longrightarrow & H^2(k^{\text{un}}/k; \mathbb{Z}) \\ & & & \searrow & \\ & & & & H^3(k^{\text{un}}/k; U_{k^{\text{un}}}) = 0 \end{array}$$

[Link to Diagram](#)

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

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

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 that annihilates it. As a corollary, taking the LES above yields  $H^i(G; \mathbb{Z}) = H^{i-1}(G; \mathbb{Q}/\mathbb{Z})$  for  $i \geq 2$ . Thus

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

and in fact

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

■

*Proof (of b).*

Here we'll have to use the structure of  $U_{k_n^{\text{un}}}$ . 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  $\text{Fil}_r U_{k_n} = \{u \in U_{k_n} \mid u \equiv 1 \pmod{\pi^r}\}$  for  $\pi$  a uniformizer.

**Fact**

We can identify

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

where  $\kappa$  denotes residue fields,  $\kappa_n/\kappa$  is the unique degree  $n$  extension, and  $\kappa^+$  is the additive group. Why: use that these look like power series, and the associated graded picks off the  $r$ th 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,



Check 2!

To prove 1, we used

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

and

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

where we used a filtration

$$\text{Fil}_r U_{k^{\text{un}}} = \begin{cases} U_{k^{\text{un}}} & r = 0 \\ \{x \mid x \equiv 1 \pmod{\pi^r}\} & r \geq 1. \end{cases}$$

and

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

We now want to show

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

**Proposition 10.1.2 (?)**.

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

*Proof (?)*.

$H^1$  here classifies forms of SESs

$$0 \rightarrow k \rightarrow V \rightarrow k \rightarrow 0,$$

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

**Theorem 10.1.3 (?)**.

For  $k$  any field,  $H^{>0}(k; (k^{\text{sep}})^+) = 0$ .

*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  $M \in \mathbf{H}\text{-Mod}$  then

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

Now use that

$$H^*(\text{Gal}(L/k); k[\text{Gal}(L/k)]) = H^*(1; k) = 0 \quad * > 0.$$

■

*Proof (of Shapiro's lemma).*

Let  $P^\bullet \rightrightarrows \mathbb{Z} \in \mathbb{Z}[G]\text{-Mod}$  be a free resolution and use Frobenius reciprocity to write

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

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

■

*Proof (of theorem, part b).*

We now want to prove (3),

$$H^*(k_{/k}^{\text{un}}; U_{k^{\text{un}}}/\text{Fil}^r) = 0 \quad * > 0.$$

By induction on  $r$ , since we have a SES

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

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  $H^*(k_{/k}^{\text{un}}; U_{k^{\text{un}}}) \rightarrow \varprojlim_r H^*(k_{/k}^{\text{un}}; U_{k^{\text{un}}}/\text{Fil}_r)$ . We can move an inverse limit in:

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

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  $D = \text{End}(V) \in \text{Tw}/k$  for some  $V \in \text{Tw}$  of dimension  $n$ , then

$$D \times_k L = \text{End}(V \times_k L) \in \text{Tw}/L.$$

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  $n := \#\text{Gal}(L/k)$ .

*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  $v : D \rightarrow \mathbb{Z} \cup \{\infty\}$  extending the valuation on  $K \subseteq D$  given by  $1/n \text{val}(\text{Nm}_{D/k}(x))$ . 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

$$\mathcal{O}_D := \{x \mid v(x) \geq 0\} \subseteq D$$

$$\mathfrak{m}_D := \{x \mid v(x) > 0\} \subseteq D$$

$$\mathcal{I} := \mathcal{O}_D / \mathfrak{m}_D,$$

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

$$f := [\mathcal{I} : k]$$

Degree of field extensions

$$e := [\text{val}(k) : \text{val}(D)]$$

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  $L \in \text{Alg}_k$  with  $L \subseteq D$  satisfies  $\dim_k L \leq n$ .

*Proof (?)*

It's enough to prove this for  $\text{Mat}(n \times n; k)$ , 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  $\alpha$  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:

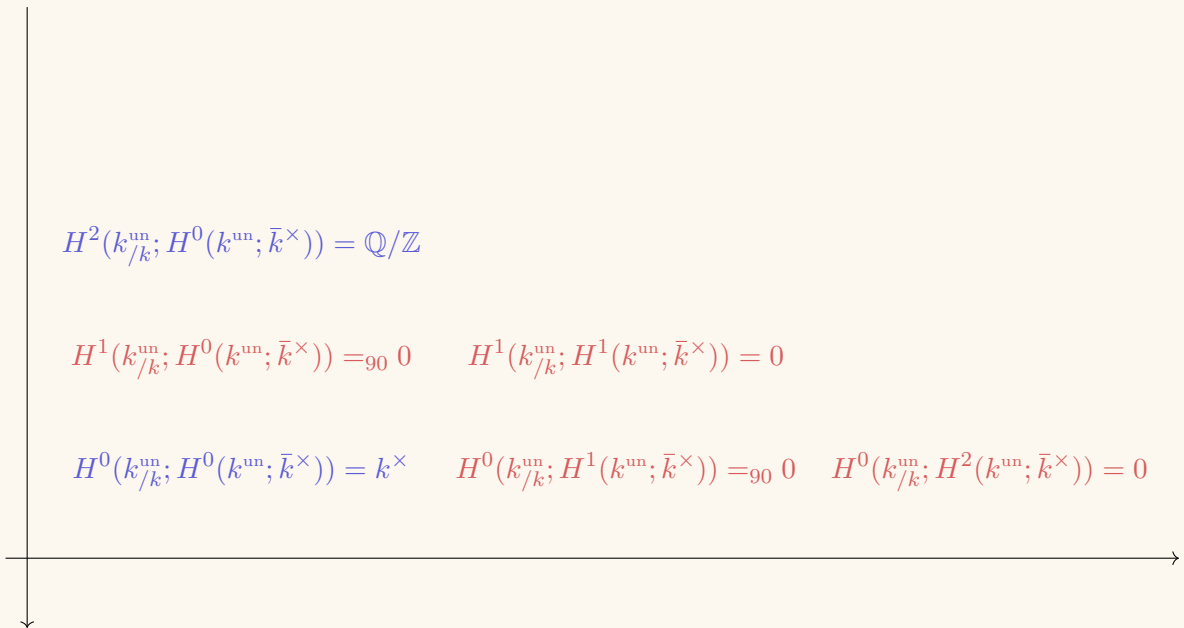
$$\mathbb{Q}/\mathbb{Z} \cong H^2(k^{\text{un}}/k; (k^{\text{un}})^\times) \xrightarrow{\sim} H^2(k; \bar{k}^\times).$$

*Proof (of claim).*

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

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

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

$$0 \rightarrow \text{Br}(k^{\text{un}}/k) \rightarrow \text{Br}(k) \rightarrow \text{Br}(k^{\text{un}}).$$

■

# 11 | Tuesday, September 21

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

- Examples
- A SES for  $L$  a number field:

$$0 \rightarrow \text{Br}(L) \rightarrow \bigoplus_{v \in \text{Pl}(k)} L_{\hat{v}} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

- 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

$$\chi : \text{Gal}(k^{\text{sep}}/k) \rightarrow C_n = \langle \sigma \rangle$$

and set  $k_{\chi}$  to be the fixed field.

**Definition 11.1.2** (Cyclic Algebra)

For  $a \in k^{\times}/(k^{\times})^n$ , write

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

**Remark 11.1.3:** We have

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

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

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

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

**Theorem 11.1.5(?)**

Let  $\pi$  be a uniformizer of  $\mathcal{O}_K$ . Every CSA is equivalent to one of the form

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

**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  $\text{Br}(k) \rightarrow \mathbb{Q}/\mathbb{Z}$ . 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  $\text{Gal}(k_n/k) \xrightarrow[\text{can}]{\sim} C_n$  (where we take Frob as the canonical generator).
- Then  $[D] \mapsto \frac{v(\sigma)}{n} \in \mathbb{Q}/\mathbb{Z} = \text{Br}(k)$ , 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

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

Hence any character

$$\chi : \text{Gal}(k^{\text{sep}}/k) \rightarrow C_2 = \mu_2$$

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

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

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

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

### 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  $\alpha$  by  $X \in \mathrm{SB}$ , 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)

$$\mathbb{I}_k := \prod'_v (k_{\widehat{v}}^\times, \mathcal{O}_{k_{\widehat{v}}}^\times) = \left\{ (x_v) \in \prod_v k_{\widehat{v}}^\times \mid x_v \in \mathcal{O}_{k_{\widehat{v}}}^\times \text{ for almost all } v \right\}.$$

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

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

**Fact 11.2.6**

$$\mathbb{I}_k = \operatorname{colim}_S \mathbb{I}_{k,S}.$$

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

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

where  $C_L$  is the idele class group.

**Proposition 11.2.8** (?).

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

$$H^2(k; \mathbb{I}_{k^{\text{sep}}}) = \bigoplus_{v \in \text{Pl}(k)} \text{Br}(k_{\widehat{v}}),$$

**Theorem 11.2.9** (?).

$$H^1(L/k; C_L) = 0$$

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

This will imply

$$H^1(k; C_{k^{\text{sep}}}) = 0$$

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

*Proof (sketch).*

We can write

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

$$= \varinjlim_T H^2(L/k; \mathbb{I}_{L,T}),$$

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

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

■


**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  $k \in \text{Field}$ , we have a SES  $1 \rightarrow k^\times \rightarrow \mathbb{I}_k \rightarrow C_k \rightarrow 1$ . An exercise from last time: for  $\text{Pl}(k)$  the places of  $k$ , prove that

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

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

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


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:

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

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

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:**

$$H^2(L/k; \prod_{w/v} L_w^\times) = \text{Br}(L_{\widehat{v}/k_{\widehat{v}}})$$

$$H^2(L/k; \prod_{w/v} L_w^\times) = 0.$$

*Proof (of 1).*

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

■

*Proof (of 2).*

Write

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

■

Corollary 12.1.2(?).

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

[Link to Diagram](#)

## 12.2 Injectivity

**Theorem 12.2.1 (Injectivity).**

$\text{Br}(k) \hookrightarrow \bigoplus_v \text{Br}(k_{\widehat{v}})$  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  $M \in \mathbf{G}\text{-Mod}$  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

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

Since  $d$  is prime to  $p$ ,  $\text{res}$  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  $\text{Gal}(L/k)$  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  $G := \text{Gal}(L/k)$  a  $p$ -group, then let  $H \leq G$  be a nontrivial normal cyclic subgroup. Then the inflation-restriction exact sequence yields

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

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  $M \in \mathbf{G}\text{-Mod}$ , define the **Herbrand quotient** as

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

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  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  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  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  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

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

and so

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

Now to show that the sizes are equal, Recall that

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

Thus we get

$$\begin{aligned} 0 \rightarrow H^1(G; M) \rightarrow \text{coker}(M \xrightarrow{g-1} M) \xrightarrow{\sum g^i} \ker(M \xrightarrow{g-1} M) \rightarrow H^2(G; M) \rightarrow 0 \\ \implies 0 \rightarrow H^1(G; M) \rightarrow M_G \xrightarrow{\sum g^i} M^G \rightarrow H^2(G; M) \rightarrow 0, \end{aligned}$$

so

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

**Lemma 12.2.12 (?).**

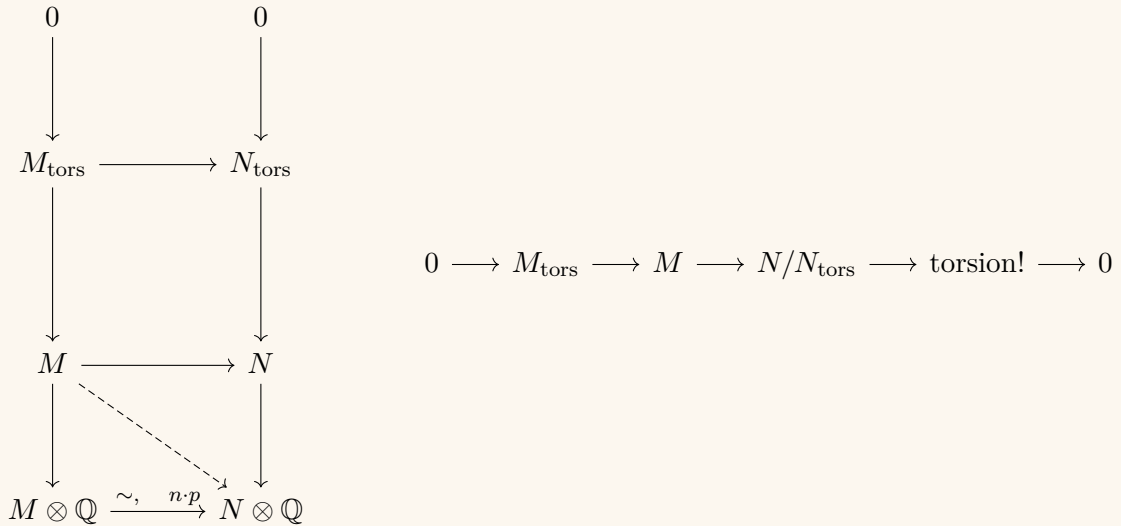
If  $M, N$  are finitely generated in  $\mathbf{G}\text{-Mod}$  and  $M \otimes \mathbb{R} \cong N \otimes \mathbb{R} \in \mathbf{G}\text{-Mod}$ , then  $q(M) = q(N)$ .

**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  $M/\text{tors} \rightarrow N/\text{tors}$  with finite kernel and cokernel.



[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  $G \in \text{Grp}$  and  $V_1, V_2 \in \text{G-Mod}$  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  $\text{Hom}$  commutes with tensor products in the following way:

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

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  $V^G := \ker(V^{\oplus q} \xrightarrow{q} \bigoplus_{g \in G} V)$ . 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  $\mathbb{A}_k^n$  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 primes under a set of generators of the class group of  $L$ , letting  $T$  be the set of primes of  $L$  over  $S$ , we have

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

*Proof (1 and 2 imply 3).*

There is a SES

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

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

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

*Proof (of 1).*

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

$$\begin{aligned} q(\mathbb{I}_{L,T}) &= \prod_{v \in S} q\left(\prod_{w \in \text{Pl}(L)} L_w^\times\right) \\ &= \prod_{v \in S} \frac{\#H^2(L_v/k_v; L_v^\times)}{\#H^2(L_v/k_v; L_v^\times)} \\ &= \prod_{v \in S} \# \text{Br}(L_v/k_v) \\ &= \prod_{v \in S} [L_v : k_v]. \end{aligned}$$

■

*Proof (of 2).*

Write  $L_1 := \text{Hom}_{\text{Set}}(T, \mathbb{Z})$  and

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

Dirichlet's unit theorem implies  $L_2 \hookrightarrow L_1^0 \otimes \mathbb{R} := \{\mathbf{x} \mid \sum x_i = 0\}$  is a lattice. We can write

$$\begin{aligned} L_1 &= \bigoplus_{v \in S} \bigoplus_{w/v} \mathbb{Z} \\ &= \bigoplus_{v \in S} \text{Ind}_{\text{Gal}(L_v/k_v)}^{\text{Gal}(L/k)} \mathbb{Z}, \end{aligned}$$

Thus

$$\begin{aligned} q(L_1) &= \prod_{v \in S} q\left(\text{Ind}_{\text{Gal}(L_v/k_v)}^{\text{Gal}(L/k)} \mathbb{Z}\right) \\ &= \prod_{v \in S} q(L_v/k_v; \mathbb{Z}) \\ &= \prod_{v \in S} [L_v : k_v]. \end{aligned}$$

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

$$q(L_1^0) = q(L_1)/q(L/k; \mathbb{Z}) = \frac{\prod [L_v : k_v]}{[L : k]}.$$

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

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

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

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

■

**Fact 13.0.4** (from class field theory)

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

How to prove: reduce to Kummer extensions, adjoin  $p$ th roots of unity, etc.

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

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

## 13.1 Proof

**Theorem 13.1.1 (Hasse-Minkowski).**

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

**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  $q(\mathbf{x}) = a$ .

**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  $v \in \text{Pl}(k)$ . 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  $q'(\mathbf{x}, z) := q(\mathbf{x}) - az^2$ . 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

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

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

*Proof (n = 4 case).*

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

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

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

[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:

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

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

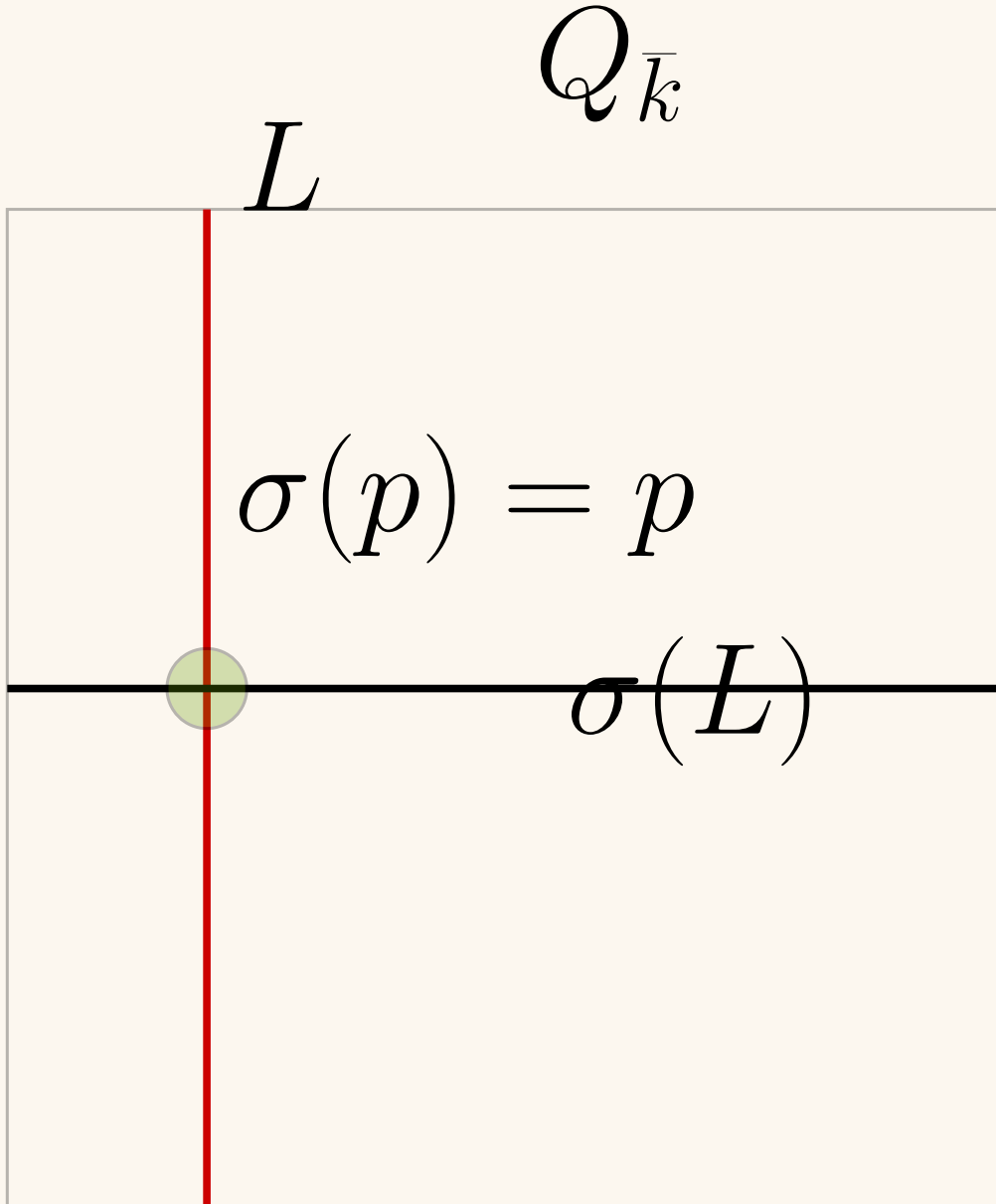
so  $X_{k'}$  is disconnected.

- We can take  $[Q] \in H^1(k; \mathcal{O}_n) \xrightarrow{\det} H^1(k; \mu_2)$ , and it maps to  $[k']$ .
- $\text{Gal}(\bar{k}/k)$  acts on  $\text{Pic}(Q) \cong \mathbb{Z}^{\times 2}$ , and this action factors through  $\{\pm 1\}$ . Here  $\mathcal{O}_n = \text{Aut}(\sum x_i^2)$ .
  - Why: this action preserves the *effective cone* in  $\text{Pic}(Q_{\bar{k}})$  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  $[L] \in \text{Pic}Q$  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  $\text{Gal}(k'/k) \curvearrowright L$ , so take  $\sigma \in \text{Gal}(k'/k)$ . 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  $Q = a_1x_1^2 + a_2x_2^2 + G(x_3, \dots, x_n)$ .

**Claim:**  $G$  represents  $k_{\widehat{v}}$  for almost all  $v \in \text{Pl}(k)$ .

It's enough to show that  $G'(x_3, \dots, x_{n+1}) := G(x_3, \dots, x_n) + ax_{n+1}^2$  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  $v$ ,  $G(x_3, \dots, x_n)$  represents *every* element of  $k$ .

Let  $U \subseteq (\prod k_{\widehat{v}})^{\times n-2} k[v]$  be the set  $\{(x_3, v), \dots, (x_n, v)\}$  such that there exists an  $(x_1, v), (x_2, v)$  with  $Q(x_1, \dots, x_n) = 0$ . 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  $(x_3, v), \dots, (x_n, v)$  with  $Q(x_1, \dots, x_n) = 0$  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  $Q'(z, x_3, \dots, x_n) = -cz^2 + G(x_3, \dots, x_n)$ . 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  $\kappa$ , there is an isomorphism  $\text{Br}(R) \xrightarrow{\sim} \text{Br}(\kappa)$ .

**Remark 15.0.2:** We'll prove a stronger claim that there is a bijection  $\text{SBSch}/_R/ \sim \rightarrow \text{SBSch}/_k/ \sim$ , which requires some deformation theory. A summary of obstruction theory for schemes:

Let  $A \in \mathbf{CRing}$ ,  $I \trianglelefteq A$  is square zero ideal, and  $X_{/A/I}$  a smooth scheme. Then there exists a functorial class  $\text{obs}(X) \in H^2(X; \mathbf{T}_X \otimes_{A/I} I)$  such that  $X$  admits a flat lift to  $A$  iff  $\text{obs}(X) = 0$ . 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  $E \rightarrow X$ , the cohomology would be in  $\text{End}(E)$ .

See also tangent/cotangent complex.

*Proof (?)*.

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

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

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  $\text{obs}(S_n) = 0$ , since

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

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  $X \in \mathbf{Var}_{/k}$  and let  $A \in \mathbf{Br}(X)$  (e.g. represented by an Azumaya algebra), then

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

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

- For  $k = \mathbb{R}$ , the map  $X(\mathbb{R}) \rightarrow \text{Br}(k) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$  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  $A \in \text{Br}(X)$ , 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  $\psi$  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

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

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  $A \in \text{Br}(X)$ . Then

- The following map on adèles is locally constant:

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

- $X(\mathbb{A})^A := (A^*)^{-1}(0)$  is closed and open.
- $X(\mathbb{A})^{\text{Br}} = \bigcap_{A \in \text{Br}(X)} X(\mathbb{A})^A$  is closed.
- $\overline{X(k)} \subseteq X(\mathbb{A})^{\text{Br}}$ .
- If  $X$  is proper, then  $X(\mathbb{A})^{\text{Br}} \neq X(\mathbb{A})$  and weak approximation does not hold.

*Proof (?)*.

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

**Warning 15.0.6**

The adelic topology is not the product topology.

**Definition 15.0.7** (Symbol Algebra)

For  $k \in \text{Field}$  and let  $\chi : \text{Gal}(\bar{k}/k) \rightarrow C_n$  and  $a \in k^\times / (k^\times)^n$ , then recall that  $(\chi, a) := L_\chi \langle x \rangle_\sigma / \langle x^n - a \rangle$  where  $L_\chi$  is the fixed field of  $\chi$  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  $U = \{y^2 + z^2 = (3 - x^2)(x^2 - 2)\}$  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  $\mu_n(k) \rightarrow C_n$  induces a bijection

$$k^\times / (k^\times)^n \xrightarrow{\sim} \left\{ \chi : \text{Gal}(\bar{k}/k) \rightarrow C_n \right\}$$

$$a \mapsto k[x] / \langle x^n - a \rangle.$$

For  $n = 2$  and  $\text{ch } k \neq 2$ , 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

$$H^1(k; C_n) \times H^1(k; \mu_n) \rightarrow H^2(k; \mu_n)$$

$$\chi \mapsto [\chi] \smile [a].$$

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

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

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

**Corollary 15.0.10(?)**.

$$(\chi, a) = 0 \iff a \in \text{Nm}_{L/k} L^\times.$$

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

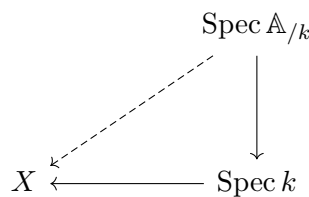
**Exercise 15.0.12 (?)**

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

# 16 | Tuesday, October 19

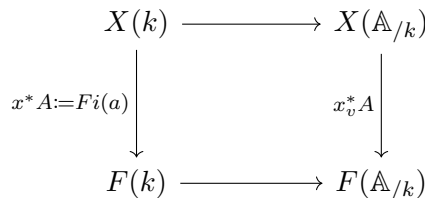
Missing some stuff! Find notes.

**Remark 16.0.1:** Let  $k$  be a number field,  $X \in \text{Var}/_k$  a variety, and  $\mathbb{A}/_k$  the adeles over  $k$ . Let  $F : \text{Sch}^{\text{op}} \rightarrow \text{Set}$  be a functor, we can then consider an  **$F$ -obstruction to rational points**. A rational point is the data of a morphism  $\text{Spec } k \rightarrow X$ , denoted  $X(k) = \text{Sch}(\text{Spec } k, X)$ , and adelic points  $X(\mathbb{A}/_k) = \text{Sch}(\mathbb{A}/_k, X)$ . Since there is a morphism  $k \rightarrow \mathbb{A}/_k \in \text{Ring}$ , this yields a morphism  $X(k) \rightarrow X(\mathbb{A}/_k)$  (noting contravariance). Note that an adelic point is a lift:



[Link to Diagram](#)

Moreover,  $F$  induces a diagram. Let  $i : \text{Spec } k \rightarrow X$  denote the inclusion, and  $x \in X(k)$  be a  $k$ -point. Then writing  $F(k) := F(\text{Spec } k)$ , we have the following:



[Link to Diagram](#)

**Definition 16.0.2 (?)**

Let  $A \in F(X)$ , then

$$\begin{aligned}
 X(\mathbb{A}/_k)^A &:= \left\{ (x_v) \in X(\mathbb{A}/_k) \mid x_v^*A \in \text{im} \left( F(k) \rightarrow F(\mathbb{A}/_k) \right) \right\} \\
 X(\mathbb{A}/_k)^F &:= \bigcap_{A \in F(X)} X(\mathbb{A}/_k)^A.
 \end{aligned}$$

**Example 16.0.3(?):** For  $F(-) := \text{Br}(-)$ , the resulting  $X(\mathbb{A}/_k)^F$  is the **Brauer-Manin obstruction**. Consider  $A \in \text{Br}(X)$  for  $X = V(y^2 + z^2 = (x^2 - 2)(3 - x^2))$ , then any  $k$ -rational point would yield  $x^*A \in \text{Br}(k)$  and thus  $x_v^*A \in \text{Br}(\mathbb{A}/_k)$ . The claim is that  $\text{Br}(\mathbb{A}/_k)^A = \emptyset$ . So consider  $\left\{ (x_v) \in \text{Br}(\mathbb{A}/_k) \mid x_v^*A \in \text{im} \left( \text{Br}(k) \rightarrow \text{Br}(\mathbb{A}/_k) \right) \right\}$ .

**Exercise 16.0.4** (?)

Show this set is empty!

## 16.1 Descent Obstruction

**Definition 16.1.1** (fppf morphisms)

A morphism  $U \rightarrow X \in \text{Sch}$  is **fppf** if

- $f$  is flat<sup>a</sup>,
- $f$  is locally of finite presentation.<sup>b</sup>

<sup>a</sup>Flatness is a local condition:  $f_q : \mathcal{O}_{X,p} \rightarrow \mathcal{O}(U, q)$  for  $q \in f^{-1}(p)$  should be a flat morphism of algebras, where  $A \rightarrow B$  is flat if  $- \otimes_A B$  is flat as a functor on  $\mathbf{A}\text{-Mod}$ .

<sup>b</sup>There exist affine open covers  $\mathcal{V} \rightrightarrows X$  and  $\mathcal{U}_i \rightrightarrows f^{-1}(V_i)$  such that  $f|_{\mathcal{U}_{ij}} : \mathcal{U}_{ij} \rightarrow V_i$  is induced by  $B_i \rightarrow A_{ij} \in \text{Ring}$  of finite presentation. So  $B \rightarrow A \in \text{Ring}$  yields  $A = B[x_0, \dots, x_n]/I$  with  $I$  finitely generated.

**Remark 16.1.2:** Recall that  $\text{GrpSch} \leq \text{Sch}$  is the subcategory of group objects.

**Definition 16.1.3** (?)

For  $G \in \text{AlgGrp}$  or  $\text{GrpSch}/X$ , and let

$$F(-) = H^1(-; G) = \{G\text{-torsors over } X \text{ locally fppf trivial}\}.$$

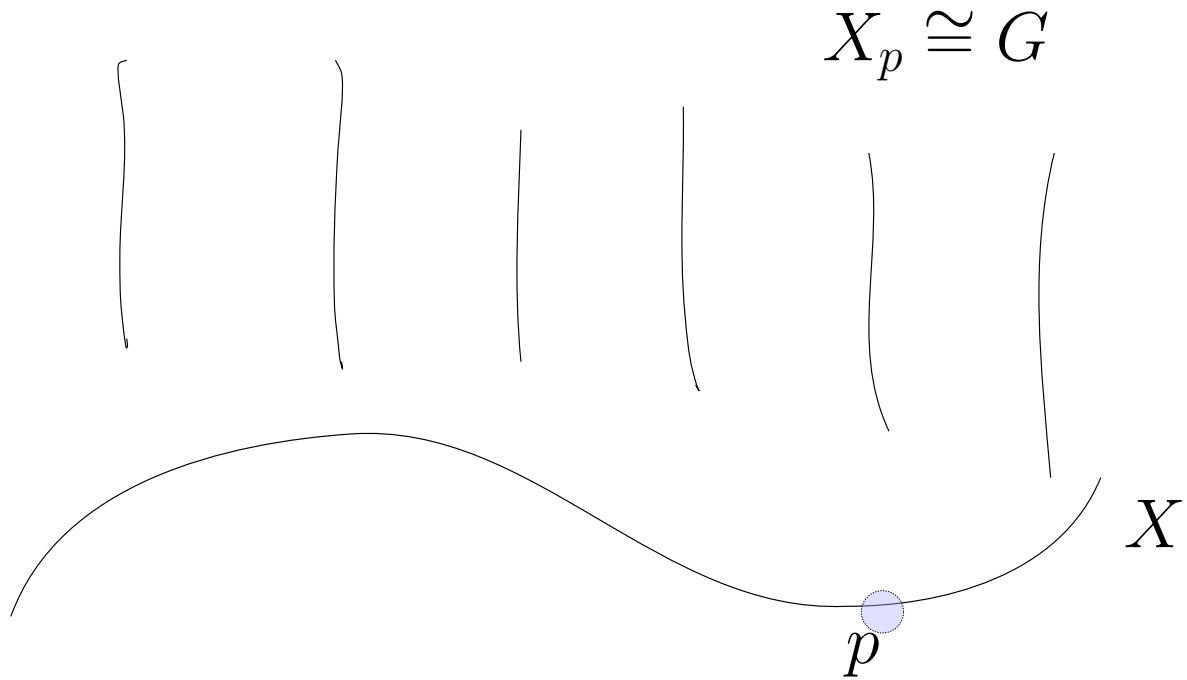
*The fppf site is much more flexible than the étale site!  
Examples are any morphisms  $X \rightarrow \text{Hilb}(\mathbb{P}^n)$ .*

**Definition 16.1.4** ( $G$ -torsors)

A  **$G$ -torsor over  $X$**  is an object  $T \in \text{Sch}/X$  with a  $G$ -action  $G \text{ fp } XT \xrightarrow{\sigma} T$  such that there is an isomorphism

$$G \text{ fp } XT \xrightarrow[(\sigma, \pi_2)]{\sim} T \text{ fp } XT.$$

**Remark 16.1.5:** How to think about torsors: a family whose fibers are abstractly isomorphic to  $G$ , but not canonically.



So the fibers are not canonically identified with  $G$ , but  $G$  acts naturally in a freely transitive way on them. This is essentially the same data as a principal  $G$ -bundle.

**Remark 16.1.6:** Let  $L \rightarrow X$  be a line bundle, so there exists a cover  $\mathcal{U} \rightrightarrows X$  with  $L|_{U_i} \cong \mathbb{A}^1 \times U_i$  and transition functions

$$\mathbb{A}^1 \times (U_i \times U_j) \xrightarrow{(t_{ij}, \text{id})} \mathbb{A}^1 \times (U_i \times U_j)$$

where  $t_{ij} : U_i \times U_j \rightarrow \mathbb{G}_m$ . Then one can obtain a  $\mathbb{G}_m$ -torsor  $L \setminus \{0\} \rightarrow X$  by removing the zero section, and in fact all such  $\mathbb{G}_m$ -torsors arise this way. One can check here that  $\mathbb{G}_m(X) \cong \text{fp } XT \xrightarrow{\sim} T^{\times 2}_X$ .

**Example 16.1.7 (of  $\text{GrpSch}/_X$ ):**

- Take  $G := \mathbb{G}_a, \mathbb{G}_m$  and consider  $G \times X$ , then one can define a multiplication by multiplying the first factors. This generalizes to work for any  $G \in \text{AlgGrp}$ .
- An elliptic curve over  $\text{Spec } \mathbb{Z} \setminus P$  for  $P$  a finite set of primes.
- $\mathbb{Z}/n$  and  $\mu_n$ .

**Remark 16.1.8:** Another formulation:  $\text{GrpSch}/_X$  are representable functors

$$F : \text{Sch}^{\text{op}}/_X \rightarrow \text{Grp}$$

$$Y \mapsto \text{Sch}/_X(Y, G),$$

which composes with  $\text{Grp} \xrightarrow{\text{Forget}} \text{Set}$  in a certain way (?).

**Remark 16.1.9:** Next time: descent obstructions.

# 17 | Descent (Tuesday, October 26)

Missed first few boards, find notes / see phone pics.

**Remark 17.0.1:** If  $G \in \text{smAffGrpSch}/X$  and  $T/X$  is a **locally fppf trivial**  $G$ -torsor, then  $T$  is **etale locally trivial** by a slicing argument.

Setup: let  $X \in \text{Var}/k$  and  $G \in \text{GrpSch}/k$  with  $T/X \in \mathbf{G}\text{-Torsors}$ . Partition  $X(k)$  as

$$X(k) = \coprod_{\tau \in H^1(k;G)} \{x \in X(k) \mid T_x \cong \tau\}.$$

Note that  $H^1(k;G) \in \mathbf{G}\text{-Torsors}/k$ . Let  $\tau \in H^1$  be such a torsor and  $G_\tau$  be the corresponding **inner form**: note that  $G$  acts on itself by conjugation, so inner forms are in the image of the induced map on  $H^1$ :

$$\begin{array}{ccc} \text{im conj}^* & \longrightarrow & \{\text{forms of } G\} \\ \uparrow \text{conj}^* & & \uparrow \cong \\ H^1(k;G) & \xrightarrow{\text{conj}^*} & H^1(k; \text{Aut } G) \end{array}$$

[Link to Diagram](#)

**Exercise 17.0.2** (important: on what descent means and how to compute with it)  
 Prove the following claim:  $\tau \in H^1(k;G)$  is a left  $G$ -torsor, and thus  $\tau$  is naturally a *right*  $G$ -torsor.

**Remark 17.0.3:** Let  $G$  be a discrete group and  $T \in \mathbf{G}\text{-Torsors}$ , or equivalently a group scheme over an algebraically closed field (in characteristic zero). Write  $T^r := \{T, T \times G \rightarrow T : tg := g^{-1}t\}$  to exchange left and right actions, and apply this construction at the level of points. Hint: you'll need to use **descent** to check this.

**Remark 17.0.4:** On twisted **torsors** : define  $T_\tau := G \backslash \begin{smallmatrix} T \times \tau \\ x \end{smallmatrix}$ , and observe that  $T_\tau$  is a right  $G_\tau$  torsor via an action on  $\tau$ .

**Proposition 17.0.5(?)**.  
 There is an equality

$$\{x \in X(k) \mid T_x \cong \tau\} = \text{im}(T_\tau(k) \rightarrow X(k)).$$



*Proof (?)*.

Note that  $x \in \text{im}(T_\tau(k) \rightarrow X(k)) \iff T_\tau|_x$  is a trivial  $G_\tau$ -torsor, since having a rational point implies being a trivial torsor since that point can be used to translate. This happens iff  $G \backslash_x^T \times_X \tau \cong \tau$ .

Conversely, left a rational point and check that you get the graph of an isomorphisms (after base change). ■

**Corollary 17.0.6 (?)**.

One can partition

$$X(k) = \coprod_{\tau \in H^1(k; G)} \text{im}(T_\tau(k) \rightarrow X(k)).$$

**Remark 17.0.7:** Everything up until now works in  $\text{AlgSpaces} \geq \text{Sch}$ , so it's a mostly formal construction thus far.

**Remark 17.0.8:** We showed the following proposition in the case of  $\text{PGL}_n$ : assignments of points to Brauer classes were locally constant.

**Proposition 17.0.9 (Local constancy of evaluation).**

Let  $k \in \text{LocalField}$  and  $X \in \text{Sch}/_k$  proper. <sup>a</sup>

For  $G \in \text{GrpSch}/_k^{\text{ét}}$  and  $T \in \text{G-Torsors}/_X$ , then the following map is locally constant:

$$\begin{aligned} X(k) &\rightarrow H^1(k; G) \\ x &\rightarrow T_x. \end{aligned}$$

<sup>a</sup>Possibly not needed here, but included in Poonen's statement.

**Remark 17.0.10:** How did this proof go before? We showed something didn't deform, i.e. an argument in cohomology of the tangent bundle, and used Artin approximation.

*Proof (?)*.

The point: étale sheaves don't deform, i.e.  $H^1(\mathbb{T}_{T/X}) = 0$  for  $\mathbb{T}$  the relative cotangent bundle (i.e.  $H^1$  with coefficients in the tangent sheaf). See Poonen for a proof use Krasner's lemma. A word on this proof: for a constant group scheme, this is a constant Galois cover and the field extensions don't change under small perturbations (i.e. of the coefficients of the polynomial). ■

**Corollary 17.0.11 (?)**.

The image  $\text{im}(X(k) \rightarrow H^1(k; G))$  is finite.

*Proof (?)*.

Use that the map is proper and  $X(k)$  is compact.

Remark 17.0.12:

## 17.1 Selmer Sets

**Definition 17.1.1** (Selmer Sets)

Let  $k \in \text{NumberField}$ ,  $X \in \text{Var}/k$ ,  $G \in \text{smAffAlgGrp}/k$ ,  $T \in \text{G-Torsors}/X$ . Define

$$\text{Sel}_T(k; G) := \left\{ \tau \in H^1(k; G) \mid \tau_{k_{\widehat{v}}} \in \text{im} \left( X(k_{\widehat{v}}) \rightarrow H^1(k_{\widehat{v}}; G) \right) \text{ for all } v \in \text{Pl}(k) \right\}.$$

**Example 17.1.2(?)**: If  $A/k \in \text{AbVar}$  and  $G := A[n]$  with  $T : A \xrightarrow{[n]} A$ , then  $\text{Sel}_T(k; G)$  is the Selmer group of  $A$ .

**Remark 17.1.3**: Unpacking this definition, we can write this as

$$\text{Sel}_T(k; G) = \left\{ \tau \in H^1 \mid T_\tau(k_{\widehat{v}}) \neq \emptyset \right\} \supseteq \left\{ \tau \mid T_\tau(k) \neq \emptyset \right\}.$$

Then

$$X(k) = \coprod_{\tau \in \text{Sel}_T(k; G)} \text{im} (T_\tau(k) \rightarrow X(k)).$$

# 18 | Thursday, October 28

**Remark 18.0.1**: Let  $k \in \text{GlobalField}$ ,  $G \in \text{GrpSch}/k$ ,  $T \in \text{G-Torsors}/X$ . We defined the Selmer group as

$$\text{Sel}_{T/X}(k; G) := \left\{ \tau \in H^1(k; G) \mid \tau_{k_{\widehat{v}}} \in \text{im} \left( X(k_{\widehat{v}}) \xrightarrow{x \rightarrow T_x} H^1(k_{\widehat{v}}; G) \right) \right\}.$$

**Theorem 18.0.2(?)**.

For  $G$  smooth affine and  $X$  proper,  $\text{Sel}_{T/X}(k; G)$  is finite.

**Corollary 18.0.3(?)**.

The following disjoint union is finite if  $X$  is proper:

$$X(k) = \coprod_{\tau \in \text{Sel}_{T/X}(k; G)} \left\{ x \in X(k_{\widehat{v}}) \mid \tau_x \cong \tau \right\}.$$

**Corollary 18.0.4 (Weak Mordell-Weil theorem).**

For  $A \in \text{AbVar}/k$ , which is a smooth proper group scheme, then  $A(k)/mA(k)$  is finite for any  $m \in \mathbb{Z}_{\geq 0}$ .

**Remark 18.0.5:** Note that Mordell-Weil is about finite generation of  $A(k)$ , which implies that the quotient is finite – for counterexamples, take  $\mathbb{Q}$  and  $\mathbb{Q}/m\mathbb{Q} = 0$ . Existence of [variations of Hodge structure](#): follows from [nonabelian Hodge theory](#).

**18.1 Proof of finiteness of Selmer Sets**

**Remark 18.1.1:** Let  $T$  be defined as multiplication by  $n$  to get a SES

$$0 \rightarrow A[n] \rightarrow A \xrightarrow{x \mapsto nx} A \rightarrow 0.$$

Then we get a diagram

$$\begin{array}{ccc} A(k) & \xrightarrow{x \mapsto T_x} & H^1(k; A[n]) \\ \downarrow & \nearrow & \downarrow \\ A(k)/nA(k) & \longrightarrow & \text{Sel}_{T/X}(k; A[n]) \end{array}$$

[Link to Diagram](#)

**Remark 18.1.2:** We'll separately handle the ramified and unramified cases. We'll need to set up some notation: let  $k \in \text{GlobalField}$ ,  $S \subseteq \text{Pl}(( ) k)$  a finite subset of places,  $\mathcal{G} \in \text{GrpSch}/\mathcal{O}_{k,S}$ . There is a SES

$$0 \rightarrow \mathcal{G}^0 \rightarrow \mathcal{G} \rightarrow \mathcal{G}/\mathcal{F} \rightarrow 0,$$

where  $\mathcal{G}_0$  is the component of the identity. Assume  $\mathcal{F}$  is finite étale, which can always be achieved by enlarging  $S$  if necessary. We'll use Roman letters to denote fibers, whence we get a SES over  $k$ :

$$0 \rightarrow G^0 \rightarrow G \rightarrow F \rightarrow 0.$$

**Definition 18.1.3 (?)**

Define the set of torsors unramified away from  $S$ :

$$H_S^1(k; G) := \left\{ \tau \in H^1(k; G) \mid \tau_{k_v} \in \text{im} \left( H^1(\mathcal{O}_{k_v}; \mathcal{G}) \rightarrow H^1(k; \mathcal{G}) \right) \forall v \in S \right\}.$$

Note that this set depends on the model chosen for  $\mathcal{G}$ .

**Theorem 18.1.4(?)**

The unramified case of Selmer finiteness

- $H_S^1(k; G) \rightarrow H_S^1(k; G) \rightarrow \prod_{v \in S} H^1(k_{\widehat{v}}, F)$  has finite fibers.
- If  $k \in \text{NumberField}$  then  $H_S^1(k; G)$  is finite.

**Remark 18.1.5:** This theorem is due to Lang, who was an AIDS denialist? **Yikes.**

**Remark 18.1.6:** This  $H_S^1(k; G)$  is an approximation to something slightly more natural,  $H_{\text{ét}}^1(\mathcal{O}_{k,S}; \mathcal{G})$ , the  $G$ -torsors over  $\mathcal{O}_{k,S}$ .

**Slogan 18.1.7**

Torsors for connected group schemes are not interesting?

**Theorem 18.1.8(?)**

Let  $G \in \text{smAlgGrp}/\mathbb{F}_q$  be connected, then  $H^1(\mathbb{F}_q; G) = \{\text{pt}\}$ .

**Exercise 18.1.9 (?)**

Write down a variety over  $\mathbb{F}_q$  with no rational points!

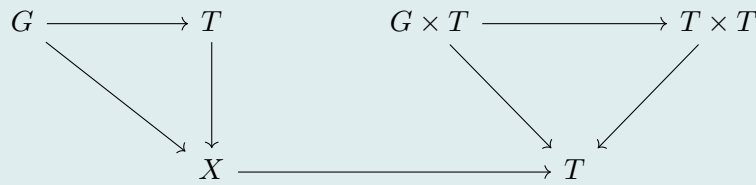
*Proof (?)*

Let  $T \in H^1(\mathbb{F}_q; G)$ , we want to show  $T(\mathbb{F}_q) \neq \emptyset$ . Given a rational point, we want to show  $G \cong T$ . Take  $G \times T \rightarrow T$  and for any  $x \in T(\mathbb{F}_q)$  take the map

$$\begin{aligned} G &\rightarrow T \\ x &\mapsto gx. \end{aligned}$$

**Exercise (?)**

Prove this is an isomorphism. Hint: use the following diagram:




[Link to Diagram](#)

Let  $t \in T(\overline{\mathbb{F}}_q)$ , then any  $t' \in T(\overline{\mathbb{F}}_q)$  satisfies  $t' = gt$  for a unique  $g \in G(\overline{\mathbb{F}}_q)$ , since this is a principal homogeneous space (so the action is free and simply transitive). Consider Frobenius-fixed elements: take  $\sigma \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ , then if  $t' = (t')^\sigma$  then  $gt = g^\sigma t^\sigma$  and  $(g^\sigma)^{-1}t^\sigma = t^\sigma$ . Now  $t^\sigma = bt$  for a unique  $b \in G(\overline{\mathbb{F}}_q)$ , so to solve this equation it suffices to show that every  $b \in G(\overline{\mathbb{F}}_q)$  can be written in the form  $b = (g^\sigma)^{-1}g$ .

**Claim:** Consider the following funny action  $G \curvearrowright G$  by  $g \cdot t := (g^\sigma)^{-1}tg$ , a twisted conjugation. This acts transitively on  $G(\overline{\mathbb{F}_q})$  and thus has one orbit.

Why this implies the theorem: take  $t = \text{id}$ , then any  $b \in G(\overline{\mathbb{F}_q})$  is in the orbit of  $t$  and  $b = (g^\sigma)^{-1}g$ . ■

**Example 18.1.11(?)**: For  $G = \mathbb{G}_a$ , this yields  $g \cdot t = tg - g^p$ . For  $G = \mathbb{G}_m$  it yields  $g \cdot t = t - g^{1-p}$ . 

**Observation 18.1.12**

For fixed  $t \in G(\overline{\mathbb{F}_q})$ , the following map is generically étale:


$$\begin{aligned} G_{\overline{\mathbb{F}_q}} &\rightarrow G_{\overline{\mathbb{F}_q}} \\ g &\mapsto (g^\sigma)^{-1}tg, \end{aligned}$$

and thus the image contains an open subset of  $G_{\overline{\mathbb{F}_q}}$ . So any two orbits are open, and hence intersect since  $G$  is connected. Since orbits are equal or disjoint, there is just one orbit.

Proof: continued next time!

**Remark 18.1.13:** Some asides on philosophy: hyperbolicity should be related to having rational points, and having “big” fundamental group and being general type. A recent theorem by Ellenberg-Lawrence-Venketesh: for  $X \in \text{Var}/k$  for  $k \in \text{NumberField}$  and  $\pi_1 X$  is big, then  $\sharp X(\mathcal{O}_{k,S})$  has height bounded above by  $H$  which grows like  $H^\varepsilon$  for any  $\varepsilon$ .

See paper: <https://arxiv.org/abs/2109.01043>

Here “big  $\pi_1$ ” means that for  $X_{\mathbb{C}}$ , there is a variation of Hodge structure on  $X$  such that the map  $X \rightarrow \mathcal{D}/\Gamma$  into the period domain is quasi-finite. 


# 19 | Tuesday, November 02

**Remark 19.0.1:** Setup: let  $k \in \text{GlobalField}$ ,  $S \subseteq \text{Pl}(k)$  a finite set of places,  $\mathcal{G} \in \text{smGrpSch}/\mathcal{O}_{k,S}$  yielding a SES

$$0 \rightarrow \mathcal{G}^0 \rightarrow \mathcal{G} \rightarrow \mathcal{F} \rightarrow 0,$$

where  $\mathcal{F} \in \text{GrpSch}$  is finite étale. After base-changing to  $k$ , this yields a SES of groups

$$0 \rightarrow G^0 \rightarrow G \rightarrow F \rightarrow 0.$$

We defined  $H_S^1(k; G) := \left\{ \tau \in H^1(k; G) \mid \tau_{k_v} \in \text{im } \varphi \forall v \notin S \right\}$  where  $\varphi : H^1(\mathcal{O}_{k_v}; \mathcal{G}) \rightarrow H^1(k; \mathcal{G})$ . 

**Slogan 19.0.2**

General principal we'll use: there should only be finitely many things over  $\mathcal{O}_{k_S}$ , see Shafarevich's conjecture.

**Theorem 19.0.3 (?)**

- a.  $H_S^1(k; G) \rightarrow H_S^1(k; F) \rightarrow \prod_{v \in S} H^1(k_{\hat{v}}; F)$  has finite fibers, and
- b. If  $k$  is a number field, then  $H_S^1(k; G)$  is finite.

**19.1 Proof****19.1.1 Proof of a**

**Claim Step 1:** For  $v \notin S$ ,  $H^1(\mathcal{O}_v; \mathcal{F}) \rightarrow H^1(k_{\hat{v}}; F)$  is injective.

*Proof (Sketch).*

First consider a fiber that is a trivial torsor over  $\{\text{pt}\}$ .  $\mathcal{F}/\mathcal{O}_{k_{\hat{v}}} \in \mathbf{F}\text{-Torsors}$ . Why? Finite things are proper (finite iff proper and affine), so by the valuative criterion of properness  $\mathcal{F}(k_{\hat{v}})$  nonempty implies  $\mathcal{F}(\mathcal{O}_{k_{\hat{v}}})$  nonempty.

Now one can use a twisting argument to show that every fiber is finite. ■

**Claim Step 2:**  $H^1(\mathcal{O}_{k_{\hat{v}}}; \mathcal{G}^0)$ .

*Proof (of step 2).*

Let  $\kappa(v)$  be the residue field.

1. We know  $H^1(\kappa(v); \mathcal{G}^0|_{\kappa(v)}) = 1$  by Lang's theorem.
2. Let  $\tau \in H^1(\mathcal{O}_{k_{\hat{v}}}; \mathcal{G}^0)$  be a torsor. Now by the infinitesimal lifting criterion for smoothness, i.e. Hensel's lemma, if  $\tau(\kappa(v))$  is nonempty then  $\tau_{\mathcal{O}_{k_{\hat{v}}}}$  is nonempty.
3.  $H_S^1(k; G) \rightarrow H_S^1(k; F)$  has finite fibers. This uses input from a hard theorem which we'll black box here.

The proof is that  $H^1(\mathcal{O}_{k_{\hat{v}}}; \mathcal{G}) \rightarrow H^1(\mathcal{O}_k; \mathcal{F}) \hookrightarrow H^1(k; F)$ , where the first map is injective by (2) above, and the second by (1). Let  $\text{III}$  denote the Tate-Shafarevich group, then  $\ker h \subseteq \text{III}_S^1(k; G) := \ker \left( H^1(k; C) \rightarrow \prod_{v \in S} H^1(k; G_{k_{\hat{v}}}) \right)$  By Borel-Serre, for  $\mathcal{G}$  affine<sup>a</sup> the latter is finite.

Now a twisting argument shows this for every fiber.

**Claim:**  $H_S^1(k; \mathcal{F}) \rightarrow \prod_{v \in S} H^1(k_{\widehat{v}}; F_{k_{\widehat{v}}})$  has finite fibers.

*Proof (?)*

Now use the source of all finiteness in arithmetic geometry: Hermite-Minkowski's theorem, using that the previous information determines the degree and discriminant.

- Choose  $(\tau_v) \in \prod_v H^1(k_{\widehat{v}}; F_{k_{\widehat{v}}})$ , and suppose  $\tau \rightarrow (\tau_v)_{v \in S}$ . As a scheme,  $\tau = \text{Spec } R$  for  $R \in \text{Alg}/k$  finite étale, so  $R = \prod_i L_i$  with  $L_i$  unramified away from  $S$ . This bounds the discriminant, so there are finitely many possibilities for  $L_i$ .
- For each  $R$  there are finitely many  $F$  actions making  $\text{Spec } R$  into a torsor. Using representability, then  $F \rightarrow \underline{\text{Aut}}_k(R)$  is a finite étale group scheme. Since both are now finite, there are only finitely many such maps.

■

■

<sup>a</sup>(conjecturally for  $\mathcal{G}$  arbitrary, thought to be true but equivalent to BSD!),

### 19.1.2 Proof of b

**Remark 19.1.1:** For the proof of (b), it's enough to show that  $\prod_v H^1(k_{\widehat{v}}; F|_{k_{\widehat{v}}})$  is finite. Krasner's lemma shows that there are only finitely many degree  $d$  extensions over a  $p$ -adic field (false for  $\text{fp}((t))!$ ), so  $k_{\widehat{v}}$  has finitely many extensions. Then there are only finitely many extensions of  $k$  of a given degree, so there are only finitely many possibilities for  $F$ -torsors.

#### Exercise 19.1.2 (?)

Produce infinitely many extensions of  $\text{fp}((t))$ .

**Remark 19.1.3:** Note: étale is stronger than smooth? In the following proof, we could take everything to be étale to simplify things.

**Remark 19.1.4:** Reminder of setup: let  $X \in \text{Var}/k$  be proper,  $G \in \text{smGrpSch}/k$  finite,  $T \in \text{G-Torsors}/X$ . We're trying to show that  $\text{Sel}_{T/X}(k; G)$  is finite.

**Step 1:** spread out. There are finitely many denominators and thus finitely many places and  $\mathcal{G}$  finite smooth and  $\mathcal{O}_{k,S'}$  a group scheme with  $\mathcal{X}$  proper over  $\mathcal{O}_{k,S'}$ . Then  $\mathcal{T}/X$  is a  $\mathcal{G}$ -torsor with  $\mathcal{G}_k = G, \mathcal{T}_k = T, \mathcal{X}_k = X$ . Let  $\tau \in \text{Sel}_{T/X}(k; G)$ , then  $\tau \in H_{S'}^1(k; G)$  since  $\tau_{k_{\widehat{v}}}$  is in the image of  $X(k_{\widehat{v}}) \rightarrow H^1(k_{\widehat{v}}; G_{k_{\widehat{v}}})$ , but  $X(k_{\widehat{v}}) = \mathcal{X}(\mathcal{O}_{k_{\widehat{v}}})$  by the valuative criterion of properness. So for a number field, the set we want is contained in a finite set and we're done in this case.

For function fields, consider  $\tau \in \text{Sel}_{T/X}(k; G) \subseteq \text{im} \left( H_{S'}^1(k; G) \rightarrow \prod_{v \in S'} H^1(k_{\widehat{v}}; F) \right)$ , and let  $\pi$  be the inclusion. The claim is that  $\pi$  has finite image. The proof is by the local constancy lemma applied to  $X(k_{\widehat{v}}) \rightarrow H^1(k_{\widehat{v}}; G/G^0)$ , which is essentially Krasner's lemma plus compactness – here we used that  $X(k_{\widehat{v}})$  is compact. Finite image plus finite fibers implies finite, so we're done.

## 19.2 Misc

### Theorem 19.2.1 (Minchev).

Let  $k \in \text{NumberField}$ ,  $X, Y \in \text{Var}/k$  geometrically integral,  $F : Y \rightarrow X$  finite étale and not an isomorphism, and let  $S \subseteq \text{Pl}(k)$  be a finite set of places and suppose  $X(\mathbb{A}^S) \neq \emptyset$ . Then  $X$  does not satisfy strong approximation, i.e.  $X(k) \hookrightarrow X(\mathbb{A}^S)$  is not dense.

### Corollary 19.2.2 (?).

If  $X$  is geometrically integral and  $\pi_1^{\text{ét}}(X_{\bar{k}}) \neq 1$ , then  $X(\mathbb{A}^S)$  nonempty implies  $X$  does not satisfy strong approximation (since  $X$  admits no interesting étale covers)

**Remark 19.2.3:** Goal: find  $v \notin S$  and  $U \in X(k_{\widehat{v}})$  open where  $U$  does not contain any  $k$ -points.

# 20 | Tuesday, November 09

**Remark 20.0.1:** The descent obstruction does not suffice!

### Theorem 20.0.2 (?).

There exists a nice  $X \in \text{Var}/\mathbb{Q}$  with  $X(\mathbb{A})^{\text{ét, Br}} \neq \emptyset$  but  $X(\mathbb{Q}) = \emptyset$ .

**Remark 20.0.3:**  $X$  will be a quadric 3-fold bundle over a curve  $C$  with  $\sharp C(\mathbb{Q}) = 1$  with 2 singular fibers. By the Lefschetz hyperplane theorem, we'll be able to understand its  $\pi_1$ , even though this won't be a Serre fibration and thus we won't get a LES in homotopy.

## 20.1 Proof

**Remark 20.1.1:** First make  $Y$ , a quadric 3-fold bundle over  $\mathbb{P}_{\mathbb{Q}}^1$  with 2 singular fibers. Since we're fibering over  $\mathbb{P}^1$ , we'll define this in two affine patches and then glue. Define

$$Y_t := \left\{ t(t-1)x_0^2 + x_1^2 + \cdots + x_4^2 = 0 \right\} \subseteq \mathbb{A}_{/t}^1 \times \mathbb{P}_{/[x_0, \dots, x_4]}^1$$

$$Y_T := \left\{ (1-T)X_0^2 + x_1^2 + \cdots + x_4^2 = 0 \right\} \subseteq \mathbb{A}_{/T}^1 \times \mathbb{P}_{/[x_0, \dots, x_4]}^1.$$



Then define a gluing by

$$\begin{aligned} t &\mapsto \frac{1}{T} \\ x_i &\mapsto x_i, \quad i = 1, \dots, 4 \\ x_0 &\mapsto \frac{T}{X_0}. \end{aligned}$$

Now check that  $Y_0, Y_1$  are singular, and  $Y_\infty = \{\sum x_i^2 = 0\}$ :



*Something about  $(\mathbb{C}^\times \times Q)/\{\pm 1\} \rightarrow \mathbb{C}^\times$ ? This makes the geometry in this situation easy.*

Since  $Y_\infty(\mathbb{R}) = \emptyset$  implies  $Y_\infty(\mathbb{Q}) = \emptyset$ . Note that if  $t = 0, 1$  this is a point, for  $0 < t < 1$  this is an ellipsoid, and for  $t > 1$  or  $t < 0$  there are no real points.

**Remark 20.1.2:** Issue:  $\mathbb{P}^1$  has lots of rational points, so we'll make a curve  $C$  with a map  $C \rightarrow \mathbb{P}^1$  and pull back. Let  $C/\mathbb{Q}$  be a smooth proper curve such that

- $\#C(\mathbb{Q}) = 1$ , so write  $c := C(\mathbb{Q})$  as this single rational point. Write  $U \subseteq C(\mathbb{R})$  as the connected component of the identity. The real points are compact 1-manifolds, so a disjoint union of circles whose number depends on  $g(C)$ . Fun question: what is  $\pi_0 \mathcal{M}_g(\mathbb{R})$ ?
- $C \xrightarrow{f} \mathbb{P}^1$  such that
  - $f(c) = \infty$  such that
  - $f$  is étale at  $c$  and also over  $0, 1 \in \mathbb{P}^1(\mathbb{Q})$ .
  - $f(U) \ni 1$ .

**Example 20.1.3 (?):**  $y^2 = x^3 - 3$  is such a curve, see LMFDB.

- Probably the point is  $\infty$ !

- Pick a uniformizer at  $\infty$ , then compose with an affine map  $z \mapsto az + b$  to obtain the 2nd condition.
- $f(U)$  contains an open subset of  $\mathbb{P}^1(\mathbb{R})$ , using that  $f$  is étale and thus a local homeomorphism, so apply the implicit/inverse function theorems. So compose with a generic  $z \mapsto z + 1$  such that  $f(U) \ni 1$ . This doesn't mess up the previous affine map, since it's generic.

Now define  $X := Y \times_{\mathbb{P}^1} C$  as the pullback.

**Claim:**  $X(\mathbb{Q}) = \{\infty\}$ .

*Proof (?)*.

Note

$$X(\mathbb{Q}) \xrightarrow{\pi} C(\mathbb{Q}),$$

and  $\pi^{-1}(c) \cong Y_\infty$  which has no rational points. ■


## 20.2 Showing $X(\mathbb{A})^{\text{ét}, \text{Br}}$

**Remark 20.2.1:** Next goal: show the étale-Brauer set is empty.

**Example 20.2.2 (?):** We can show  $X(\mathbb{A})^{\text{Br}} \neq \emptyset$ .

1. An exercise using the Leray spectral sequence shows there is a surjection  $\text{Br}(C) \rightarrow \text{Br}(X)$ .
2. Observe that  $x \in X(\mathbb{A})$  is also in  $X(\mathbb{A})^{\text{Br}}$  if
  - $\pi(x_\infty) \in C(\mathbb{Q}_v)$  is equal to  $C$  for all finite  $v$ .
  - $\pi(x_\infty) \in U$ .
3. Find such a  $(x_v) \in X(\mathbb{A})$ .
  - For  $v$  finite, choose  $x_v \in Y_\infty(\mathbb{Q}_v)$ . Then  $\{[x_0 : \cdots : x_n] \mid \sum x_i = 0\} \neq \emptyset$ .
  - For  $v$  infinite, choose any  $c'$  lying over  $1 \in \mathbb{P}^1$ , so  $c' \in U \cap f^{-1}(1)$ . Then  $X_{c'} \cong Y_1$  but  $Y_1(\mathbb{R}) \neq \emptyset$  since it contains  $p = [1 : 0 : \cdots : 0]$ .


Why (2) is true: for  $v$  finite,  $\text{inv}_v(x_v^* \alpha) = \text{inv}_v(\pi(x_v)^* \alpha') = \text{inv}_v(c^* \alpha')$  where  $\alpha \in \text{Br}(X)$ ,  $\alpha = \pi^* \alpha'$ ,  $\alpha' \in \text{Br}(C)$ , and the same holds for  $v$  replaced by  $\infty$ . Use that this function is constant on  $U$  since it's connected. Now  $\sum_v \text{inv}_v(x_v^* \alpha) = \sum_v \text{inv}_v(c^* \alpha') = 0$ , which shows it's in the Brauer set.

**Remark 20.2.3:** So the Brauer-Manin obstruction it not sufficient to obstruct rational points. 

## 20.3 Étale-Brauer-Manin Set

**Remark 20.3.1:** Recall the definition:

$$X(\mathbb{A})^{\text{ét,Br}} := \bigcap_{\substack{T \in H^1(X; G) \\ G \text{ finite étale}}} \bigcup_{\tau \in H^1(k; G)} \text{im} \left( T^\tau(\mathbb{A})^{\text{Br}} \rightarrow X(\mathbb{A}) \right).$$

Let  $(x_v) \in X(\mathbb{A})$  as above. 

**Claim:** For each finite étale  $G$  and each  $T \in H^1(X; G)$  there exists a  $\tau \in H^1(k; G)$  such that  $(x_v)$  lifts to  $T^\tau(\mathbb{A})^{\text{Br}}$ .

*Proof (?)*

In steps:

1. (SGA1)  $T$  is a pullback of  $\tilde{T} \in \mathbf{G}\text{-Torsors}/C$ , using that  $\pi_1 X = \pi_1 C$ .
2. There exists a  $\tau \in H^1(k; C)$  such that  $c \in C(\mathbb{Q})$  lifts to  $\tilde{c} \in \tilde{T}^\tau(\mathbb{Q})$ .
3. For  $v$  finite, use the diagram:

$$\begin{array}{ccc} T^\tau(\mathbb{Q}_v) & \longrightarrow & X(\mathbb{Q}_v) & \ni x_v \\ \downarrow & & \downarrow & \\ \tilde{c} \in \tilde{T}^\tau(\mathbb{Q}_v) & \longrightarrow & C(\mathbb{Q}_v) & \end{array}$$

[Link to Diagram](#)

Then  $T_{\tilde{c}}^\tau \cong X_c$  implies  $x_v$  lifts.

4. For  $v$  infinite, we have  $x_\infty \in Y_1(\mathbb{R}) = X_{c'}(\mathbb{R})$ .
  - Check that  $c'$  lifts to  $c'' \in \tilde{T}^\tau(\mathbb{R})$  in the same connected component of  $\tilde{c}$ . This is because  $\tilde{T}^\tau(\mathbb{R}) \rightarrow C(\mathbb{R})$  is étale, and thus locally a covering map and thus surjective on any nonempty component. Thus  $T_{c''}^\tau \cong X_{c'}$  and thus  $x_\infty$  lifts.

■

# 21 | Chabauty-Coleman (Thursday, November 11)

## Theorem 21.0.1 (Coleman-Chabauty).

For  $X \in \text{Sch}/\mathbb{Q}$  a proper curve with  $g(X) \geq 2$  and  $\text{rank}_{\mathbb{Z}} \text{Jac}(X)(\mathbb{Q}) < g$  where  $X$  has good reduction at  $p > 2g$ ,  $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2$

**Remark 21.0.2:** Idea: choose  $x \in X(\mathbb{Q})$ , define a map

$$\begin{aligned} \text{AJ}_x : X &\xrightarrow{\text{Abel-Jacobi}} \text{Jac}(X) \\ y &\mapsto [\mathcal{O}(y - x)]. \end{aligned}$$

Then  $X^n \rightarrow \text{Jac}(X)$  by  $\mathbf{y} \mapsto \sum \text{AJ}_x(y_i)$  is surjective for  $n \geq g$ . Note that

$$\text{Hom}(T, \text{Jac}(X)) = \left\{ \mathcal{L} \in \text{Pic}(X \times T) \mid \mathcal{L} \text{ has degree 0 on each fiber of } X \times T \rightarrow T \right\} / \text{Pic}(T)$$

This equals  $\left\{ \mathcal{L} \in \text{Pic} X \times X \mid \mathcal{L} \text{ has fiberwise degree 0} \right\} / \text{Pic}(X)$ . Note that the LHS is  $\mathcal{O}(\{x\} \times X \rightarrow \Delta)$ .

**Claim:** For  $X^n \xrightarrow{\sum \text{AJ}_x} \text{Jac}(X)$  is surjective for  $n \geq g$ .

*Proof (?)*.

ETS that the following map is surjective:

$$\begin{aligned} X^n &\rightarrow \text{Pic}^n(X) \\ \mathbf{y} &\mapsto \mathcal{O}\left(\sum y_i\right). \end{aligned}$$

Given  $[\mathcal{L}] \in \text{Pic}^n(X)$ , for  $\mathcal{L} = \mathcal{O}(D)$  for  $D$  effective iff  $H^0(\mathcal{L}) \neq 0$ , so ETS  $H^0(\mathcal{L} \neq 0)$  for  $\deg \mathcal{L} \geq g$ . By Riemann-Roch:

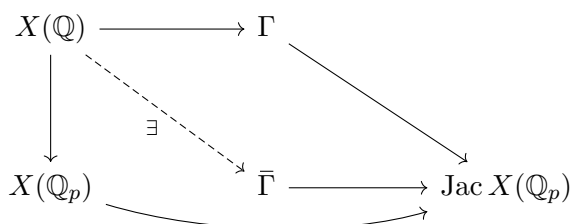
$$\dim H^0(\mathcal{L}) - \dim H^1(\mathcal{L}) = \deg \mathcal{L} + 1 - g.$$

The RHS is 1, so  $\dim H^0(\mathcal{L}) \geq 1$ . ■

## Slogan 21.0.3

$X$  generates  $\text{Jac}(X)$ , and  $\text{Jac}(X)$  is the Albanese of  $X$ .

**Remark 21.0.4:** Let  $\Gamma = \text{Jac } X(\mathbb{Q}) \subseteq \text{Jac } X(\mathbb{Q}_p)$ . We have a factorization:



[Link to Diagram](#)

Here  $\bar{\Gamma}$  has  $\dim n < g$  and  $\text{Jac } X(\mathbb{Q}_p)$  has dimension  $g$ . A fact from  $p$ -adic Lie groups: they're all direct sums of balls!

Now construction functions on  $\text{Jac } X(\mathbb{Q}_p)$  vanishing on  $\bar{\Gamma}$ . Then  $f_i|_{X(\mathbb{Q}_p)}$  vanish on  $X(\mathbb{Q}_p) \cap \bar{\Gamma} \supseteq X(\mathbb{Q})$ .

This will show  $X(\mathbb{Q})$  is finite. We'll show that not all of the  $f_i$  are identically zero: ETS that  $X(\mathbb{Q}_p) \not\subseteq \bar{\Gamma}$ , which will be true since  $X$  generates its Jacobian. Take whichever  $f_i \neq 0$ , which is a  $p$ -adic analytic function, then  $f_i$  will have finitely many zeros.

**Remark 21.0.5:** There is a hypothesis that  $\text{rank}_{\mathbb{Z}} \text{Jac } X(\mathbb{Q}) < g$  can be replaced by  $\dim \bar{\Gamma} < g$ .

## 21.1 Proofs

**Lemma 21.1.1 (?)**  
 Let  $\Gamma \leq A(\mathbb{Q}_p)$  be a finitely-generated abelian subgroup for  $A \in \text{AbVar}$ . Then  $\dim_{\mathbb{Q}_p} \bar{\Gamma} \leq \text{rank}_{\mathbb{Z}} \Gamma$ .

**Fact 21.1.2**  
 Any  $p$ -adic manifold  $X$  is locally isomorphic to  $\mathbb{Z}_p^{\times \dim X}$ .

*Proof (?)*  
 For  $\Gamma' \subseteq \mathbb{Z}_p^{\times n}$  a finitely-generated abelian group,  $\dim \bar{\Gamma}' \leq \text{rank}_{\mathbb{Z}} \Gamma'$ . Pick generators  $g_1, \dots, g_n$  generators, then write a linear map

$$\begin{aligned}
 \gamma : \mathbb{Z}_p^r &\rightarrow \mathbb{Z}_p^n \\
 e_i &\mapsto g_i.
 \end{aligned}$$

The image is closed of dimension  $n = \text{rank } \gamma$ . We'll now reduce the original lemma to proving this statement. This is because any *abelian*  $p$ -adic Lie group is of the form  $\mathbb{Z}_p^{\times n} \times$  something finite for some  $n$ . If  $A$  has good reduction at  $p$ , then  $A(\mathbb{Q}_p) \cong \mathbb{Z}_p \times A(\mathbb{F}_p)$ . Recall

that there are maps:

$$\begin{aligned}\exp : T_0 A(\mathbb{Z}_p) &\rightarrow A(\mathbb{Q}_p) \\ \log : \text{sp}^{-1}(0) &\rightarrow A(\mathbb{Z}_p),\end{aligned}$$

where  $\text{sp}$  is the specialization map, and this induces an isomorphism of abelian groups. The goal is to now construct a  $p$ -adic analytic function on  $A(\mathbb{Q}_p)$  vanishing on  $\bar{\Gamma}$ . This construction: due to Coleman. Fix  $\omega \in H^0(A_{\mathbb{Q}_p}, \Omega_{A/\mathbb{Q}_p}^1)$ , then there exists a  $p$ -adic analytic function

$$\begin{aligned}A(\mathbb{Q}_p) &\rightarrow \mathbb{Q}_p \\ Q &\mapsto \int_0^Q \omega.\end{aligned}$$

This map is determined by

- $Q \rightarrow \int_0^Q \omega$  is a morphism of topological groups,
- FTC: locally near 0, if  $f$  is a  $p$ -adic analytic function with  $\omega = df$ , then  $\int_0^Q \omega = f(Q) - f(0)$ .

■

**Remark 21.1.3:** Take  $\bar{\Gamma} \subseteq \mathbb{Q}_p$ , then for  $U := \bar{\Gamma} \in B_0$  a ball around the origin, consider  $\log(U) \subseteq T_Q(A) = \mathbb{Q}_p^{\times n}$ . Let  $v_1, \dots, v_s \subseteq \mathbf{T}_0^\vee A$  be dual vectors vanishing on  $\log \bar{\Gamma}$ . Then

- $\mathbf{T}_0^\vee A \cong H^0(A, \Omega_A^1)$
- $f_i(Q) = \int_0^Q v_i$ , viewing  $v_i$  as a 1-form.

## 22 | The Mordell Conjecture (Tuesday, November 23)

**Theorem 22.0.1 (Faltings).**

For  $K \in \text{NumberField}$  and  $X/k$  a smooth curve of genus  $g \geq 2$ . Then

$$\#X(k) < \infty.$$

**Example 22.0.2 (?):** Consider

$$x^n + y^n = 1.$$

Note that finiteness of rational points here is a weak form of Fermat: scaling out the denominators yields a rational solution to FLT. This has finitely many rational solutions for  $n \geq 4$ , which ensures

$g \geq 2$ .

Another example is  $C \subseteq \mathbb{P}^2$  a smooth curve, then we have finiteness when  $\deg C \geq 4$ .

**Remark 22.0.3:** Strategy of proof: finite map with finite fibers, a standard way to prove a set is finite. Note that Faltings proved a number of other famous conjectures along the way to proving this:

**Theorem 22.0.4 (Shafarevich for curves).**

Let  $K \in \text{NumberField}$  and  $S \subseteq \text{Pl}(k)$  a finite set of places. The set of proper curves over  $k$  of genus  $g$  with good reduction outside of  $S$  is finite after modding out by isomorphism.

**Remark 22.0.5:** Rephrasing:  $\mathcal{M}_g$  Deligne-Mumford stack, i.e. the functor sending a ring  $R$  to the groupoid of smooth proper curves over  $R$ , has finitely many  $\mathcal{O}_{k,S}$  points:

$$\#\mathcal{M}_g(\mathcal{O}_{k,S}) < \infty.$$

Note the stark contrast for  $\mathbb{Q}$ , where  $\mathcal{M}_2(\mathbb{Q})$  has infinitely many points: take

$$E := \{y^2 = x(x-1)f(x)\} \quad \deg f = 3 \text{ separable}$$

where  $0, 1$  are not roots of  $f$ . This produces an infinite family of genus 2 curves.

**Remark 22.0.6:** The Shafarevich conjecture for curves implies Mordell: fix  $S$  such that  $X$  has a smooth proper model  $\mathcal{X}/\mathcal{O}_{k,S}$  with  $X(k) = \mathcal{X}(\mathcal{O}_{k,S})$ . Then we win if we can find a finite morphism  $\mathcal{X} \hookrightarrow \mathcal{M}_{g'}/\mathcal{O}_{k,S}$  for some  $g'$ . Note that if these were affine, this would be impossible. The existence of such maps is the **Kodaira-Parshin trick**:

- Over  $\mathbb{C}$ , existence was given by Kodaira,
- Over  $k$ , existence due to Parshin.

Faltings' (and others') proof pass though this trick.

**Remark 22.0.7:** Note that a special case of Shafarevich was proved by Faltings, Shafarevich proved it for all curves. Recent results along these lines: proving  $\mathcal{O}_{k,S}$  points are not Zariski-dense, or are finite, for other interesting moduli spaces.

**Theorem 22.0.8 (Shafarevich for abelian varieties).**

For  $k \in \text{NumberField}$ ,  $S \subseteq \text{Pl}(k)$  finite, and  $g, d > 0$ , the set of isomorphism classes of abelian varieties of dimension  $g$  with a polarization of degree  $d$  over  $k$  with good reduction outside of  $S$ , is finite. Then

$$\#\mathcal{A}_{g,d}(\mathcal{O}_{k,S}) < \infty.$$

**Remark 22.0.9:** Line bundles are maps to Picard,  $d$  is the degree. For  $d = 1$ , these are principally polarized.

**Remark 22.0.10:** It's enough to consider the case  $d = 1$ , which is not obvious – this is referred to as Zahrin's trick, and shows  $A, A^8$  always has a polarization of degree 1. Then Shafarevich for AVs implies Shafarevich for curves, using the Torelli map:

$$\begin{aligned} \mathcal{M}_g &\rightarrow \mathcal{A}_g \\ [C] &\mapsto [\text{Jac}(C), \Theta]. \end{aligned}$$

This is a finite map!

**Definition 22.0.11** (Tate Modules)

$A \in \text{AbVar}/_k$  and  $\ell$  some prime, the  $\ell$ -adic Tate module of  $A$  is defined as

$$T_\ell(A) := \varprojlim_n A[\ell^n](\bar{k}) \cong \mathbb{Z}_\ell^{\times 2g},$$

and  $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ .

**Remark 22.0.12:** Recall that finite generation of a field is being finitely generated over a prime field.

**Theorem 22.0.13** (*Tate Conjecture*).

For  $A_1, A_2 \in \text{AbVar}/_k$  with  $k$  finitely generated,

1.  $V_\ell(A_i)$  are semisimple Galois representations.
2. After tensoring homs with  $\mathbb{Z}_\ell$ , we get an isomorphism of  $\mathbb{Z}_\ell$ -modules:

$$\text{Hom}_k(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \text{Hom}(T_\ell(A_1), T_\ell(A_2)) \otimes \mathbb{Z}_\ell.$$

**Remark 22.0.14:** Part 1 is already very deep, it's a special case of a conjecture we know almost nothing about. In fact, it's false over  $\mathbb{Q}_p$ : take

$$E : y^2 = x(x-1)(x-p) \quad /\mathbb{Q}_p.$$

This has multiplicative reduction. Similarly, take

$$E : y^2 = x(x-1)(x-t) \quad /\mathbb{C}(t),$$

since the monodromy matrix  $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$  is not diagonalizable. Note that  $\overline{\mathbb{C}(t)}$  are the Puiseux series  $P$ . Any topological generator of  $\text{Gal}(P/\mathbb{C}(t)) \cong \widehat{\mathbb{Z}}(1)$  acts on  $T_\ell(A)$  by a matrix conjugate to this.

**Remark 22.0.15:** The general conjecture that we know almost nothing about:

**Conjecture 22.0.16.**

For  $X/k$  smooth proper,

1.  $G_k \curvearrowright H^i(X_{\bar{k}}; \mathbb{Q}_\ell)$  semisimply.
2.  $\text{CH}^i(X) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow H^{2i}(X_{\bar{k}}; \mathbb{Q}_\ell(i))^{G_k}$  is surjective.



**Remark 22.0.17:** Extremely hard problems! Probably Fields material.

**Theorem 22.0.18 (Main difficult ingredient).**

For  $A \in \text{AbVar}/_k$ , there exist only finitely many isomorphism classes of abelian varieties over  $k$  isogenous to  $A$ .

*Proof (Sketch/idea).*

Take  $X/_k$  smooth proper with  $g(X) \geq 2$  and good reduction outside of  $S$ . For  $\ell$  a prime, there is a map

Define

- $\mathcal{M}_{g'}(\mathcal{O}_{k,S}) = \{\text{Curves of genus } g' \text{ over } k \text{ with good reduction outside } S\} / \sim$  and

$$\text{KP} : X(k) \rightarrow \mathcal{M}_{g'},$$

corresponding to the Kodaira-Parshin trick.

- $\mathcal{A}_{g'}(\mathcal{O}_{k,S})$  for the PPAVs of dimension  $g'$  with good reduction outside of  $S$  (mod isomorphism).
- $\text{Rep}_{2g'}(G_{k,S \cup \{\ell\}})$  for the set of semisimple  $\mathbb{Q}_\ell$  Galois representations of rank  $2g'$  and *weight*  $-1$  unramified outside of  $S \cup \{\ell\}$  such that the characteristic polynomials of Frobenius (a conjugacy class) outside of  $S \cup \{\ell\}$  have integer coefficients.

Here  $\ell$  is the ambient prime. Weight  $-1$  means the eigenvalues of Frobenius are algebraic numbers  $\alpha$  where any embedding  $\mathbb{Q}(\alpha_j) \hookrightarrow \mathbb{C}$  and  $|\alpha| = |k(v)|^{\frac{1}{2}}$ . Frobenius having integer coefficients comes from the Weil conjectures.

Assembling these, we get a chain of maps

$$X(k) \xrightarrow{\text{KP}} \mathcal{A}_{g'}(\mathcal{O}_{k,S}) \xrightarrow{\text{Jac}} \mathcal{A}_{g'}(\mathcal{O}_{k,S}) \xrightarrow{V_\ell} \text{Rep}_{2g'}(G_{k,S \cup \{\ell\}}; \mathbb{Q}_\ell),$$

which we claim all have finite fibers, and the last set is finite:


- KP has finite fibers by construction
- Jac has finite fibers by the Torelli theorem
- $V_\ell$  has finite fibers, which is more difficult. By the Tate conjecture, the fiber over a representation in  $V$  are isogenous AVs over  $k$ , but such sets are finite.

■

**Theorem 22.0.19 (?).**

$$\#\text{Rep}_N(G_{k,S}; \mathbb{Q}_\ell) < \infty.$$

**Remark 22.0.20:** We'll discuss this in detail next time, but the idea is that representations are determined by traces of group elements. For  $\Gamma \xrightarrow{\rho} \text{GL}(V)$  a representation over  $\text{ch } k = 0$ , the semisimplification  $\rho^{\text{ss}}$  is determined by  $\text{Tr} \circ \rho$ . We can use that Frobenii are dense, and it's enough to determine this representation on a dense set, so we consider  $\text{Tr}(\rho(\text{Frob}))$ . This is still an infinite set,

so we have to argue that finitely many determine it, but this comes from the bound on eigenvalues. 

## 23 | Tuesday, November 30

### 23.1 Faltings Theorem

#### Definition 23.1.1 (?)

Write  $\text{Rep}_N^*(G_{k,S}; \mathbb{Q}_\ell)$  for semisimple continuous representation  $G_{k,S \cup \{\ell\}} \rightarrow \text{GL}_n(\mathcal{O}_\ell)$  of weight -1 such that for all  $v \in S \cup \{\ell\}$ , the characteristic polynomial of  $\text{Frob}_v$  has integer coefficients. Note that the roots are  $\alpha_i \in \overline{\mathbb{Q}}$  such that  $\mathbb{Q}(\alpha_i) \hookrightarrow \mathbb{C}$  and  $|\alpha_i| = q^{\frac{i}{2}}$ .

#### Theorem 23.1.2 (Faltings).

$\#X(k) < \infty$ .

#### Theorem 23.1.3 (?).

$\text{Rep}_N^*(G_{k,S}, \mathcal{O}_\ell)$  is finite.

#### 23.1.1 Proof

#### Lemma 23.1.4 (A very important fact).

If  $\Gamma$  is a group and  $\Gamma \xrightarrow{\rho} \text{GL}_n(L)$  is a semisimple representation over  $L$  a field of characteristic zero. Then  $\rho$  is determined by  $\text{Tr} \circ \rho : \Gamma \rightarrow L$ , i.e. any two representations for which these composites agree differ by conjugacy.

#### Fact 23.1.5

$\rho \in \text{Rep}_N^*(G_{k,S}, \mathcal{O}_\ell)$  is determined by  $\left\{ \text{Tr} \circ \rho \circ \text{Frob}_v \mid v \in S \cup \{\ell\} \right\}$  since the Frobenii are dense in  $G_{k,S \cup \{\ell\}}$  by Chebotarev density.

#### Fact 23.1.6

Fix  $v \notin S \cup \{\ell\}$ , then there are only finitely many possibilities for  $\left| \text{Tr} \circ \rho \circ \text{Frob}_v \right| < N \cdot |\kappa(v)|^{\frac{1}{2}}$ , since traces of Frobenii are sums of eigenvalues.

**Remark 23.1.7:** This provides a finite set of Frobenii whose traces determine  $\rho$ . Given  $\rho_1, \rho_2$ , take the group ring of the Galois group and consider the map

$$\mathbb{Q}_\ell[G_{k,S \cup \{\ell\}}] \xrightarrow{\rho_1 \times \rho_2} \text{Mat}(n \times n; \mathbb{Z}_p)^{\times 2},$$

where we used that  $GL_n(\mathbb{Z}_p) \leq GL_n(\mathbb{Q}_p)$  is a maximal compact subgroup. The goal is to find a set of places  $T$  such that  $\left\{ (\rho_1, \rho_2)(\text{Frob}_v) \mid v \in T \right\}$  spans the image, which we can do since the RHS is a finite-dimensional  $\mathbb{Z}_p$  module.

**Remark 23.1.8:** Let  $\tilde{k}$  be the compositum of all extensions of  $k$  unramified outside of the set of bad places  $S \cup \{\ell\}$  of bounded degree  $\ell < 2n^2$ , the dimension of the RHS above. This is a finite extension by Hermite-Minkowski. Let  $\tilde{k}^{\text{cl}}$  be the Galois closure, and by Chebotarev choose  $T$  such that  $\left\{ \text{Frob}_v \right\}_{v \in T}$  cover all conjugacy classes of  $\text{Gal}(\tilde{k}^{\text{cl}}/k)$ .

**Claim:** For  $\rho_1, \rho_2 \in \text{Rep}_N^*(G_{k,S}; \mathcal{O}_\ell)$ , if  $\text{Tr}(\text{Frob}_v|_{\rho_1}) = \text{Tr}(\text{Frob}_v|_{\rho_2})$  for all  $v \in T$ , then  $\rho_1 \cong \rho_2$ .

*Proof (?).*

Consider  $\mathbb{Z}_\ell[G_{k,S}] \xrightarrow{(\rho_1, \rho_2)} \text{Mat}_{N \times N}(\mathbb{Z}_\ell)^{\times 2}$ , write  $M := \text{im}(\rho_1, \rho_2)$ . ETS that the images of  $\text{Frob}_v$  generate this as a  $\mathbb{Z}_\ell$  module. By Nakayama, it's enough to check that they generate  $M/\ell M$ . Note that  $\#(M/\ell M)^\times < \ell^{2N^2}$ , so write  $\tau : G_{k,S \cup \{\ell\}} \rightarrow (M/\ell M)^\times$ , then  $\tau$  factors through  $\text{Gal}(\tilde{k}^{\text{cl}}/k)$ . Then  $\text{im}(\left\{ \text{Frob}_v \mid v \in T \right\}) = \text{im } \tau$ . ■

## 23.2 The Kodaira-Parshin Trick

**Theorem 23.2.1 (Parshin).**

Let  $X$  be a curve over  $\mathcal{O}_{k,S}$ ,  $g(X) \geq 2$ . After potentially increasing  $k$  and  $S$ , there exists a finite map of algebraic varieties

$$X' \rightarrow \mathcal{M}_{g'}/\mathcal{O}_{k,S}$$

for some  $g'$  where  $X'$  is a finite étale cover of  $X$ .

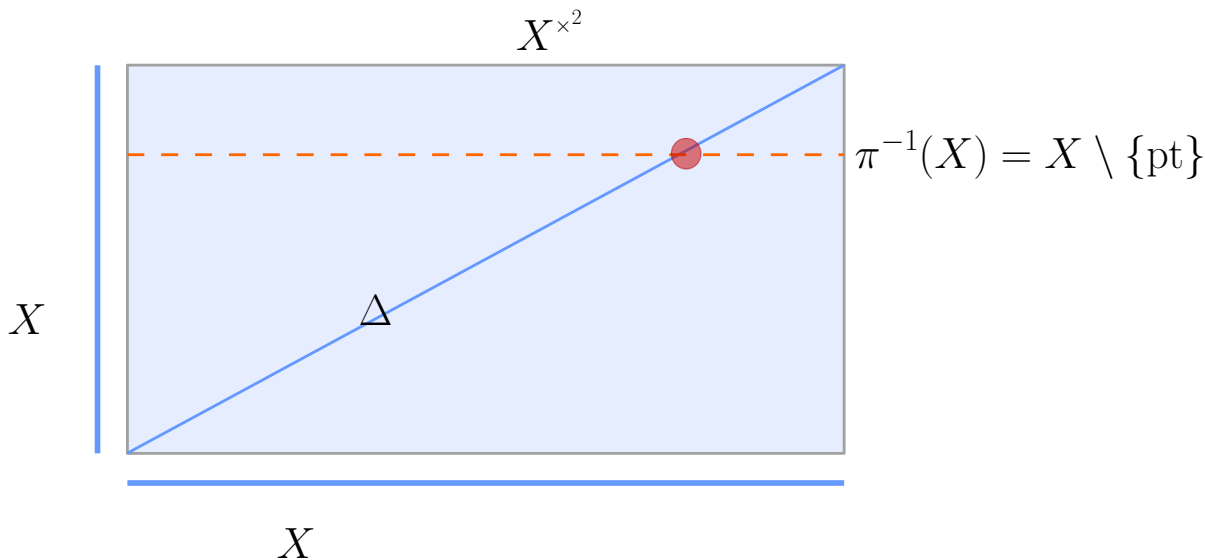
**Remark 23.2.2:** Note that  $\mathcal{M}_2$  is affine and can't contain a smooth proper curve. In general it isn't even proper, so it's difficult to map a proper thing into a non-proper thing. Note that the RHS is a stack over  $\mathcal{O}_{k,S}$ . Why compactify in general: argue something is an open condition, degenerate to the boundary where the objects are easier to work with and show it holds there and thus on an open containing it.

**Remark 23.2.3:** Note that  $\text{Hom}(X, \mathcal{M}_{g'})$  is the of smooth proper morphisms  $Y \rightarrow X$  over  $\mathcal{O}_{k,S}$  such that the geometric fibers are curves of genus  $g'$ . Take  $\mathcal{Y} \xrightarrow{\pi} X$  and  $x \in X$  such that  $\pi^{-1}(x)$  is a cover of  $X$  ramified only at  $x$ .

### Slogan 23.2.4

$X$  is a moduli space of branched covers of  $X$  branched only at a single point.

Idea: create a moduli space of such covers. Take  $\eta : X^{\times 2} \setminus \Delta \rightarrow X$  where the fiber over  $X$  is  $X \setminus \{x\}$ .



**Remark 23.2.5:** Over  $\mathbb{C}$ , note that  $X$  is covered by  $\mathbb{H}$  so  $\pi_2 X = 1$  and  $\eta$  is a fibration, so taking the LES in homotopy yields a SES

$$1 \rightarrow \pi_1(X \setminus \{pt\}) \rightarrow \pi_1(X^{\times 2} \setminus \Delta) \rightarrow \pi_1(X) \rightarrow 1.$$

Here  $\pi_1(X) = \langle a_1, b_1, \dots, a_g, b_g \mid \prod [a_i b_i] = 1 \rangle$ . Pick any  $\gamma : \pi_1(X \setminus \{pt\}) \rightarrow S_3$  which doesn't send the loop around the puncture to the identity, i.e.  $\gamma(\prod [a_i b_i]) \neq \text{id}$ . This now has ramification at a point.

Define  $\Gamma := \{g \mid \pi_1(X^{\times 2} \setminus \Delta) \mid \gamma^g \text{ is conjugate to } g\}$ , i.e. there exists  $h_g \in S_3$  such that for all  $x \in \pi_1(X \setminus \{pt\})$  we have  $\gamma(gxg^{-1}) = h_g \gamma(x) h_g^{-1}$  for all  $x \in \pi_1(X \setminus \{pt\})$ .

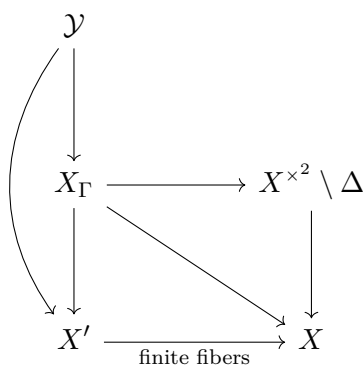
**Claim:**  $[\Gamma : \pi_1(X^{\times 2} \setminus \Delta)] < \infty$  has finite index and contains  $\pi_1(X \setminus \{pt\})$ .

**Claim:** This yields a group morphism

$$\begin{aligned} \Gamma &\rightarrow S_g \\ g &\mapsto h_g. \end{aligned}$$

**Remark 23.2.6:** Some words on why these are true: stabilizers of groups acting on finite sets have finite index, and the subgroup claim comes from sending  $h_g \rightarrow \gamma(g)$ .

**Remark 23.2.7:** The construction:



[Link to Diagram](#)

The fibers of  $\mathcal{Y} \rightarrow X$  are disjoint unions of covers of  $X$  ramified at  $x$ . Since we now have a family of curves,  $\mathcal{Y} \rightarrow X'$  yields a map  $X' \rightarrow \mathcal{M}_{g'/\mathbb{C}}$ .

**Claim:** This map is not constant.

**Remark 23.2.8:** Suppose all of the fibers are isomorphic to some fixed  $Y$  of a fixed genus, then  $\text{Hom}(Y, X)$  would be infinite. By Hurwitz, there's a bound on the degree of such a map since  $g(Y)$  is fixed, so there are only finitely many.  $\zeta$

**Remark 23.2.9:** To do everything over  $\mathcal{O}_{k,S}$ , we use  $\pi_1^{\text{ét}}$  instead of  $\pi_1$  and include  $2, 3 \in S$ . Since the map is unramified over  $\mathbb{C}$ , it's ramified at only finitely many primes, so just add those to  $S$ .

## 24 | Thursday, December 02

### 24.1 Setup

**Conjecture 24.1.1 (Tate conjecture, general).**

Let  $X \in \text{sm Proj Var}/_k$  for  $k$  a finitely generated field. Conjecturally the cycle class map is surjective:

$$\text{CH}^i(X)_{\mathbb{Q}_\ell} \twoheadrightarrow H^{2i}(X_{\bar{k}}; \mathbb{Q}_\ell(i))^{G_k}.$$

Replacing rational equivalence by *homological equivalence* is conjectured to yield a bijection, although this is closer to tautological – one quotients by the kernel of this map. A conjecture with more content: replacing rational equivalence with *numerical equivalence* yields a bijection, where one essentially quotients by the intersection pairing.

**Remark 24.1.2:** Recall that we're proving  $\#X(k) < \infty$ . Note

$$X(k) \xrightarrow{kP} \mathcal{M}_{g'}(\mathcal{O}_{k,S}) \xrightarrow{\text{Jac}} \mathcal{A}_{g'}(\mathcal{O}_{k,S}) \xrightarrow{V_\rho} \text{Rep}_{2g'}^*(G_{k,S}; \mathbb{Q}_\ell).$$

Last time we constructed KP and showed that  $\text{Rep}_{2g'}$  above is finite. The strategy: proving some finiteness statement, prove a special case of the Tate conjecture (generally widely open), then get a stronger finiteness result.

**Theorem 24.1.3 (Faltings, Tate conjecture for AVs over a number field).**

For  $A, B \in \text{AbVar}/_k$ ,  $k \in \text{NumberField}$ ,

1. The Tate modules  $V_\ell(A), V_\ell(B)$  are semisimple  $G_k$ -modules.
2. There is a bijection

$$\text{Hom}(A, B) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \text{Hom}_{G_k}(T_\ell(A), T_\ell(B)),$$

where the LHS are isogenies.

**Remark 24.1.4:** This won't be true for  $p$ -adic fields, but there is a version that works for finitely-generated fields, e.g. function fields of varieties defined over number fields.

**Theorem 24.1.5 (Faltings, a finiteness result).**

Isogeny classes over  $k$  are finite.

**Theorem 24.1.6 (Tate?).**

Faltings' finiteness result implies the Tate conjecture

**Remark 24.1.7:** The proof idea: use a **height** defined by Faltings:

$$\mathcal{A}_g(k) \rightarrow \mathbb{R}$$

satisfying

- For all  $N$ ,  $\#\{[A] \in \mathcal{A}_g(k) \mid h([A]) < n\}$  is finite.
- If  $A \sim B$  are isogenous, then  $|h(A) - h(B)| < C = C(A)$  a constant.

Note that these imply the finiteness result since  $\{h(B) \mid B \sim A\} < \infty$ . There is a general height machine theory here, which extends this theory to (nice, e.g. DM) stacks. Recent work is going into extending height theories to more complicated stacks, e.g. algebraic spaces.

## 24.2 Proof: Finiteness implies the Tate conjecture

**Claim:**  $\text{Hom}(A, B)$  is torsionfree.

*Proof (?)*.

This is because  $\text{Hom}(A, B) \hookrightarrow \text{Hom}(T_\ell(A), T_\ell(B))$  since the  $\ell^\infty$ -torsion points are dense, and the RHS is torsionfree. ■

**Claim:** There is a functor

$$T_\ell : \text{AbVar}/k \otimes \mathbb{Z}_\ell \rightarrow \text{Rep}_{G_k}$$

which is

- Faithful (and we'll want to show it's full)
- $\text{Hom}(A, B)$  is finitely generated.

*Proof (?)*.

The proof is essentially checking over  $\mathbb{C}$ . ■

**Claim:** The following cokernel is torsionfree:

$$\text{coker}(\text{Hom}(A, B) \otimes \mathbb{Z}_\ell \rightarrow \text{Hom}(T_\ell(A), T_\ell(B))).$$

*Proof (?)*.

Again, check over  $\mathbb{C}$ ! ■

**Claim:** The truth of the Tate conjecture is preserved under base change: given  $K/k$  a finite extension, the Tate conjecture for  $K$  implies the Tate conjecture for  $k$ .

*Proof (?)*.

Without loss of generality, let  $K'/k$  be finite Galois.

**Claim:** For semisimplicity, the claim is that if  $\Gamma' \leq \Gamma$  is a subgroup of finite index and  $\rho : \Gamma \rightarrow \text{GL}_n(\mathbb{Q}_\ell)$ , then if  $\rho|_{\Gamma'}$  semisimple implies  $\rho$  is semisimple.

*Proof (?)*.

Proof: get a splitting  $\rho \xrightarrow{s} \rho'$  and use an averaging argument on  $\Gamma/\Gamma'$  (a la Maschke's theorem). This works since  $\mathbb{Q}_\ell$  is positive characteristic. ■

**Claim:** For the homs, the claim is that  $\text{Hom}(A_{K'}, B_{K'}) \otimes \mathbb{Z}_\ell \rightarrow \text{Hom}(T_\ell(A), T_\ell(B))$  is bijective.

*Proof (?)*.

Noting that we already have injectivity over any field. Let  $\sigma \in \text{Hom}(T_\ell A, T_\ell B)$ , then there exists  $f : A \rightarrow B$  over  $k$  such that  $T_\ell(f) = \sigma$ . Since  $f$  is  $G_k$ -equivariant, we get density by Galois descent. ■

Reduce to  $A = B$  by using  $A \times B$ . Reduce to proving the following:

**Claim:** If  $W \subseteq V_\ell(A)$  is a Galois stable subspace, there exists a  $u \in \text{End}(A) \otimes \mathbb{Q}_\ell$  with  $u(V_\ell(A)) = W$ .

*Proof (?)*.

For semisimplicity, use that subrepresentations are continuous? Then use a double coset trick. ■

Reduce to showing this for  $W$  a maximal isotropic subspace for the Weil pairing (a symplectic form). This is Zahrin’s trick: replace  $A$  with  $A^{\times 4}$ , gives a way to “complete” any subspace  $W \subseteq T_\ell(A)$  to a maximal isotropic. The proof uses the Lagrange 4-squares theorem, how neat! Write

$$G_n := \frac{W \cap T_\ell(A) + \ell^n T_\ell(A)}{\ell^n T_\ell(A)} \subseteq A[\ell^n], \quad B_n := A/G_n.$$

Then if  $W$  is maximal isotropic,  $B_n$  is a PPAV and thus so is  $A$ . The actual theorem Tate proves:

**Theorem 24.2.1 (?)**.


It suffices to show that  $\{B_n\}_{n \geq 1}$  is finite.

*Proof (Idea)*.

Write  $A \xrightarrow{\psi_n} A/G_n = B_n$  and  $\psi_n^\vee : B_n \rightarrow A$ , and from the construction of  $G_n$  and unwinding definitions yields

$$\psi_n(T_\ell(B_n)) = W \cap T_\ell(A) + \ell^n T_\ell(A).$$

So  $\text{im}(\psi_n)$  is “converging” to  $W \cap T_\ell(A)$ . Use that eventually the  $B_n$  stabilize to compose  $\gamma_n : A \xrightarrow{\psi_n} B_n \xrightarrow{\psi_n^\vee} A$  and replace this with  $\gamma_n : A \rightarrow B \rightarrow A$ . Use that  $\text{End}(A) \otimes \mathbb{Z}_\ell$  is a compact space to get a convergent subsequence. ■

**Remark 24.2.2:** The upshot: there exist finitely many PPAVs isogenous to  $A$ . 

## 24.3 Faltings Heights



**Remark 24.3.1:** Write  $\tilde{\mathcal{A}} \rightarrow \mathcal{A} := \mathcal{A}_{\text{univ},g} \rightarrow \mathcal{A}_g$  for the universal family, and define a line bundle  $\mathcal{L} := \bigwedge^{\text{top}} s^* \Omega_{\tilde{\mathcal{A}}/\mathcal{A}}^1$ . A fact is that  $\mathcal{L}$  is ample, since there exists a compactification of  $\mathcal{A}_g$  to which  $\mathcal{L}$  is ample. This is a hard theorem and involves Siegel modular forms.

**Remark 24.3.2:** Define a height function associated to  $\mathcal{L}$ :

$$\tilde{h} : \mathcal{A}_g(\mathbb{Q}) \xrightarrow{\mathcal{L}} \mathbb{P}^N(\mathbb{Q}) \rightarrow \mathbb{R}$$

$$\left[ \frac{x_0}{x_i} : \dots : \frac{x_n}{x_i} \right] \mapsto \max(|x_i|, |x'_i|).$$

This is the height machine, but it's fairly incomputable.

**Remark 24.3.3:** A definition by Faltings: for  $A$  semisimple, write

$$H(A) = \prod_{k \rightarrow \mathbb{C}} \int_{A(\mathbb{C})} \eta \wedge \bar{\eta} \quad \eta \in H^0(\bar{A}/\mathcal{O}_K; \Omega_A^g),$$

taking a Néron model  $\bar{A}$  for  $A$ . Then define

$$h(A) = \frac{1}{[k : \mathbb{Q}]} \log(H(A)).$$

**Theorem 24.3.4 (Faltings).**

There exist constant  $c_1, c_2$  such that

$$|h(A) - \tilde{c}_1 h(A)| < c_2$$

where the  $c_i$  do not depend on  $A$ .

**Proposition 24.3.5 (?).**

For  $f : A \rightarrow B$  an isogeny induces  $\bar{A} \rightarrow \bar{B}$  on Néron models, and

$$h(B) - h(A) = \frac{1}{2} \log \deg(f) \cdot \frac{1}{[K : \mathbb{Q}]} \log \text{length } s^* \Omega_{/?}^1.$$

# 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? 7

Something about Hilbert 90 . . . . . 24

Check 2! . . . . . 37

Missing some stuff! Find notes. . . . . 61

# Definitions

3.2.1	Definition – Brauer Groups . . . . .	11
3.2.4	Definition – Group cohomology . . . . .	11
4.2.4	Definition – Galois cohomology . . . . .	14
4.2.5	Definition – Brauer Groups . . . . .	14
5.0.5	Definition – Reduced Complex . . . . .	16
5.2.1	Definition – Forms/descent, a pseudo-definition . . . . .	18
6.2.1	Definition – Torsor . . . . .	21
6.4.5	Definition – Brauer group . . . . .	23
7.1.4	Definition – Severi-Brauers . . . . .	24
7.1.6	Definition – CSAs/Azumaya Algebras . . . . .	25
7.1.8	Definition – Opposite algebra . . . . .	25
7.1.9	Definition – Morita equivalence . . . . .	25
7.2.2	Definition – Twisted vector spaces . . . . .	26
7.2.8	Definition – Index and period . . . . .	28
8.0.8	Definition – Reduced norm and trace . . . . .	31
8.0.11	Definition – Semilinear group rings . . . . .	31
9.1.10	Definition – ? . . . . .	36
10.2.4	Definition – Valuations on division algebras . . . . .	40
10.2.5	Definition – Valuation ring . . . . .	41
11.1.2	Definition – Cyclic Algebra . . . . .	43
11.2.3	Definition – Ideles . . . . .	45
11.2.5	Definition – S-ideles . . . . .	46
12.2.7	Definition – Herbrand Quotient . . . . .	49
13.1.2	Definition – Quadratic forms representing elements . . . . .	54
15.0.7	Definition – Symbol Algebra . . . . .	60
16.0.2	Definition – ? . . . . .	61
16.1.1	Definition – fppf morphisms . . . . .	62
16.1.3	Definition – ? . . . . .	62
16.1.4	Definition – $G$ -torsors . . . . .	62
17.1.1	Definition – Selmer Sets . . . . .	66
18.1.3	Definition – ? . . . . .	67
22.0.11	Definition – Tate Modules . . . . .	80
23.1.1	Definition – ? . . . . .	82

# Theorems

2.1.10	Theorem – ?	7
3.0.2	Theorem – Lang-Weil Estimates	8
4.1.5	Proposition – ?	13
5.0.2	Proposition – ?	16
5.1.1	Proposition – Spectral Sequences	17
5.1.3	Proposition – Inflation/Restriction Exact Sequence	17
5.2.6	Proposition – ?	18
6.1.2	Theorem – A meta-theorem	20
6.2.2	Theorem – ?	21
6.3.2	Theorem – ?	21
6.4.7	Theorem – ?	24
7.1.7	Theorem – Classification of CSAs	25
7.1.10	Theorem – ?	25
7.2.5	Proposition – Properties of categories of twisted vector spaces	27
7.2.6	Proposition – ?	27
7.2.7	Theorem – ?	27
8.0.2	Theorem – ?	29
8.0.3	Theorem – ?	29
8.0.9	Proposition – ?	31
8.0.10	Theorem – ?	31
8.1.2	Theorem – ?	32
8.1.5	Theorem – Tsem	32
9.0.2	Theorem – Hasse principle for Severi Brauers	33
9.1.7	Theorem – ?	35
10.1.2	Proposition – ?	38
10.1.3	Theorem – ?	38
10.1.5	Theorem – Hasse	40
11.1.5	Theorem – ?	44
11.2.2	Proposition – ?	45
11.2.8	Proposition – ?	46
11.2.9	Theorem – ?	46
12.2.1	Theorem – Injectivity	48
12.2.2	Theorem – Actual IRL application of Sylow theorems	49
12.2.5	Theorem – ?	49
13.0.1	Theorem – ?	51
13.0.3	Theorem – ?	52
13.0.6	Theorem – ?	54
13.1.1	Theorem – Hasse-Minkowski	54
13.1.3	Theorem – a stronger one	54
14.0.2	Theorem – ?	55
14.0.4	Theorem – ?	56

15.0.1	Proposition – ?	57
15.0.4	Proposition – ?	58
17.0.5	Proposition – ?	64
17.0.9	Proposition – Local constancy of evaluation	65
18.0.2	Theorem – ?	66
18.1.4	Theorem – ?	68
18.1.8	Theorem – ?	68
19.0.3	Theorem – ?	70
19.2.1	Theorem – Minchev	72
20.0.2	Theorem – ?	72
21.0.1	Theorem – Coleman-Chabauty	76
22.0.1	Theorem – Faltings	78
22.0.4	Theorem – Shafarevich for curves	79
22.0.8	Theorem – Shafarevich for abelian varieties	79
22.0.13	Theorem – Tate Conjecture	80
22.0.18	Theorem – Main difficult ingredient	81
22.0.19	Theorem – ?	81
23.1.2	Theorem – Faltings	82
23.1.3	Theorem – ?	82
23.2.1	Theorem – Parshin	83
24.1.3	Theorem – Faltings, Tate conjecture for AVs over a number field	86
24.1.5	Theorem – Faltings, a finiteness result	86
24.1.6	Theorem – Tate?	86
24.2.1	Theorem – ?	88
24.3.4	Theorem – Faltings	89
24.3.5	Proposition – ?	89

## Exercises

3.2.3	Exercise – ?	11
4.2.7	Exercise – ?	15
5.2.7	Exercise – ?	19
6.1.3	Exercise – ?	20
6.2.3	Exercise – ?	21
10.2.10	Exercise – ?	41
11.1.9	Exercise – ?	45
11.2.10	Exercise – ?	47
12.2.10	Exercise – A fun one	50
12.2.14	Exercise – ?	51
15.0.9	Exercise – Homework	60
15.0.12	Exercise – ?	60
16.0.4	Exercise – ?	62
17.0.2	Exercise – important: on what descent means and how to compute with it	64
18.1.9	Exercise – ?	68
18.1.10	Exercise – ?	68
19.1.2	Exercise – ?	71

# Figures

## List of Figures