The Brauer Manin Obstruction to the Local to Global Principle

Luke Askew

Contents

1 The Local to Global Principle

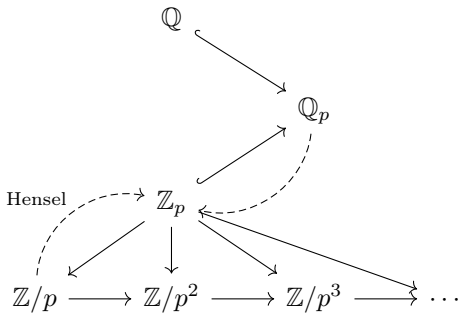
There are algorithms for solving diophantine equations for all p-adic numbers, and for certain varieties this suffices to show the existence of rational points. We begin by explaining why rational solution imply adelic solutions, sketch why we can calculate adelic solutions, and provide varieties where this is not strong enough to provide a rational solution.

1.1 Adele Rings

Note that for any ring R, we can realize diophantine equations in R using the universal map $\mathbb{Z} \to R$ to induce $\mathbb{Z}[\underline{x}] \to R[\underline{x}]$. When a ring homomorhism agrees

with the universal morphism, it is readily observed that the induced polynomial maps agree and so $0 \mapsto 0$ under any ring homomorphism provides a puhing forward of solutions to diophantine equations along these morphisms.

For p prime, then consider the following diagram where solid arrows denote ring homomorphisms and dotted arrows denote lifting of integral polynomial solutions.



The dotted arrow lifting solutions in $\mathbb{Z}/p = \mathbb{F}_p$ to $\mathbb{Z}_p$ uses Hensel's lemma while the arrow lifting soltions from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ is more dubious; it works when restricting to projective varieties where we view $\mathbb{Q}_p$ as the fraction field of $\mathbb{Z}_p$ to clear multiples of the denominators.

Note that there is a counterexample showing homogenious polynomials really are required; namely, $px - 1$ which has a solution in $\mathbb{Q}_p$ but not in $\mathbb{Z}_p$.
We can therefore observe not only that the existence of a rational solution induces a $\mathbb{Q}_p$ solution to a diophantine equation, but that there is a $\mathbb{Q}_p$ solution if and only if there is a solution in $\mathbb{F}_p$.

Because this works for all primes p, we wish to create the smallest ring packaging together all of this information. Also note that rational solutions give real solutions, so it makes sense to consider the colomit of all completions of $\mathbb{Q}$.

Definition 1. The **Adele Ring** $\mathbb{A}_k$ of a global field k is the colimit over all completions of k.

For example, the Adele Ring $\mathbb{A}_\mathbb{Q}$ of $\mathbb{Q}$ is the ring $\mathbb{R} \bigoplus_{p \text{ prime}} \mathbb{Q}_p$. The colimit construction gives a universal diagonal map $\Delta : \mathbb{Q} \to \mathbb{A}_\mathbb{Q}$. Note that the coproduct is the correct construction in the category of rings because we require all but finitely many entries in a tuple to be zero, which corresponds well to the fact that all but finitely many valuations of an element of a global field are 0. This meshes with our intuition $\mathbb{Q}$, for which we can factor a reduced element to get a finite number of primes in the numerator and denominator. For general number fields, we can define valuations for any prime ideal in a similar way.

1.2 Computing if $X(\mathbb{A}_{\mathbb{Q}}) = \emptyset$

In particular, we can compute the solutions to a diophantine equation in $\mathbb{A}_{\mathbb{Q}}$. First, recall that we can bound the solutions to a diophantine equation in $\mathbb{R}$ using generalizations of Cauchy's bound and use Lipchitz continuity to create a maximal partition of this region so that the intermediate value theorem can pick up all possible zeros. We note that these ideas are enough to give an algorithm for factoring a polynomial in $\mathbb{Q}[T]$ into irreducibles as given in [8, 18].Since for each $\mathbb{Q}_p$, we can calculate all solutions, it suffices to bound the number of p that we need to check.

Theorem 1 (Lang Weil Bound, 1954)**.** *Suppose X is a variety in $\mathbb{P}^n$ of dimension r, degree d. Then there exists a constant $A(n, d, r)$ depending on n, d, r such that*

$$|\#V(\mathbb{F}_p) - p^r| \leq (d-1)(d-2)p^{r-1/2} + A(n,d,r)p^{r-1}.$$

[7]
Making this explicit, note that for all constants c there is always some N_c for which $r > N$ gives $p^r > cp^{r-1/2}$, so we will need $\#V(\mathbb{F}_p) \neq 0$. In particular, this tells us that there are solutions mod p to all but finitely many p with a computable upper bound, and the bound is found in the proof of the statement.

1.3 The Local to Global Principle for Varieties

From the above discussion, we have that for any variety X, $X(\mathbb{Q}) \subseteq X(\mathbb{A}_{\mathbb{Q}})$. If X is such that $X(\mathbb{A}_{\mathbb{Q}})$ is inhabited implies $X(\mathbb{Q})$ is inhabited, then we say that X satisfies the **local to global principle**. Quadratic forms satisfy the local to global principle, but in degree 3 we get a counterexample due to Selmer for the projective variety defined by $3x^3 + 4y^3 + 5z^3$[10].

Instead of following this example, let's construct our own by using $\mathbb{F}_p^\times$ cyclic gives $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$, so $3, -3$, or -1 is square mod $p \geq 5$, so we could consider the image of $p(x) = (x^2-3)(x^2+1)(x^2+3)$ in $\mathbb{Z}_p$, and we can observe 1 and 0 are solutions mod 2 and 3. Note that many of our earlier theorems ask for a projective variety and that these solutions still work for the projectization to $\mathbb{Z}[x, y]$ by setting $y = 1$.

2 Brauer Groups of Fields

We begin by collecting some results from [6, XVII]

2.1 Central Simple Algebras

Let k be a field.

Definition 2. A **central simple k-algebra** is a simple k k-algebra, so has no nontrivial two sided ideals, which is simple, so has center k.

Lemma 1. *A is a simple k-algebra if and only if $A \cong M_n(D)$ for some division ring D which is a finite dimensional extension of k with center k and $n \geq 1$. Furthermore n and D are uniquely determined by A.*

Definition 3. We say two central simple k-algebras A and B are **Brauer equivalent** provided $A \cong M_n(D)$ and $B \cong M_m(D)$ for some n, m.

These definitions allow us to make a group using the division rings over k using the tensor product. Provided a k algebra A, one shows $A \otimes_k M_n(F) \cong M_n(A)$ hence for A and B central simple k-algebras we have

$$A \otimes_k B \cong M_n(D) \otimes M_m(D') \cong D \otimes D' \otimes M_{nm}(k) \cong C$$

for some central simple k-algebra C and division rings D and D'. We see that properties of the tensor product give a group law:

Definition 4. The **Brauer group** of a field k is given by the set of equivalence classed of central simple k-algebras with the operation of taking tensor products.

Note that we get inverses by taking the opposite algebra of a skewfield, i.e. the algebra where $a * b = ba$ and that we could define the group under the set of finite division algebras with center k.

We give the example of computing the Brauer group of finite fields and the real numbers. Since any finite ring extension of $\mathbb{F}_p$ is finite, classifying finite division rings is easy as there's only one, $\mathbb{F}_p$ so the Brauer group is trivial.

For $\mathbb{R}$ we sketch a proof for the well known result of Frobenius, suppose D is a division algebra with center $\mathbb{R}$ and $D \neq \mathbb{R}$. Then there exists some $\alpha \in D - \mathbb{R}$, and we get $\mathbb{R}(\alpha) \cong \mathbb{C}$ since α will commute with itself and $\mathbb{R}$ and we have $i = \sqrt{-1} \in D$. As the center of $\mathbb{C}$ is itself, we have an element $\beta \in D$ such that $i\beta \neq \beta i$, in particular $\mathbb{C} \oplus \beta\mathbb{C} \subseteq D$. Considering the conjugation by i map on D gives that the fixed component will be only $\mathbb{C}$ and we can observe the eigenvalues will only be ± 1 since it is an involution. Hence multiplication by β sends anything not in $\mathbb{C}$ to $\mathbb{C}$ and vice versa, and twice multiplication is also an automorphism which must preserve $\mathbb{C}$ and everything outside, which gives that both are 2 dimensional over $\mathbb{R}$. Running through the list of finite groups of order 8 this immediately provides $D \cong \mathbb{R}[Q_q]$ where Q_8 is the quaternion group, hence $D \cong \mathbb{H}$, the standard quaternions. As $|Br(\mathbb{R})| = 2$, we have $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

2.2 Group Cohomology

The main reference for this subsection is [2].

Definition 5. In an abelian category, the right derived functors of $\hom(A,-)$ provide the Ext groups:

$$Ext^i(A,B) = R^i \hom_(A,-)(B)$$

in other words, $Ext^i(A,B)$ is the ith cohomology group of an injective resolution

$$0 \to B \to I_0 \to I_1 \to ...$$

under $\hom(A,-)$.

Definition 6. The **nth cohomology group** of a group G with coefficients in M is

$$H^n(G,M) \cong Ext^n_{\mathbb{Z}[G]}(\mathbb{Z},M).$$

More concretely, we have a functor $\hom_(\mathbb{Z},-) : \mathbb{Z}[G]-mod \to Ab$ and we're taking the homology of an injective resolution of M in this category and considering the cohomology of it image under the functor. Note that this agrees with the usual definition of and group cohomology from projective resolutions thanks to some categorical nonsense. The projective resolutions then agrees with the concrete cocycle and coboundary interpretation, but we take this view to highlight the connection with Étale cohomology later.

Theorem 2 (Hilbert's Theorem 90)**.** *Let F/k be a Galois extenion of fields with cyclic Galois group $G = \langle g \rangle$, then*
(i) $H^1(G, F^\times) = 0$
(ii) For any $a \in F$ with norm 1, there is $b \in F$ such that $a = b/g(b)$.

The proof that (i) implies (ii) works by considering the cocycles and coboundaries directly.[7, 302]

A fun example is deriving the rational perametrization of the unit circle. Note that the unit circle is all elements in $\mathbb{Q}(i)$ with norm 1 and the Galois group is generated by complex conjugation, so we have $|x+iy| = 1$ if and only if

$$x + iy = \frac{z}{\bar{z}} = \frac{u+iv}{u-iv} = \frac{u^2-v^2}{u^2+v^2} + i\frac{2iv}{u^2+v^2}$$

for some rational $u, v \in \mathbb{Q}$. [3]

Definition 7. The **cohomological Brauer group** $Br(k) = H^2(Gal(\overline{k}/k), \overline{k}^\times)$ which is often written $H^2(k, \overline{k}^\times)$.

Theorem 3. *The cohomological Brauer group equals the Brauer group defined with central simple algebras.*

Theorem 4. *The Brauer group of a local field is isomorphic to $\mathbb{Q}/\mathbb{Z}$.*

3 Étale Cohomology

The purpose of étale cohomology is to calculate cohomology on a finer topology for a scheme than is provided by the Zariski topology and to generalize the idea of a locally biholomorphic map between complex analytic spaces to schemes over other rings.

For example, we have that for a smooth complex curve X of genus g, from algebraic topology we know that the singlular cohomology group $H^1(X(\mathbb{C}), \mathbb{Z}) \cong \mathbb{Z}^{2g}$ and by the universal coefficient theorem, $H^1(X(\mathbb{C}), \mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$, and these will agree with the étale cohomology group $H^1_{et}(X, \mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$, though it does still disagree for integral cohomology.[9, 170]

The reference for this section is $[9, ch6]$

3.1 Grothendieck Topologies

Grothendieck topologies aren't topologies, but they do generalize the notion of a topology on a space to a sort of open cover for a category. For example, let $Open(X)$ be the category of open sets on a topological space X where the morphisms are inclusion arrows. A Grothendieck topology on $Open(X)$ can be given by the families of morphisms together covering any open set U of X.

Definition 8. A **Grothendieck topology** for a category $\mathcal{C}$ is a subclass $\mathcal{T}$ of morphisms $\{U_i \to U\}$ for with common target U for all objects U called open coverings satisfying:

(i) Isomorphisms are open coverings: $A \cong B$ gives that $A \to B \in \mathcal{T}$ and $B \to A \in \mathcal{T}$.

(ii) Open coverings of open coverings are open coverings: If $V_{ij} \to U_i$ cover all U_i covering U in $U_i \to U \in \mathcal{T}$, we have that the compositions $V_{ij} \to U \in \mathcal{T}$

(iii) A base extension of an open covering is an open covering: if $\{U_i \to U\} \in \mathcal{T}$ and $V \to U$ is a morphism then we have pullbacks (fiber products) $V \times_U U_i$ with $\{V \times_U U_i \to V\} \in \mathcal{T}$

$$\begin{array}{ccc} V \times_U U_i & \dashrightarrow & U_i \\ \vdots & & \downarrow \\ V & \longrightarrow & U \end{array}$$

We interpret the first axiom as giving licence to think of the Grothendieck topology of the categorical skeleton of $\mathcal{C}$. The second generalizes the idea from topology that we can refine our open covers, as covering all open sets again will compose to a full cover. The third generalizes our notions of continuous maps.

The inverse of an open set is an open set generalizes to the pullback of an open cover along a morphism in $\mathcal{C}$ is an open cover.

Definition 9. A pair $(\mathcal{C}, \mathcal{T})$ where $\mathcal{T}$ is a Grothendieck topology on $\mathbb{C}$ is called a **site**

For intuition, a Grothendieck topology is to a topology what a site is to a topological space.

Making this explicit, let's pick up the introductiory example on $Open(X)$ to define the **Zariski site** $X_{\text{zar}} = (Open(X), \mathcal{T})$ where $\mathcal{T}$ consists of families $\{U_i \to U\}$ such that $\cup_i U_i = U$.

3.2 The Étale Site

Definition 10. Suppose S is finitely presented over R, i.e. $S \cong \frac{R[X_n]}{(f)}$. A ring morphism $\varphi : R \to S$ is **étale** provided $det(\frac{j}{x_i})_{i,j=1}^n)$ is invertible in S.

This determinant condition is why this is in some way generalizing a locally biholomorphic map between complex analytic spaces.

Take the map $\mathbb{Z} \to \mathbb{Z}[x]/(x^2)$ given by the composition of the inclusion into the polynomial ring and the projection to the quotient. We have that the determinant $2x$ is not invertible in in $\mathbb{Z}[x]/(x^2)$, so the morphism is not étale . This would work similarly for all commutative rings R since one observes the image of $\pi(2)x$ under $\pi : \mathbb{Z} \to R$ will always be nilpotent.

Generalizing, considering $\mathbb{Z} \to \mathbb{Z}[x]/(x^k)$ for $k > 2$ gives the same behavior corresponding to the critical point at $x = 0$.

However, is we take $\mathbb{Z} \to \mathbb{Z}[x]/(ax)$ for $a \in \mathbb{Z}^\times$, we get determinant a, so this morphism is étale for $a = \pm 1$. Replacing $\mathbb{Z}$ with a field k gives an étale morphism for $achar(k)$. In the univariate case, we're just looking for $(f, f') = 1$.

Definition 11. A morphism of schemes is textbfétale if its restriction to affine open sets can be found from *tale* ring morphisms.

That this will help us form a étale topology is very reminiscent of how the Zariski topology starts with ring maps that we want to have be continuous, so we define varieties to be our closed sets.

Lemma 2. *The following are equivelant for a morphism of schemes:*

(i) it is étale
(ii) it is smooth of relative dimension 0
(iii) it is flat and unramified

Definition 12. The **big étale site** of a scheme X is $X_{et} = (Schemes_X, \mathcal{T})$ where $\mathcal{T}$ has families of *tale* morphisms $\{\phi_i : U_i \to U\}$ such that $\cup_i \phi_i(U_i) = U$.

For an affine example, take $X \cong spec(\mathbb{Z})$ and consider the affine schemes over X which are in bijection with commutative rings because $(\mathbb{Z})$ is final in the category of affine schemes. Consider $spec(\mathbb{Z}/n\mathbb{Z})$, where all primes are given by prime p divisors of n. Since open sets are primes missing an ideal, we seek a collection of étale ring maps $\phi_i \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}[\underline{x}]$ having inverses covering all of $\mathbb{Z}/n\mathbb{Z}$. Note that the étale condition for affine schemes is just a restriction on the target of our morphisms, so a first example would be $\{\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\}$ where the determinant condition is vacuously satisfied, but we could also take $\{\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}[\underline{x}]/(\underline{f})\}$ so long as the f_i don't degenerate; take $\underline{f} = \{f = ax\}$ with $(a, n) = 1$ for example.

Definition 13. Let F be a presheaf on $\mathcal{C}$ where $(\mathcal{C}, \mathcal{T})$ is a site. Then F is a sheaf provided

$$F(U) \to \prod_i F(U_i) \rightrightarrows \prod_{i,j} F(U_i \times_U U_j)$$

is exact for all open coverings $\{U_k \to U\}$.

this should remind us of the concrete sheaf gluing and locality axioms. Defining the category of abelian sheaves to be sheaves valued in Ab with natural transformations for morphisms yields a small abelian category, so has enough injectives (see the appendix).

3.3 Brauer Groups of Schemes

[9, 6.4] Fix a scheme X and $\cdot \in \{Zar, et\}$ so that $X_\cdot$ is a site.

Definition 14. The functor $H^q_\cdot(X, -) : \{\text{abelian sheaves on } X_\cdot\} \to Ab$ given by $F \to H^q_\cdot(X, F)$ is the qth derived functor of the global sections functor $F \mapsto F(X)$.

Definition 15. For a fixed ring R we get a group scheme $\mathbb{G}_m$ called the **multiplicative group scheme** which is given by $spec(A[t, t^{-1}])$ where the multiplication $m : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ is given by the ring map sending $x \mapsto x \otimes x$.

Lemma 3. *We have that the functor of points* $\hom(-, \mathbb{G}_m)$ *produces a sheaf on* $Schemes_R$.

Notation is often abused in the context of cohomology, write $H^q_{\cdot}(X, \mathbb{G}_m)$ for $H^q_{\cdot}(X, \hom(-, \mathbb{G}_m))$.

The cohomology of $\mathbb{G}_m$ is particularly interesting. The zeroth cohomology group gives the units in the seperable closure of R if R is a field, the first gives Pic and the second gives the Brauer group.

Definition 16. The **Brauer group** of a scheme X is $H^2_{et}(X, \mathbb{G}_m)$

Theorem 5. *The category* $Gal(\overline{k}/k) - mod$ *is equivelant to the category of abelian sheaves on* $(Spec(k))_{et}$.

This is proved by producing a functorial Galois correspondence with inverse.

Corollary 1. The Brauer group definitions for a field and for the spectrum of a field agree.

It can be surprisingly difficult to actually calculate a Brauer group for a scheme over a arithmetically complex field like $\mathbb{Q}$. In 2021, Ure [13] developed an algorithm for finding the torsion subgroups of of $Br(E)$ when E is an elliptic curve over k of characteristic not 2 or 3 by considering central simple algebras over $k(E)$.

The story for real curves is better. For real affine curves C, Demeyer and Knus [1] proved that the Brauer group of C is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^s$ where s denotes the number of connected components (in the Euclidean topology) of X. Hence $E_1 : x^3 - x = y^2$ defined over $\mathbb{R}$ will have Brauer group $(\mathbb{Z}/2\mathbb{Z})^2$ while $E_2 : x^3 + x = y^2$ has Brauer group $(\mathbb{Z}/2\mathbb{Z})$.

Tsen's theorem can be used to get a handle on Brauer groups of curves too. The theorem states that a function field K of an algebraic curve over an algebraically closed field has vanishing Galois homology groups $H^i(K, K^\times)$ for $i \geq 1$. Interpreted under the equivelance with étale cohomology, this gives that the Brauer group vanishes for such curves. Take for example E_i defined over $\mathbb{C}$ or $\overline{Q}$
[9, 204]
All this keeps with the trend of Brauer groups being more unwieldy for fields that are more arithmetically interesting. There are even results for how unwieldy this process gets for central simple algebras. If A is a central simple algebra over k, A field L of finite degree over k splits A if and only if there exists an algebra B similar to A containing L such that $[B : k] = [L : k]^2$. We will see in the next section that the Brauer group can give restrictions on which Adelic points on a variety are rational, and there is even a way where

the groups can explain when varieties have rational but no integral points. In [5], Kresch and Tschinkel give two examples where such an obstruction exists, namely $y^2z - (4x - z)(16x^2 + 20xz + 7z^2) = 1$ and $-2x^4 - y^4 + 18z^4 = 1$.

4 Functorial Obstructions

The reference for this section is [9, Ch8].

4.1 Setup

Let F be a presheaf valued in Set (or another category with a forgetful composition to Set) on the category of schemes over k, $Schemes_k$, and X a k-variety. Each $A \in F(X)$ gives a commutative diagram

$$\begin{array}{ccc} X(k) & \hookrightarrow & X(\mathbb{A}_k) \\ \downarrow{\scriptstyle ev_A} & & \downarrow{\scriptstyle ev_A} \\ F(k) & \longrightarrow & F(\mathbb{A}) \end{array}$$

where the horizontal maps are found from the inclusion $k \to \mathbb{A}_k$.

Call $X(Spec(L))$ $X(L)$. The vertical maps are defined for any k algebra L as a map $ev_A : X(L) \to F(L)$. Since $X(R) = \hom(spec(L), X)$, we get $x \in X(L)$ to provide $F(X) \xrightarrow{F(x)} F(L)$ under F. This map sends A to $ev_A(x) \in F(x)F(L)$. Replace L with k and $\mathbb{A}_k$ to get the above diagram by functoriality.

This diagram helps us restrict the possible k rational points in $X(\mathbb{A}_k)$. If a point p is k-rational, it will lie in the image of $F(k) \to F(\mathbb{A})$, so each A restricts possible k rational points in $X(\mathbb{A}_k)$ to those mapping into this image.

Let $X(\mathbb{A})^A \subseteq X(\mathbb{A})$ be elements mapping into the image of $F(k) \to F(\mathbb{A})$. We define

$$X(\mathbb{A})^F = \bigcap_{A \in F(X)} X(\mathbb{A})^A$$

which is such that

$$X(k) \subseteq X(\mathbb{A})^F \subseteq X(\mathbb{A}).$$

Definition 17. A F obstruction to the local to global principle is when $X(\mathbb{A}) \neq \emptyset$ while $X(\mathbb{A})^F = \emptyset$.

In other words, the local to global principle fails because of considering the image of $F(k)$ in $F(\mathbb{A})$.

For example, we can take F the functor of points for $\mathbb{Q}$, so $F = \hom(-, Spec(\mathbb{Q}))$, and X the affine line over $\mathbb{Q}$ given by $Spec(\mathbb{Q}[x])$.

First, we calculate

$$F(X) \cong \hom(Spec(\mathbb{Q}[x]), Spec(\mathbb{Q}) \cong \hom_{Cring}(\mathbb{Q}, \mathbb{Q}[x]) \cong 0$$

so the evaluation maps are zero. Computing the rest of the square, we calculate:

$$X(\mathbb{Q}) = \hom(Spec(\mathbb{Q}), Spec(\mathbb{Q}[x])) \cong \hom_{cring}(\mathbb{Q}[x], \mathbb{Q}) \cong \mathbb{Q}$$

and

$$X(\mathbb{A}_{\mathbb{Q}}) = \hom(Spec(\mathbb{A}_{\mathbb{Q}}), Spec(\mathbb{Q}[x])) \cong \hom_{cring}(\mathbb{Q}[x], \mathbb{A}_{\mathbb{Q}}) \cong \mathbb{A}_{\mathbb{Q}}$$

and $F(\mathbb{A}_{\mathbb{Q}})$ is similar. We therefore get

$$\begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{A}_{\mathbb{Q}} \\ \downarrow & & \downarrow \\ 0 & \longrightarrow & 0 \end{array}$$

and so we can calculate $X(\mathbb{A}_{\mathbb{Q}})^F = \mathbb{A}_{\mathbb{Q}}$, so this functor did not restrict our set.

To find useful functors for the functorial obstructions to the local to global principle, we should find functors which give an easily computable $F(\mathbb{A}_k)$ and which cut down the possibilities coming from $X(\mathbb{A}_k)$.

4.2 The Brauer Manin Obstruction

We explore the obstruction coming about because of the Brauer group functor to define the **Brauer set** $X(\mathbb{A})^{Br}$. To do this,we collect some lemmas.

Lemma 4. *The Brauer group of a ring of Adeles for a global field k satisfies $Br(\mathbb{A}_k) \cong \bigoplus_v Br(k_v)$ where the v range all valuations and k_v is the completion of k with respect to v.*

Lemma 5. *There is a short exact sequence*

$$0 \longrightarrow Br(k) \longrightarrow \bigoplus_v Br(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

This allows us to fit together the following commutative diagram:

$$\begin{array}{ccccccccc} & & X(k) & \hookrightarrow & X(\mathbb{A}_k) & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & Br(k) & \hookrightarrow & \bigoplus_v Br(k_v) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where the last map $\bigoplus_v Br(k_v) \to \mathbb{Q}/\mathbb{Z}$ is just a sum over the elements in the Brauer groups.

This provides us that $X(\mathbb{A})^{Br} = \{(x_v) \in \mathbb{A}_k | \sum_v \alpha|_v = 0 \text{ for all } \alpha \in Br(X)\}$.

The following establishes that the Brauer Manin obstruction is quite strong:

Theorem 6. *If C is a smooth proper elliptic curve over a global field k with Jacobian J, then under the assumption that the Tate-Shafarevich group $Ш(J)$ is finite, then $C(k) = \emptyset$ and $C(\mathbb{A}_k)$ is inhabited then $C(\mathbb{A}_k)^{Br} = \emptyset$.*

[11, 114]

According to this theorem, the Brauer Manin obstruction suffices to show $C : 3x^3 + 4y^3 + 5z^3$ will have a trivial Brauer set.

A Right Derived Functors

The references for this section are [12] and [14].
Suppose $\mathcal{C}$ and $\mathcal{D}$ are abelian categories and $F : \mathcal{C} \to \mathcal{D}$ is a left exact functor, i.e. a functor such that for any short exact sequence in $\mathcal{C}$ we get an exact sequence in $\mathcal{D}$ in the image of F of the following form:

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

$$0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C)$$

then the idea of a right derived functor is to continue this into a long exact sequence in $\mathcal{D}$, extending the sequence to the right.

Definition 18. An injective object I in a category $\mathbb{C}$ has that for any morphism $f : A \to I$ and any monomorphism $i : A \hookrightarrow B$ there is an extension such that $f = g \circ i$.

$$\begin{array}{ccc} B & & \\ {\scriptstyle i}\uparrow & \searrow^{g} & \\ A & \xrightarrow{f} & I \end{array}$$

Lemma 6. *If $\mathcal{C}$ is abelian, and I is an injective element then we have the following:*

$i : I \hookrightarrow A$ a monomorphism gives $A \cong coker(i) \oplus I$

$A \cong \oplus_i A_i$ gives all A_i injective if and only if A is injective.

Proof. To see the first, take the identity monomorphism to construct the following plit exact sequence:

$$0 \longrightarrow I \underset{g}{\overset{i}{\rightleftarrows}} A \xrightarrow{\pi} coker(i) \longrightarrow 0$$

and for the second observe that it follows directly from the universal property of the coproduct.

□

Lemma 7. *The injective abelian groups are divisible. That is, for every $n \in \mathbb{Z}$ and $g \in G$ there is $y \in G$ such that $ny = g$.*

Proof. We have morphisms $g : \mathbb{Z} \to G$ where $n \mapsto ng$ for all $g \in G$, so supposing G is not divisible gives some n for which $\mathbb{Z} \to [1/n]\mathbb{Z}$ does not extend to a commuting triangle, so G is not injective.

The other direction needs choice and will be omitted.

□

Definition 19. An abelian category $\mathcal{C}$ has **enough injectives** provided any object A of $\mathcal{C}$ there exists an injective object I and a monomorphism $A \hookrightarrow I$.

Theorem 7. *The category $R - mod$ has enough injectives, so by the Freyd-Mitchell embedding theorem, all small abelian categories have enough injectives. We can find one such example for any A by taking $I = \prod_{x \neq 1 \in A} \mathbb{Q}/\mathbb{Z}$.[4]*

If we have enough injectives, we can form a chain long exact sequence of the form:

$$0 \longhookrightarrow A \longhookrightarrow I_0 \longhookrightarrow I_1 \longhookrightarrow \cdots$$

where the I^i are injective. This is called an **injective resolution** of A.

Definition 20. The i**th right derived functor** of F is the functor assigning the ith homology group of the following chain complex:

$$0 \longhookrightarrow 0 \longhookrightarrow F(I_0) \longhookrightarrow F(I_1) \longhookrightarrow \cdots$$

i.e. the kernel of the map out of $F(I_i)$ modulo the image of $F(I_{i-1})$.

Note that a map $A \to B$ gives a map of their injective resolutions which gives a map on these homology groups, so the derived functor is functorial.

Theorem 8. *These homology groups are independant of the choice of injective resolution. Equivelently, the image of any two injective resolutions under a left exact functor are homotopy equivelant.*

References

[1] F. R. Demeyer and M. A. Knus, *The brauer group of a real curve*, Proceedings of the American Mathematical Society **57** (1976), no. 2, 227–232.

[2] Pierre Guillot, *A gentle course in local class field theory*, Cambridge University Press, Cambridge, England, November 2018.

[3] Georges Elencwajg (https://mathoverflow.net/users/450/georges elencwajg), *Intuition for group cohomology*, MathOverflow, URL:https://mathoverflow.net/q/10903 (version: 2010-01-06).

[4] josephz (https://math.stackexchange.com/users/381305/josephz), *Let r be a noetherian ring, then the category of r-modules has enough injectives*, Mathematics Stack Exchange, URL:https://math.stackexchange.com/q/2810268 (version: 2018-06-06).

[5] Andrew Kresch and Yuri Tschinkel, *Two examples of brauer-manin obstruction to integral points*, Bulletin of the London Mathematical Society **40** (2008), no. 6, 995–1001.

[6] Serge Lang, *Algebra*, 3 ed., Graduate Texts in Mathematics, Springer, New York, NY, August 2002 (en).

[7] Serge Lang and Andre Weil, *Number of points of varieties in finite fields*, American Journal of Mathematics **76** (1954), no. 4, 819.

[8] J.S. Milne, *Fields and galois theory*, 2021.

[9] Bjorn Poonen, *Rational points on varieties*, Graduate studies in mathematics, American Mathematical Society, Providence, RI, December 2017 (en).

[10] Ernst S. Selmer, *The diophantine equation ax3+by3+cz3=0*, Acta Math **85** (1951), 203.

[11] Alexei Skorobogatov, *Cambridge tracts in mathematics: Torsors and rational points series number 144*, Cambridge University Press, Cambridge, England, May 2001.

[12] R. P. Thomas, *Derived categories for the working mathematician*, (2000).

[13] Charlotte Ure, *Prime torsion in the brauer group of an elliptic curve*, 2019.

[14] Wikipedia, *Derived functor — Wikipedia, the free encyclopedia*, http://en.wikipedia.org/w/index.php?title=Derived%20functoroldid=1078021739, 2022.