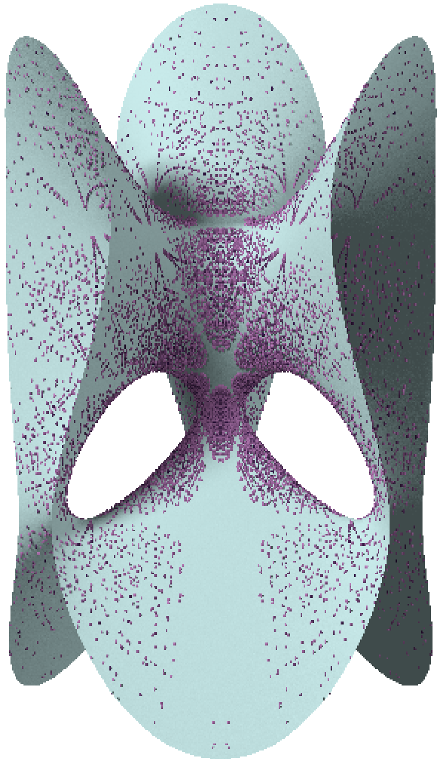


Notes: These are notes live-tex'd from a graduate course on rational points taught by Daniel Litt at the University of Georgia in Fall 2021. As such, any errors or inaccuracies are almost certainly my own.

Rational Points

Lectures by Daniel Litt. University of Georgia, Fall 2021

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

Last updated: 2021-09-13

Table of Contents

Contents

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

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

Some natural questions:

Remark 2.0.3 ***(Topic 1: Are there any common solutions?):*** More generally, does $X := V(f_1, \cdots, f_n)$ have any rational points? How many rational points are there? Finitely many, or infinitely many?

Remark 2.0.4 ***(Topic 2: what is the distribution of points?):***

- How many points are there of height at most N, where $\mathrm{ht}(a/b) = \max(|a|, |b|)$?

- Are they Zariski dense? I.e. are there solutions outside of the ideal $\langle f_i \rangle$?
- Are they *potentially* dense, i.e. dense after some finite extension $k \hookrightarrow k'$?
- Choosing $k \hookrightarrow \mathbb{C}$ or $\mathbb{Q}_p$, are the solutions dense in the analytic topology on $X(\mathbb{C}), X(\mathbb{Q}_p)$? If not, what is the closure?

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

Remark 2.0.5 ***(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 2.0.6 ***(Topic 3': Weak and Strong Approximation):*** As an example,

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

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

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

Remark 2.0.7 ***(Topic 4: effectiveness and decidability questions.):*** Given a variety $X_{/\mathbb{Q}}$, is there an actual algorithm that decides if $X(\mathbb{Q}) = \emptyset$? This is known over $\mathbb{Z}$, but open for $\mathbb{Q}$ and most (not all) number fields. Are there special classes of varieties where the answer of yes? For curves, this is only known contingent on open problems (the abc conjecture, the section conjecture, Birch-Swinnerton-Dyer, etc).

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

Remark 2.0.8: Other possible topics:

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

2.1 Examples of Hasse Principles

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

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

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

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

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

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

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

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

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

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

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

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

Proof (Sketch/idea).

1. Write $X = V(f_1, \cdots, f_n)$ with a nonempty smooth locus $X^{\mathsf{sm}} \subseteq X$ which is a variety (just adjoin inverses of partial derivatives appearing in minors of Jacobian matrices). So

$$X^{\mathsf{sm}}/\mathcal{O}_{K,S} = \mathcal{O}_K\left[\frac{1}{N}\right] \text{ which is smooth over } \mathcal{O}_{K,S}$$

2. Use Lang-Weil to show that $X^{\mathsf{sm}}(\mathcal{O}_{K,S}/\mathfrak{p}) \neq \emptyset$ for almost all $\mathfrak{p}$.
3. Use smoothness and Hensel's lemma to get $X^{\mathsf{sm}}(\widehat{\mathcal{O}_{K,S}^{\mathfrak{p}}})$.

■

3 | Tuesday, August 24

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

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

■

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

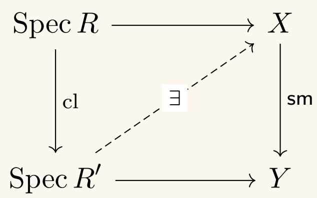
$$\#X(\mathbb{F}_{q^k}) = (1 + O(q^{\frac{1}{2}}))q^{k \dim X}.$$

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

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

Proof (?).
Use

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



Taking $R := R'/I$ with I nilpotent.

Link to Diagram

See Hartshorne chapter 3, in the exercises!

■

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

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

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

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

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

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

■

3.1 Brauer Groups

Remark 3.1.1: Some upcoming topics:

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

3.1.1 The Brauer-Manin Obstruction

Remark 3.1.2: Setup:

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

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

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

which fits into a SES

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

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

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

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

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

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

Link to Diagram

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

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

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

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

3.1.2 The Hasse Principle for Severi-Brauers

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

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

we have

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

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

3.2 Brauer Groups and Galois Cohomology

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

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

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

We can take invariants and coinvariants:

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

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

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

Definition 3.2.4 (Group cohomology)

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

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

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

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

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

4 | Group Cohomology (Thursday, August 26)

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

4.1 Computing Examples

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

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

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

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

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

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

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

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

This yields

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

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

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

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

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

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

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

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

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

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

4.2 Functoriality

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

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

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

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

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

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

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

It's functorial in M, and $\mathrm{tr}_{G/T} \circ \iota^*$ is multiplication by $m := [G:T]$. 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).
- $H^1(G;\mathbb{Z}) = \mathrm{Hom}_{\mathsf{Grp}}(G;\mathbb{Z})$, which is always torsionfree.
- $H^2(G;M)$ classifies extensions of G by M in the following sense: G' occurring in a "SES" $\xi : 0 \to M \to G' \to G \to 1$ such that the action of G on M by conjugation is the given G-module structure on M. Moreover $\xi = 0$ in $H^2(G;M)$ iff ξ splits, then $G' \cong G \rtimes M$. For M a trivial G-module, these are *central extensions.*

Warning 4.2.3

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

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

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

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

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

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

Definition 4.2.5 (Brauer Groups)

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

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

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

Note: we've used that

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

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

5 | Tuesday, August 31

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

$$\cdots \;\substack{\longrightarrow\\\longrightarrow\\\longrightarrow\\\longrightarrow}\; G^{\times 3} \;\substack{\longrightarrow\\\longrightarrow\\\longrightarrow}\; G^{\times 2} \rightrightarrows G$$

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

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

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

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

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

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

and

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

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

■

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

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

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

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

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

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

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

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

The boundary maps are given by

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

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

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

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

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

5.1 Some Formal Properties

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

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

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

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

$$0 \to H^1\left(\frac{G}{H}; M^H\right) \to H^1(G; M) \to H^1(H; M)^{\frac{G}{H}} \to H^2\left(\frac{G}{H}; M^H\right) \to H^2(G; M)$$

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

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

Example 5.2.5 ***(?):*** The groups $\mathrm{SO}(p,q)_{/\mathbb{R}}$, the matrices preserving a quadratic form $\mathrm{diag}(1, \cdots, 1, -1, \cdots, -1)$ with p copies of 1 and q copies of -1, and these are all forms of $\mathrm{SO}(p+q)_{/\mathbb{C}}$.

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

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

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

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

Proof (?).
Recall that

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

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

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

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

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

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

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

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

■

■

6 | Thursday, September 02

6.1 Correspondence of Forms

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

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

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

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

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

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

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

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

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

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

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

where the action is given by f.

■

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

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

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

6.2 Torsors

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

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

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

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

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

6.3 Example: Kummer Theory

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

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

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

Proof (?).
Use the SES

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

which yields a LES

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

and identifying terms yields

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

■

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

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

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

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

6.4 Geometry of Brauer Groups

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

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

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

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

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

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

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

Claim: One needs to show the following:

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

The group operation here is $G' \cdot G'' := G' \underset{G}{\times} G''/A$, 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 $1 \to Z \to H' \to H \to 1$ is a SES of groups with a G-action such that Z is in the center of H'. Then there is a "LES"

$$1 \to Z^G \to (H')^G \to H^G \xrightarrow{\delta_0} H^1(G;Z) \to H^1(G;H') \to H^1(G;H) \xrightarrow{\delta_1} H^2(G;Z)$$

Link to Diagram

Note that some terms here are only sets, so exactness means that differentials surject onto kernels, and $H^1(G;Z) \curvearrowright H^1(G;H')$ and $H^1(G;H)$ is the quotient by this action.
Remark 6.4.4:

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

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

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

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

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 *(?).*

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

7 | Tuesday, September 07

7.1 Intro: Historical POV on Brauer Groups

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

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

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

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

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

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

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

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

Example 7.1.5 *(?):*

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

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

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

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

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

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

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

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

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

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

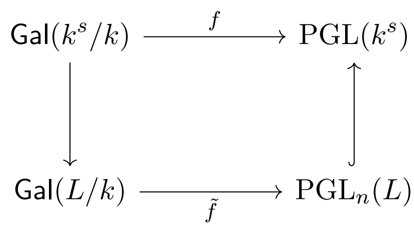
- $[A] = [B] \iff A, B$ are Morita equivalent.
- $[A]^{-1} = [A^{\mathrm{op}}]$.
- $[A] \cdot [B] = [A \otimes_k B]$.

7.2 The Boundary Map and Twisted Vector Space

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

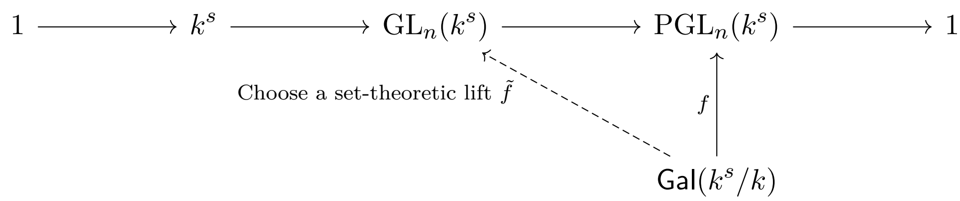
$$H^1(k; \mathrm{PGL}_n(k^s)) \to H^2(k; (k^s)^\times).$$

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



Link to Diagram

To compute this boundary, we use the original SES:



Link to Diagram

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

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

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

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

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

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

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

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

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

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

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

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

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

3. There are natural functors

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

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

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

5. There is an equivalence of categories

$$\mathsf{Tw}_{\mathrm{id}/k} \xrightarrow{\sim} \mathsf{Vect}_{/k}.$$

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

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

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

■

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

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

■

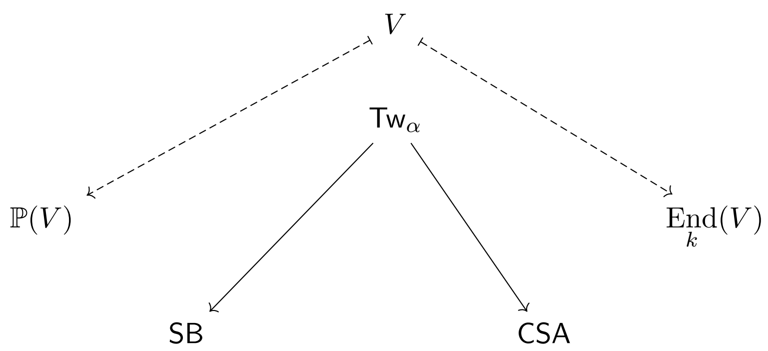
Definition 7.2.8 (Index and period)
Given $H^2(k; (k^s)^\times) = \mathrm{Br}(k)$ (which we'll prove soon), the **period** of α is the order of α, and the **index** is defined the minimal n such that α is in the above image. I.e.,

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

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

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

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



Link to Diagram

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

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

8 | Thursday, September 09

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

- α-twisted vector spaces Tw_α

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

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

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

is n-torsion.

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

Proof (?).
Take a SES

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

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

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

This sequence is exact since we can write $\mathrm{Mor}_{\mathsf{Tw}_\alpha} = (-) \otimes_k {V_1}^\vee$. It's enough to split this SES, since any splitting $s : \mathrm{Mor}_{\mathsf{Tw}_\alpha}(V_1, V_2) \to \mathrm{Hom}(V_1, W)$ would allow taking $s(\mathrm{id}_{V_1})$ to split the original. But this sequence does split, since $\mathrm{Mor}_{\mathsf{Tw}_\alpha}(V_1, V_1)$ is free, thus projective.

■

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

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

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

■

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

:::{.corollary title="?"} 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 8.0.6 *(?).*
For $X_{/k}$ a Severi Brauer, $X \cong \mathbb{P}^n_{/k} \iff X(k) \neq \emptyset$.

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

$$\begin{array}{ccccc} H^1(k; \mathrm{GL}_n) & \longrightarrow & H^1(k; \mathrm{PGL}_n) & \longrightarrow & 0 \in H^2(k; (k^s)^\times) \\ [\alpha] & \longmapsto & [X] & \longmapsto & 0 \end{array}$$

Link to Diagram

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

■

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

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

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

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

■

Definition 8.0.7 (Reduced norm and trace)
Let $A \in \mathsf{CSA}_{/k}$, then there are maps

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

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

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

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

Proposition 8.0.8 *(?).*
For $A \in \mathsf{CSA}_{/k}$, then if there exists a nonzero $f \in A$ with $\mathrm{Nm}_{A_{/k}}(f) = 0$, then A is not a division algebra.

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

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

Theorem 8.0.9 *(?).*
There is a surjection

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

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

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

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

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

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

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

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

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

Question 8.0.11
Can this construction be done in SB or Tw_α?

8.1 Computing Brauer Groups

Remark 8.1.1:

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

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 $\operatorname{Br}(k) = 0$.

Remark 8.1.3: Note that Chevalley-Warring (?) exactly says that finite fields are C_1.

Proof (of theorem).

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

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

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

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

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

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

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

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

ToDos

List of Todos

8

Definitions

Theorems

Exercises

Figures

List of Figures