Universität Duisburg-Essen

Université Paris-Sud 11

Mémoire de Master 2 en Mathématiques

Obstruction de Manin et familles des variétés

Author:
Yisheng TIAN

Supervisor:
Prof. David HARARI

Academic year 2016/2017

To my parents

Acknowledgements

First of all, I am sincerely grateful to my advisor Prof. David Harari. I thank him for guiding me to this interesting area and giving me the subject of this report. I also thank him for his kindness, great patience with me and numerous valuable comments for my report. In particular, his interesting explanation makes me feel many fancy notions down to earth during this semester. Finally, I also appreciate him for his suggestions about interesting seminars and for his help during my application for a Ph.D. scholarship.

In Université Paris-Sud, I would like to thank Prof. Elisabeth Bouscaren, Prof. François Charles, Prof. Laurent Clozel, Prof. Olivier Fouquet and Prof. Joël Riou for their kind help in both mathematic and linguistic problems in Orsay. I also appreciate Prof. Ulrich Görtz, Prof. Daniel Greb, Prof. Marc Levine, Prof. Vytautas Paškūnas, Dr. Aurélien Rodriguez and Dr. Matthias Wendt who helped me to study mathematics and to adapt abroad life in Universität Duisburg-Essen. A warm thanks goes to Dr. Barinder Banwait, Dr. Federico Binda, Dr. Adeel Khan, and Dr. Tim Kirschner who helped me a lot to deal with exercises and to give talks. Finally I thank Prof. Ke Chen, Prof. Xiaowu Chen and Prof. Mao Sheng in China for who taught me the foundations of algebraic geometry and number theory and I also thank them for their suggestions for graduate school of mathematics.

I would like to thank ALGANT Consortium for giving me the chance to study in Essen, Germany and Orsay, France. A warm thanks goes to all my friends for their help, encourage and accompany. A special thanks goes to Yibing Liu who picked me up in Düsseldorf and helped me a lot in Germany.

Finally, I thank my parents for their endless support and my fiancée Xiaoli Wei for being always with me.

Contents

Conventions

We fix some notation and conventions as follows.

Algebra

We write $L|K$ for a field extension $K \subset L$. When $L|K$ is Galois, we write $\mathrm{Gal}(L|K)$ for its Galois group. For a field K, we will denote by K_s a separable closure of K and by $\overline{K}$ an algebraic closure of K. Let Σ be a set endowed with a $\mathrm{Gal}(\overline{K}|K)$-action. Then we will denote by $(g, \sigma) \mapsto {}^g\sigma$ for the $\mathrm{Gal}(\overline{K}|K)$-action. Let S be a set endowed with a G-action for some group G, then we write $(g, s) \mapsto g.s$ for the G-action.

We will use Gothic letters to denote categories. For example, $\mathfrak{Ab}$ is the category of abelian groups, $\mathfrak{Gr}$ is the category of groups, $\mathfrak{Mod}_G$ is the category of G-modules for a group G and etc.

Let $L|K$ be a finite field extension. Then we simply write $H^q(L|K)$ for $H^q(\mathrm{Gal}(L|K), L^\times)$. When we want to emphasize how the maps between cohomology groups go, we will write explicitly $H^q(\mathrm{Gal}(L|K), L^\times)$.

Algebraic geometry

Let X be a scheme. We write $\mathcal{O}_X$ for the structure sheaf on X and we denote by $\mathcal{O}_{X,x}$ the stalk at x. For each $x \in X$, $\mathcal{O}_{X,x}$ is a local ring with maximal ideal $\mathfrak{m}_x$ and we write $\kappa(x)$ for the residue field. We write $X^{(q)}$ for the set of points on X of codimension q. If X is an integral scheme, then we write $K(X)$ for the function field of X. For an integral scheme X defined over a field k, we also employ $k(X)$ to denote its function field. For instance, let X be an integral $\mathbb{Q}$-scheme, then we write $\mathbb{Q}(X)$ for the function field of X.

Let k be a field and let $\overline{k}$ be an algebraic closure of k. Let X be a scheme over k, then we write $\overline{X} = X \times_k \overline{k}$.

We say X is a k-variety if X is separated and of finite type over k. An integral k-variety is a reduced and irreducible k-variety. We say X satisfies some geometrical property $\mathcal{P}$ if $\overline{X}$ satisfies the property $\mathcal{P}$. For example, we say a k-variety X is geometrically integral (resp. geometrically reduced, etc) if $\overline{X}$ is integral (resp. reduced, etc).

We say a variety X over k is split if it contains a non-empty smooth open set U which is geometrically integral over k, i.e. U is integral and k is algebraically closed in $k(U)$. We say a k-variety X is geometrically split if the $\overline{k}$-variety $\overline{X}$ is split. Note that X is geometrically split iff X contains a non-empty smooth open subset.

Let S be a base scheme and let $f : X \to Y$ be a morphism of S-schemes. We say f is an X-point on Y and we write $Y(X) := \mathrm{Hom}_S(X, Y)$ for all X-points on Y over S. If $X = \operatorname{Spec} A$ for some ring A, then we write $Y(A) := \mathrm{Hom}_S(\operatorname{Spec} A, Y)$ instead of $Y(X)$.

The Brauer group $\mathrm{Br}(X)$ of a scheme X will always mean the cohomological Brauer group $H^2_{\text{ét}}(X, \mathbb{G}_m)$. We write $\mathrm{Br}_{\mathrm{Az}}(X)$ for the classes of similar Azumaya algebras over X. Let X be a variety over k provided with $p : X \to \operatorname{Spec} k$. Then we obtain two natural homomorphisms $p^* : \mathrm{Br}(k) \to \mathrm{Br}(X)$ and $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})^{\mathrm{Gal}(\overline{k}|k)}$. We write

$$\mathrm{Br}_0(X) = \mathrm{Im}(\mathrm{Br}(k) \to \mathrm{Br}(X))$$
$$\mathrm{Br}_1(X) = \mathrm{Ker}\left(\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})^{\mathrm{Gal}(\overline{k}|k)}\right).$$

Finally, we fix notation on cohomology groups. Let X be a scheme, let $\mathcal{G}$ be a sheaf of abelian groups in the Zariski topology and let $\mathcal{F}$ be an étale sheaf of abelian groups. Then we write $H^q_{Zar}(X, \mathcal{G})$ for the usual cohomology groups defined by the derived functors of the global section functor. We write $H^q(X, \mathcal{F})$ for the cohomology groups with values in $\mathcal{F}$ in the étale topology. Let $\mathfrak{U}$ be a covering in the étale topology over X, then we write $\check{H}^q(\mathfrak{U}|X, \mathcal{F})$ for the Čech cohomology groups with values in $\mathcal{F}$ with respect to the covering $\mathfrak{U}$. The Čech cohomology groups $\check{H}^q(X, \mathcal{F})$ is the limit of $\check{H}^q(\mathfrak{U}|X, \mathcal{F})$ where $\mathfrak{U}$ runs through all coverings in the étale topology.

Arithmetic

Let K be a henselian field with respect to a non-archimedean valuation v. Let κ be the residue field of v. Then for each algebraic extension $L|K$, v extends uniquely to a non-archimedean valuation of L. If $L|K$ is a finite extension, then we say $L|K$ is unramified if $\kappa_L|\kappa$ is separable and $[L : K] = [\kappa_L : \kappa]$. An algebraic extension is called unramified if it is a union of finite unramified subextensions. The composite of all unramified extensions inside an algebraic closure $\overline{K}$ of K is simply called the maximal unramified extension of K and we denote it by K_{nr}. The residue field of K_{nr} is the separable closure of κ. If κ is perfect, then the residue field of K_{nr} is an algebraic closure of κ. Moreover, K_{nr} contains all the roots of $x^m - 1$ for m not divisible by the characteristic of κ because the separable polynomial $x^m - 1$ splits over κ_s and hence it also splits over K_{nr} by Hensel's lemma. In practice, κ will sometimes be finite. In this case, $K_{nr}|K$ is generated by these roots of unity because these roots generate $\kappa_s|\kappa$.

If k is a number field, we write Ω_k or simply Ω for the set of places of k. We denote by Ω_∞ the archimedean places of k and Ω_f the finite places of k, so we have $\Omega = \Omega_\infty \bigsqcup \Omega_f$. For $v \in \Omega$, we denote by k_v the completion of k with respect to the place v. For each finite place $v \in \Omega_f$, we write $\mathcal{O}_v$ for the ring of integers of k_v. Let $S \subset \Omega$ be a finite subset, we write $\mathcal{O}_{k,S}$ be the ring of S-integers, i.e.

$$\mathcal{O}_{k,S} := \{x \in k \mid |x|_v \leq 1, \text{ for } v \notin S\}.$$

We will write $\mathbb{A}_k$ for the associated ring of adeles of k. Finally, for a subset $S \subset \Omega$, we put $k_S = \prod_{v \in S} k_v$ and $k^S = \prod_{v \in \Omega - S} k_v$.

If M is a discrete $\mathrm{Gal}(\overline{k}|k)$-module, then we write

$$Ш^q(k, M) := \mathrm{Ker}(H^q(k, M) \to \prod_{v \in \Omega} H^q(k_v, M)).$$

If A is an abelian variety over k, then $Ш(A) = Ш^1(k, A(\overline{k}))$ is its Tate-Shafarevich group.

Part I

Classical Notions

Introduction

A Diophantine equation is a polynomial equation in at least two unknown with coefficients in $\mathbb{Z}$ which we only concern whether it has integral solutions or not. People have spent lots of times on answering some typical questions like the existence of a solution, the cardinality of the set of solutions, whether it is possible to find all solutions in theory and etc. In 1900, Hilbert proposed determining whether a Diophantine equation is soluble in $\mathbb{Z}$ or not, which is known as the Hilbert's tenth problem. Due to M. Davies, H. Putnam, J. Robinson, Ju. Matijasevic and G. Chudnovsky, the answer to Hilbert's tenth problem is negative. More precisely, let $f(t; x_1, \ldots, x_n) = 0$ be a polynomial equation with coefficients in $\mathbb{Z}$. Then for a certain integer t, there is no algorithm that would tell us whether the equation is soluble in $\mathbb{Z}$ or not.

For a homogeneous Diophantine equation, to find a non-trivial solution in $\mathbb{Z}$ is equivalent to find a solution in $\mathbb{Q}$. This suggests us, in general, to ask the existence of rational solutions of $f(t; x_1, \ldots, x_n) = 0$ first. In fact, this does not reduce the difficulty of finding a solution. But thanks to Hensel's lemma, usually it will be much easier to find solutions in $\mathbb{Q}_p$ and $\mathbb{R}$ rather than in $\mathbb{Q}$. More generally, let k be a number field and let V be a k-variety. Hensel's lemma may provide k_v-points on V for each place v, then it is natural to ask whether there is a k-point on V. We are now in a position to state the Hasse principle. We say a family of varieties over k satisfies the Hasse principle, if for each variety V in this family, $V(k_v) \neq \emptyset$ for each v will imply $V(k) \neq \emptyset$. A variety defined by one quadric equation was the first non-trivial example when the Hasse principle holds (Minkowski-Hasse theorem). Now our strategy is to show a family of varieties satisfy the Hasse principle, then to find k-points on each variety in this family reduces to find k_v-points.

In the middle of the twentieth century, mathematicians began to consider when the Hasse principle fails. They discovered concepts such as Selmer group of an elliptic curve, the Tate-Shafarevich group, and the Cassels-Tate form on it, and finally Manin first found a general obstruction to the Hasse principle. We briefly introduce the idea as follows. Let X be a variety over k and let $\mathbb{A}_k$ be the adelic ring over k. The idea is to find a closed subset C such that $X(k) \subset C \subset X(\mathbb{A}_k)$. Then the emptiness of C obstructs the existence of k-points on X. Manin also found a good substitute to the Hasse principle when it fails and it is the statement that the Manin obstruction to the Hasse principle is the only obstruction. A more precise statement for principal homogeneous space under an abelian variety with finite Shafarevich group is theorem 6.2.3 in [47]. This means that if we are given solutions in k_v satisfying certain conditions for each v, then there is also a solution in k. The Manin obstruction is the only one for many types of homogeneous spaces of linear algebraic groups. This is one possible generalization of the Minkowski-Hasse theorem for quadrics.

It was Skorobogatov who first found a counter-example to the Hasse principle which is not described by the Manin obstruction. This leads us to the notion of torsors and descent obstructions. Let X be a k-variety and let G be an algebraic group over k. An X-torsor under G is an fppf X-variety Y endowed with a G-action compatible with $Y \to X$ which is locally in appropriate topology a direct product. Now suppose Y is a principal homogeneous space of an elliptic curve E defined over k, G is a finite subgroup of E and $X = Y/G$. Assume $X(k_v) \neq \emptyset$ for each place v of k, then by descent theory we sometimes know that X contains no k-point. Then descent method can also be used to describe general torsors and we will use the twist operation to define the descent obstruction. We will see later this is some kind of generalization of the Brauer-Manin obstruction.

We also want to know whether the set of rational points on a variety is Zariski dense. In this report, the Zariski density for nice varieties are proved by weak approximation which is a stronger statement than the Hasse principle asking whether $X(k)$ is dense inside $\prod X(k_v)$. We usually study weak approximation and the Hasse principle at the same time, because the proof can often be given at the same stage. The above topics form the first part of this report.

The first chapter collects well-known results such as group cohomology, nice morphisms of schemes, Grothendieck's topology, cohomology of abelian sheaves on topologies, birational map and end up with a collection of useful techniques. The second chapter introduce the Brauer groups of schemes and the Brauer-Manin obstruction to the Hasse principle and weak approximation. The goal of the third chapter is to introduce torsors and their twist and then state the descent obstruction.

Chapter 1

Preliminaries

The aim of this chapter is to introduce some notions and fix some notations which we will frequently use in the sequel.

1.1 Group cohomology

In this section, we establish the theory of group cohomology and introduce some canonical morphisms. We will use group cohomology theory to define Brauer groups of fields and to study torsors.

1.1.1 Derived functors

We briefly recall some basic facts about δ-functors and derived functors. The main reference is the second chapter in [49].

Definition 1.1.1. Let $\mathfrak{A}$ and $\mathfrak{A}'$ be two abelian categories. A (covariant) cohomological δ-functor between $\mathfrak{A}$ and $\mathfrak{A}'$ is a collection $T = (T^q)$ of additive functors $T^q : \mathfrak{A} \to \mathfrak{A}'$ for $q \geq 0$, together with morphisms

$$\delta^q : T^q(C) \to T^{q+1}(A)$$

defined for each short exact sequence $0 \to A \to B \to C \to 0$ in $\mathfrak{A}$ such that the following two conditions hold. Here we make the convention that $T^q = 0$ for $q < 0$.

(1) For each short exact sequence $0 \to A \to B \to C \to 0$ in $\mathfrak{A}$, there is a long exact sequence

$$\cdots \to T^{q-1}(C) \xrightarrow{\delta^{q-1}} T^q(A) \to T^q(B) \to T^q(C) \xrightarrow{\delta^q} T^{q+1}(A) \to \cdots$$

(2) For each morphism of short exact sequences from $0 \to A' \to B' \to C' \to 0$ to $0 \to A \to B \to C \to 0$ in $\mathfrak{A}$, δ^q gives a commutative diagram

$$\begin{tikzcd}
T^q(C') \arrow[r, "\delta^q"] \arrow[d] & T^{q+1}(A') \arrow[d] \\
T^q(C) \arrow[r, "\delta^q"] & T^{q+1}(A)
\end{tikzcd}$$

for each q.

Definition 1.1.2. (1) A morphism $S \to T$ of cohomological δ-functors is a collection of natural transformations $S^q \to T^q$ that commute with δ^q.

(2) A cohomological δ-functor T is **universal** if given any other δ-functor S and a natural transformation $f^0 : T^0 \to S^0$, there exists a unique morphism $T \to S$ of δ-functors extending f^0.

As an example of universal cohomological δ-functor, we introduce the right derived functors of a left exact functor between abelian categories. Let $F : \mathfrak{A} \to \mathfrak{A}'$ be a left exact functor between two abelian categories. Suppose $\mathfrak{A}$ has enough injectives. We construct the right derived functors R^qF of F for $q \geq 0$ as follows. Let A be an object of $\mathfrak{A}$, choose an injective resolution $A \to I^\bullet$ and define

$$R^qF(A) = H^q(F(I^\bullet)).$$

Theorem 1.1.1. *Let $F : \mathfrak{A} \to \mathfrak{A}'$ be a left (resp. right) exact functor between abelian categories. Suppose $\mathfrak{A}$ has enough injectives (resp. projectives). Then the derived functors R^qF (resp. L_qF) form a universal cohomological (resp. homological) δ-functor.*

Proof. See [49], Theorem 2.4.7. □

Finally we give some examples of derived functors and universal δ-functors.

Example 1.1.2. Let R be a ring and let A be an R-module.

(1) The functor

$$\mathrm{Hom}_{\mathfrak{Mod}}(A, -) : \mathfrak{Mod}_R \to \mathfrak{Mod}_R,\ B \mapsto \mathrm{Hom}_{\mathfrak{Mod}_R}(A, B)$$

is left exact. We define

$$\mathrm{Ext}^q_R(A, B) = R^q\,\mathrm{Hom}_{\mathfrak{Mod}_R}(A, -)(B).$$

(2) The functor

$$A \otimes_R - : \mathfrak{Mod}_R \to \mathfrak{Mod}_R,\ B \mapsto A \otimes_R B$$

is right exact. We define

$$\mathrm{Tor}^R_q(A, B) = L_q(A \otimes_R -)(B).$$

Both two functors are universal δ-functors since they are derived functors of some functors.

Example 1.1.3. For a topological space X, we write $\mathfrak{Ab}_X$ for the category of sheaves of abelian groups on X. Let $f : X \to Y$ be a continuous map of topological spaces. Then the direct image functor $f_* : \mathfrak{Ab}_X \to \mathfrak{Ab}_Y$, $\mathcal{F} \mapsto f_*\mathcal{F}$ is left exact. We obtain its right derived functor R^qf_* which is a universal cohomological δ-functor.

1.1.2 Group homology and cohomology

Now we introduce group homology and cohomology. Let G be a finite group. By a G-module we mean a $\mathbb{Z}[G]$-module. We denote by $\mathfrak{Mod}_G$ the category of G-modules. This is an abelian category which has enough injectives and projectives.

Group cohomology

Let G be a finite group (we will generalize the group cohomology theory to profinite groups later and then it is clear why we assume the group G is finite). We consider the functor

$$\mathrm{Hom}_G(\mathbb{Z}, -) : \mathfrak{Mod}_G \to \mathfrak{Ab},\ A \mapsto \mathrm{Hom}_G(\mathbb{Z}, A).$$

Here $\mathfrak{Ab}$ is the category of abelian groups. Since the functor $\mathrm{Hom}_G(\mathbb{Z}, -)$ is left exact and $\mathfrak{Mod}_G$ has enough injectives, we can define

$$H^q(G, A) := R^q(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -))(A),$$

for $q \geq 0$. We call $H^q(G, A)$ the q-th cohomology group of G with coefficients in A. As we have seen, for a short exact sequence $0 \to A \to B \to C \to 0$ of G-modules, we have a long exact sequence

$$\cdots \to H^{q-1}(G, C) \to H^q(G, A) \to H^q(G, B) \to H^q(G, C) \to H^{q+1}(G, A) \to \cdots$$

Remark 1.1.4. Let A be a G-module. We denote by A^G the elements of A fixed by G, i.e. $A^G = \{a \in A \mid g.a = a,\ \forall g \in G\}$. It's easy to see that $A^G = \mathrm{Hom}_G(\mathbb{Z}, A) = H^0(G, A)$.

Group homology

Similarly,

$$\mathbb{Z} \otimes_{\mathbb{Z}[G]} - : \mathfrak{Mod}_G \to \mathfrak{Ab},\ A \mapsto \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$$

is right exact and $\mathfrak{Mod}_G$ has enough projectives, hence we can define

$$H_q(G, A) := L_q(\mathbb{Z} \otimes_{\mathbb{Z}[G]} -)(A)$$

for $q \geq 0$. We call $H_q(G, A)$ the q-th homology group of G with coefficients in A. For a short exact sequence $0 \to A \to B \to C \to 0$ of G-modules, we have a long exact sequence

$$\cdots \to H_{q+1}(G, C) \to H_q(G, A) \to H_q(G, B) \to H_q(G, C) \to H_{q-1}(G, A) \to \cdots$$

Tate cohomology groups

Let G be a finite group and let A be a G-module. Let $N : A \to A$, $a \mapsto \sum_{g \in G} g.a$ be the norm. Let I_G be the kernel of the map $\mathbb{Z}[G] \to \mathbb{Z}$, $\sum_{g \in G} n_g g \mapsto \sum_{g \in G} n_g$. Then we have the Tate cohomology groups defined as follows:

$$\begin{cases} \widehat{H}^q(G, A) = H^q(G, A) & \text{if } q \geq 1 \\ \widehat{H}^0(G, A) = A^G/NA & \text{if } q = 0 \\ \widehat{H}^{-1}(G, A) = \operatorname{Ker} N/I_G A & \text{if } q = -1 \\ \widehat{H}^{-q}(G, A) = H_{q-1}(G, A) & \text{if } q \geq 2. \end{cases}$$

Proposition 1.1.5. *If G is a finite group and $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, then there is a long exact sequence*

$$\cdots \to \widehat{H}^{q-1}(G, C) \to \widehat{H}^q(G, A) \to \widehat{H}^q(G, B) \to \widehat{H}^q(G, C) \to \widehat{H}^{q+1}(G, A) \to \cdots$$

Proof. See [4], page 102, theorem 3. □

Cyclic groups

Let G be a cyclic group of order n with a generator g. We consider two special elements in $\mathbb{Z}[G]$, namely $N = 1 + g + g^2 + \cdots + g^{n-1}$ and $D = g - 1$. By abuse of notation, we write

$$N : \mathbb{Z}[G] \to \mathbb{Z}[G],\ a \mapsto Na, \quad \text{and} \quad D : \mathbb{Z}[G] \to \mathbb{Z}[G],\ a \mapsto Da.$$

Note that $N(g) = N$ holds and hence we obtain $N(\sum n_i g^i) = \sum n_i N(g^i) = \sum n_i \cdot N \in \mathbb{Z} \cdot N$. Let $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ be the map given by $(\sum a_i g^i) \mapsto \sum a_i$. By checking directly we see $\operatorname{Im} D = \operatorname{Ker} \varepsilon$.

Proposition 1.1.6. *The cohomology of a finite cyclic group is **periodic of period two**. Explicitly, we have*

$$\begin{aligned} \widehat{H}^q(G, A) &= \operatorname{Ker}(D)/\operatorname{Im}(N) = A^G/NA && \textit{for } q \equiv 0 \pmod 2, \\ \widehat{H}^q(G, A) &= \operatorname{Ker}(N)/\operatorname{Im}(D) = \operatorname{Ker} N/NA && \textit{for } q \equiv 1 \pmod 2. \end{aligned}$$

Proof. There are exact sequences

$$0 \to \operatorname{Ker} N \to \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z} \cdot N \to 0 \quad \text{and} \quad 0 \to \mathbb{Z} \cdot N \to \mathbb{Z}[G] \xrightarrow{D} \operatorname{Ker} N \to 0.$$

Therefore we obtain a periodic free resolution of $\mathbb{Z}$:

$$\ldots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0.$$

Now we apply the functors $- \otimes_{\mathbb{Z}[G]} A$ and $\operatorname{Hom}_{\mathbb{Z}[G]}(-, A)$ and take homology, then by definition of Tate cohomology groups we conclude the assertion. □

Let $h_q(A)$ denote the order of $\widehat{H}^q(G,A)$ for $q=0,1$ when it is finite. If both are finite, we define **the Herbrand quotient** $h(A) := h_0(A)/h_1(A)$.

Proposition 1.1.7. *Let G be a cyclic group and let $0 \to A \to B \to C \to 0$ be an exact sequence of G-modules. If two of the three Herbrand quotients $h(A)$, $h(B)$, $h(C)$ are defined, then so is the third and we have*

$$h(B) = h(A) \cdot h(C).$$

Proof. See [4], page 109, proposition 10. □

Proposition 1.1.8. *Let G be a cyclic group and let A be a finite G-module, then $h(A) = 1$.*

Proof. See [4], page 109, proposition 11. □

1.1.3 Standard resolution

As usual, group cohomologies can be computed by cocycles. We introduce a free resolution of the trivial G-module $\mathbb{Z}$ explicitly and it will tell us how the cocycles look like. But in fact, we are mainly interested in 1-cocylces in this report. Let L_q be a free $\mathbb{Z}$-module with a basis $(g_0, \ldots, g_q)$ of $q+1$ elements of G, and define the G-action on L_q componentwise

$$g.(g_0, \ldots, g_q) = (gg_0, \ldots, gg_q).$$

Define the differentials $d : L_q \to L_{q-1}$ by

$$d(g_0, \ldots, g_q) = \sum_{i=0}^{q} (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_q)$$

where the hat means that we omit the component g_i. The homomorphism $L_0 \to \mathbb{Z}$ is defined by sending each g_0 to $1 \in \mathbb{Z}$. Then we obtain an exact sequence

$$\cdots \to L_1 \to L_0 \to \mathbb{Z} \to 0.$$

An element of $K^q = \mathrm{Hom}_{\mathbb{Z}[G]}(L_q, A)$ can be identified with a function $f(g_0, \ldots, g_q)$ taking values in A, and satisfying the condition

$$f(g.g_0, \ldots, g.g_q) = g.f(g_0, \ldots, g_q).$$

The coboundary of f is defined by

$$d : K^q \to K^{q+1},\ f \mapsto \big((g_0, \ldots, g_{q+1}) \mapsto \sum_{i=0}^{q+1} (-1)^i f(g_0, \ldots, \hat{g}_i, \ldots, g_{q+1})\big).$$

A cochain f is uniquely determined by its restriction to systems of the form

$$(1, g_1, g_1 g_2, \ldots, g_1 \ldots g_q).$$

This leads us to interpret the elements of K^q as inhomogeneous cochains, i.e.

$$\begin{aligned} df(g_1, \ldots, g_{q+1}) =& g_1.f(g_2, \ldots, g_{q+1}) + (-1)^{q+1} f(g_1, \ldots, g_q) \\ &+ \sum_{i=1}^{q} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{q+1}). \end{aligned}$$

Example 1.1.9. (1) A 1-cocycle is a map $f : G \to A$ such that

$$0 = df(g_1, g_2) = g_1.f(g_2) - f(g_1 g_2) + f(g_1),$$

or in other words, f verifies
$$f(g_1g_2) = g_1.f(g_2) + f(g_1).$$
It is also called a **crossed homomorphism**. It is a coboundary if there exists $a \in A$ such that $f(g) = g.a - a$ for all $g \in G$.

When G acts trivially on A, we have $g.a - a = 0$ for any $g \in G$ and $a \in A$. Let $f : G \to A$ be any 1-cocycle satisfying $g.f(g_0) = f(gg_0)$, then f is a 1-coboundary iff $f(g) = g.a - a$ for some $a \in A$ which means that f is identically zero. This implies that we have the identification $H^1(G, A) = \mathrm{Hom}_G(G, A)$.

(2) A 2-cocycle is a map $f : G \times G \to A$ such that
$$g_1.f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2) = 0.$$

We end up with explicit computation on the proof of Hilbert's theorem 90.

Theorem 1.1.10 (Hilbert's theorem 90)**.** *Let $L|K$ be a finite Galois extension. Then*
$$H^1(\mathrm{Gal}(L|K), L^\times) = 0.$$

Proof. Let $c : \mathrm{Gal}(L|K) \to L^\times$ be a 1-cocycle, i.e. $c(g_1g_2) = c(g_1) \cdot {}^{g_1}c(g_2)$. Recall that distinct automorphisms of a field are linearly independent, we know that the endomorphism of L given by multiplying $\sum_{g\in\mathrm{Gal}(L|K)} c(g) \cdot g$ is not identically zero. Hence we can find $x \in L^\times$ such that $\alpha = \sum c(g) \cdot {}^g x \neq 0$. Now for each $g \in \mathrm{Gal}(L|K)$, we have
$$\begin{aligned} {}^g\alpha &= \sum_h {}^g(c(h) \cdot {}^h x) = \sum_h {}^g(c(h)) \cdot {}^{gh}x \\ &= \sum_h c(g)^{-1} \cdot c(gh) \cdot {}^{gh}x = c(g)^{-1} \sum_h c(gh) \cdot {}^{gh}x = c(g)^{-1} \cdot \alpha, \end{aligned}$$
where each h runs through $\mathrm{Gal}(L|K)$. This shows that $c(g) = {}^g\beta \cdot \beta$ for $\beta = \alpha^{-1} \in L^\times$, i.e. each 1-cocycle is a coboundary. $\square$

1.1.4 Change of groups

Let $f : G' \to G$ be a homomorphism of groups and let A be a G-module. We put $g'.a = f(g').a$ for $g' \in G'$ and $a \in A$. Then A is endowed with a G'-module structure which we denote by f^*A. For $a \in A^G$, we have $g'.a = f(g').a = a$ and hence A^G is a subgroup of $(f^*A)^{G'}$. This defines a natural transformation of the functors
$$H^0(G, -) \to H^0(G', f^*-).$$
Since derived functors form a universal δ-functor, it extends to a natural transformation
$$H^q(G, -) \to H^q(G', f^*-)$$
for all $q \geq 0$. In particular, for each $q \geq 0$ and each G-module A, we have a homomorphism
$$H^q(G, A) \to H^q(G', f^*A).$$
More generally, we consider a G'-module A' and a group homomorphism $\varphi : A \to A'$ as follows. We say that f and φ are compatible if $\varphi(g'.a) = \varphi(f(g').a) = g'.\varphi(a)$ for all $g' \in G'$. This can be visualized as the following commutative diagram
$$\begin{tikzcd} G' \times A \arrow[r, "\rho"] \arrow[d, "\mathrm{id}\times\varphi"'] & A \arrow[d, "\varphi"] \\ G' \times A' \arrow[r, "\rho'"'] & A' \end{tikzcd}$$

where $\rho(g', a) = f(g').a$ and $\rho'(g', a') = g'.a'$. This implies $H^0(G', f^*A) \subset H^0(G', A')$. Thus φ defines a homomorphism

$$H^q(G', f^*A) \to H^q(G', A')$$

for each $q \geq 0$. We obtain $H^q(G, A) \to H^q(G', A')$ by composing the homomorphisms as follows for each $q \geq 0$

$$H^q(G, A) \to H^q(G', f^*A) \to H^q(G', A')$$

and we call the resulting homomorphism the homomorphism associated to the pair (f, φ).

Example 1.1.11. If H is a subgroup of G and $\iota : H \to G$ is the inclusion, then we obtain an inclusion $A^G \hookrightarrow A^H$. By the same argument as above, it extends to homomorphisms

$$\mathrm{res} : H^q(G, A) \to H^q(H, A)$$

which are called the **restriction** homomorphisms.

Example 1.1.12. Let H be a subgroup of G and let A be a G-module. Suppose H has **finite index** in G. If $a \in A^H$ and $g \in G$, then the element $g.a$ depends only on the left coset of g (mod H). As G/H is finite, we can form the sum $N_{G/H}(a) = \sum_{s \in G/H} s.a$. For any $g \in G$, $g.N_{G/H}(a) = \sum_{s \in G/H} gs.a = N_{G/H}(a)$ holds, hence we get a homomorphism

$$N_{G/H} : H^0(H, A) \to H^0(G, A), \; a \mapsto N_{G/H}(a).$$

This is the corestriction in degree 0. Thus we obtain a homomorphism for each q

$$\mathrm{cores} : H^q(H, A) \to H^q(G, A),$$

which is called the **corestriction** homomorphism.

Example 1.1.13. Let H be a normal subgroup of G and let A be a G-module. Let $\pi : G \to G/H$ be the projection and let $\iota : A^H \to A$ be the inclusion. For $g \in G$ and $a \in A^H$, we have $g.\iota(a) = g.a = \pi(g).a = \iota(\pi(g).a)$ and hence π and ι are compatible. Here $g.a$ only depends on the coset of G/H since $a \in A^H$ and this implies $g.a = \pi(g).a$. Therefore we obtain a homomorphism for each q:

$$\inf : H^q(G/H, A^H) \to H^q(G, A)$$

and it is called the **inflation** homomorphism.

Proposition 1.1.14. *Let $q > 0$ be an integer. Suppose $H^i(H, A) = 0$ for $1 \leq i < q$. Then the following sequence is exact:*

$$0 \to H^q(G/H, A^H) \overset{\inf}{\to} H^q(G, A) \overset{\mathrm{res}}{\to} H^q(H, A).$$

Proof. See [43] page 117, proposition 5. □

Corollary 1.1.15. *Let $M|K$ be a Galois extension containing a Galois extension $L|K$. Then there is an exact sequence*

$$0 \to H^2(\mathrm{Gal}(L|K), L^\times) \to H^2(\mathrm{Gal}(M|K), M^\times) \to H^2(\mathrm{Gal}(M|L), M^\times).$$

Proof. Let $G = \mathrm{Gal}(M|K)$ and let $H = \mathrm{Gal}(M|L)$. Since $H^1(\mathrm{Gal}(M|L), M^\times) = 0$ by Hilbert's theorem 90, we can apply the previous proposition with $q = 2$. We get the exact sequence

$$0 \to H^2(\mathrm{Gal}(L|K), L^\times) \to H^2(\mathrm{Gal}(M|K), M^\times) \to H^2(\mathrm{Gal}(M|L), M^\times).$$

as required. □

1.1.5 Profinite groups

Now we introduce the cohomology to profinite groups. Let G be a profinite group and let $\{U_i\}_{i\in I}$ be the family of all open normal subgroups of G. For $i, j \in I$, we assume $i \le j$ iff $U_j \subseteq U_i$, hence $\{U_i\}_{i\in I}$ is a direct system. Then for any $i \le j$, we have canonical projections $G/U_j \to G/U_i$ and $\{G/U_i\}$ becomes an inverse system.

We can prove that $G \simeq \varprojlim_{i\in I} G/U_i$ (see [4], page 118, corollary 1). We say a G-module A is discrete, if $A = \bigcup_{i\in I} A^{U_i}$ where U_i runs through all open normal subgroups of G. In fact, $A \simeq \varinjlim_{i\in I} A^{U_i}$ because all the homomorphisms $A^{U_j} \to A^{U_i}$ are injective.

For each pair $i \le j$, we obtain an inflation homomorphism

$$\lambda_{ij} : H^q(G/U_i, A^{U_i}) \to H^q(G/U_j, A^{U_j})$$

induced by $A^{U_i} \to A^{U_j}$ and $G/U_j \to G/U_i$ as usual. Therefore we obtain a direct system of abelian groups $(H^q(G/U_i, A^{U_i}), \lambda_{ij})$.

Definition 1.1.3. Let G be a profinite group, let $\{U_i\}_{i\in I}$ be the family of all open normal subgroups of G and let A be a discrete G-module. We call

$$H^q(G, A) := \varinjlim_{i\in I} H^q(G/U_i, A^{U_i})$$

the q**-th cohomology group of** G **with coefficients in** A.

Example 1.1.16. Let $L|K$ be a Galois extension and let $\{K_i\}_{i\in I}$ be the family of all finite Galois extensions of K contained in L. We write $U_i = \mathrm{Gal}(L|K_i)$ and then U_i forms a direct system consists of all the open normal subgroups of $\mathrm{Gal}(L|K)$. Then it follows that

$$\mathrm{Gal}(L|K) \simeq \varprojlim \mathrm{Gal}(L|K)/\operatorname{Gal}(L|K_i).$$

The $\mathrm{Gal}(L|K)$-action on L makes the additive group $(L, +)$ into a $\mathrm{Gal}(L|K)$-module. Now $L^{U_i} = K_i$ and $L = \bigcup K_i$ hold, hence L is a discrete $\mathrm{Gal}(L|K)$-module. Moreover, K_i is a $\mathrm{Gal}(K_i|K)$-module and $\mathrm{Gal}(K_i|K) \simeq \mathrm{Gal}(L|K)/U_i$. Thus we conclude

$$H^q(\mathrm{Gal}(L|K), L) \simeq \varinjlim H^q(\mathrm{Gal}(K_i|K), K_i).$$

In fact, $H^q(\mathrm{Gal}(L|K), L) = 0$ for each $q \ge 1$ (see [4], page 124, proposition 2). By this fact, the cohomology theory of the additive group $(L, +)$ is not interesting. The situation is quite different when we look at the multiplicative group $L^\times$ as a $\mathrm{Gal}(L|K)$-module. Since $(L^\times)^{U_i} = K_i^\times$ and $L^\times = \bigcup K_i^\times$, $L^\times$ becomes a discrete $\mathrm{Gal}(L|K)$-module and we have

$$H^q(\mathrm{Gal}(L|K), L^\times) \simeq \varinjlim H^q(\mathrm{Gal}(K_i|K), K_i^\times).$$

We will see the application later.

1.1.6 Cup product

Let A, B be two G-modules and let $A \otimes_{\mathbb{Z}} B$ be their tensor product over $\mathbb{Z}$. We make $A \otimes_{\mathbb{Z}} B$ into a G-module by setting

$$g.(a \otimes b) = g.a \otimes g.b$$

and extending by G-linearity.

Proposition 1.1.17. *Let G be a finite group. Then there exists one and only one family of homomorphisms (called **cup product**) defined for every pair of integers (p, q) and every couple of G-modules A, B:*

$$\widehat{H}^p(G, A) \otimes_{\mathbb{Z}} \widehat{H}^q(G, B) \to \widehat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} B)$$

denoted by $a \otimes b \mapsto a \cup b$, which satisfy the following four properties:

(1) These homomorphisms are morphisms of functors, when the two sides of the arrow are considered to be covariant bifunctors in (A,B).

(2) For $p=q=0$, *the cup product*

$$(A^G/NA)\otimes_{\mathbb{Z}}(B^G/NB)\to(A\otimes_{\mathbb{Z}}B)^G/N(A\otimes_{\mathbb{Z}}B)$$

is obtained by passage to the quotient of the natural map $A^G\otimes_{\mathbb{Z}}B^G\to(A\otimes_{\mathbb{Z}}B)^G$.

(3) Let $0\to A'\to A\to A''\to 0$ *be an exact sequence of* G*-modules. If the sequence*

$$0\to A'\otimes_{\mathbb{Z}}B\to A\otimes_{\mathbb{Z}}B\to A''\otimes_{\mathbb{Z}}B\to 0$$

is also exact, then for all $a''\in\widehat{H}^p(G,A'')$ *and* $b\in\widehat{H}^q(G,B)$:

$$(\delta a'')\cup b=\delta(a''\cup b),$$

where both sides are elements of $\widehat{H}^{p+q+1}(G,A\otimes_{\mathbb{Z}}B)$.

(4) Let $0\to B'\to B\to B''\to 0$ *be an exact sequence of* G*-modules. If the sequence*

$$0\to A\otimes_{\mathbb{Z}}B'\to A\otimes_{\mathbb{Z}}B\to A\otimes_{\mathbb{Z}}B''\to 0$$

is also exact, then for all $a\in\widehat{H}^p(G,A)$ *and* $b''\in\widehat{H}^q(G,B'')$:

$$a\cup(\delta b'')=(-1)^p\delta(a\cup b''),$$

where both sides are elements of $\widehat{H}^{p+q+1}(G,A\otimes_{\mathbb{Z}}B)$.

Proof. For a proof, see [4], page 105, section 7. □

1.2 Morphisms of schemes

We introduce some special morphisms of schemes with nice properties in this section.

1.2.1 Flat morphisms

Definition 1.2.1. Let $f:X\to Y$ be a morphism of schemes.

(1) We say f is flat at $x\in X$, if $\mathcal{O}_{X,x}$ is a flat $\mathcal{O}_{Y,y}$-module via $f_x^*:\mathcal{O}_{Y,y}\to\mathcal{O}_{X,x}$, where $y=f(x)$. We say f is **flat** if f is flat at any $x\in X$.

(2) We say f is **faithfully flat** if f is flat and surjective.

Proposition 1.2.1. *(1) Open immersions are flat.*

(2) Flat morphisms are stable under base change.

(3) Flat morphisms are stable under composition.

Proof. See [34], §4.3.1, proposition 3.3. □

1.2.2 Étale morphisms

Definition 1.2.2. Let $f:X\to Y$ be a morphism of schemes.

(1) We say f is **unramified** if for any $x\in X$, $\mathfrak{m}_y\mathcal{O}_{X,x}=\mathfrak{m}_x$ holds and $\kappa(x)|\kappa(y)$ is a separable field extension where $y=f(x)$.

(2) We say f is **étale** if f is flat and unramified.

Example 1.2.2. Let $L|K$ be a finite field extension. Then $\operatorname{Spec}L\to\operatorname{Spec}K$ is unramified (hence étale) iff $L|K$ is a separable extension.

We can describe unramified morphisms by the following lemma.

Lemma 1.2.3. *Let $f : X \to Y$ be a morphism of finite type between locally noetherian schemes. Then f is unramified iff for each $y \in Y$, the fibre X_y is finite and reduced, and $\kappa(x)|\kappa(y)$ is a separable extension.*

Proof. First note that $\mathcal{O}_{X_y,x} \simeq \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,y}} \kappa(y) \simeq \mathcal{O}_{X,x}/\mathfrak{m}_y\mathcal{O}_{X,x}$. Suppose f is unramified. Then $\mathfrak{m}_x = \mathfrak{m}_y\mathcal{O}_{X,x}$. Hence $\mathcal{O}_{X_y,x} \simeq \kappa(x)$. This shows that X_y is reduced and of dimension 0. X_y is of finite type over $\kappa(y)$ hence it is quasi-compact. It follows X_y is finite. Conversely, X_y is finite implies X_y is the disjoint union of $\operatorname{Spec}\kappa(x)$ for $x \in X_y$. Hence $\kappa(x) \simeq \mathcal{O}_{X_y,x} \simeq \mathcal{O}_{X,x}/\mathfrak{m}_y\mathcal{O}_{X,x}$ and this shows that f is unramified. □

Proposition 1.2.4. *(1) Open immersions are étale.*

(2) Étale morphisms are stable under composition.

(3) Étale morphisms are stable under base change.

Proof. See [34], §4.3.2, proposition 3.22. □

1.2.3 Morphisms of finite presentation

Definition 1.2.3. Let $f : X \to Y$ be a morphism of schemes.

(1) We say f is **quasi-compact** if $f^{-1}V$ is quasi-compact for each affine open subset V of Y. In particular, an affine morphism (hence a closed immersion) is quasi-compact.

(2) We say f is **quasi-separated** if the diagonal morphism $\Delta : X \to X \times_Y X$ is quasi-compact. In particular, a separated morphism is quasi-separated since the diagonal morphism $\Delta : X \to X \times_Y X$ is a closed immersion.

Definition 1.2.4. Let $f : X \to Y$ be a morphism of schemes.

(1) We say f is of finite presentation at $x \in X$, if there exists an open affine neighbourhood $V = \operatorname{Spec} B$ of $f(x)$ in Y and an open affine neighbourhood $U = \operatorname{Spec} A$ of x in $f^{-1}(V)$ such that A is a B-algebra of finite presentation.

(2) We say f is **locally of finite presentation** if f is of finite presentation at any $x \in X$.

(3) We say f is **of finite presentation** if it is quasi-compact, quasi-separated and locally of finite presentation.

Proposition 1.2.5. *(1) Open immersions are locally of finite presentation.*

(2) Morphisms of locally finite presentation (resp. finite presentation) are stable under base change.

(3) Morphisms of locally finite presentation (resp. finite presentation) are stable under composition.

Proof. (1) Let $j : U \to X$ be an open immersion. We may assume U is an open subscheme of X. Then for each $x \in U$, we can find an open affine neighbourhood $V = \operatorname{Spec} A \subset U \subset X$. Of course A is an A-algebra of finite presentation and it follows that (1) holds.

(2) Let $f : X \to Y$ and $Y' \to Y$ be morphisms of schemes. Suppose f is locally of finite presentation. We denote by $X' = Y' \times_Y X$ and take $x' \in X'$. Let x, y and y' be the images of x' in X, Y and Y' respectively. Then by assumption, we can find two open affine neighbourhoods $V = \operatorname{Spec} B$ and $U = \operatorname{Spec} A$ of y and x respectively such that $f(U) \subset V$ and A is a B-algebra of finite presentation. Let $W = \operatorname{Spec} B'$ be an open affine neighbourhood of y' in Y' such that W is contained in the inverse image of V. Now $W \times_V U \simeq \operatorname{Spec}(B' \otimes_B A)$ is an open affine neighbourhood of x' in X' and $B' \otimes_B A$ is a B'-algebra of finite presentation.

(3) Let $f : X \to Y$ and $g : Y \to Z$ be morphisms of schemes that are locally of finite presentation. Take any $x \in X$ and let $y = f(x)$ and $z = g(y)$. We can find open affine neighbourhoods $W = \operatorname{Spec} C$ and $V = \operatorname{Spec} B$ of z and y respectively such that $g(V) \subset W$ and B is a C-algebra of finite presentation. Now f is also locally of finite presentation, we can therefore localize V at suitable $b \in B$ and find $U = \operatorname{Spec} A$ such that $f(U) \subset V_b$ and A is a B_b-algebra of finite presentation. Summing up, we obtain a C-algebra structure on A by $C \to B \to B_b \to A$ and this implies that A is a C-algebra of finite presentation. □

1.2.4 Smooth morphisms

Suppose X is an integral variety over an algebraically closed field for the moment. Then there are two equivalent definitions for X to be non-singular (cf. [28] I.5). Roughly speaking, the first definition asks the Jacobian matrix at each point is of correct rank and the second definition requires each local ring is a regular local ring. Unfortunately, these two definitions are no longer equivalent in general. Moreover, we also need the notion of smoothness over arbitrary base schemes rather than fields. In this section, we study regular (non-singular) schemes and smooth morphisms.

Definition 1.2.5. Let $f : X \to Y$ be a morphism of finite type of noetherian schemes. Take $x \in X$ and let $y = f(x)$.

(1) We say f is smooth of relative dimension d at x if there exist an open neighbourhood U of x and an open affine neighbourhood $V = \operatorname{Spec} R$ of $y \in Y$ such that

$$U \simeq \operatorname{Spec} R[T_1, \dots, T_{n+d}]/(f_1, \dots, f_n)$$

for some $f_1, \dots, f_n \in R[T_1, \dots, T_{n+d}]$ and such that

$$\operatorname{rank}\Big(\frac{\partial f_i}{\partial T_j}(x)\Big) = n,$$

where $1 \leq i \leq n$ and $1 \leq j \leq n + d$.

(2) We say $f : X \to Y$ is **smooth of relative dimension** d if it is so at x for each $x \in X$. In this case, we sometimes say X is smooth over Y or X is a smooth Y-scheme.

Proposition 1.2.6. *(1) Open immersions are smooth.*

(2) Smooth morphisms are stable under base change.

(3) Smooth morphisms are stable under composition.

Proof. (1) Let $j : U \to X$ be an open immersion. We may assume U is an open subscheme of X. Then for each $x \in U$, we can find an open affine neighbourhood $V = \operatorname{Spec} A \subset U \subset X$. This shows that open immersion are smooth of relative dimension 0.

(2) Let $f : X \to Y$ be a smooth morphism and let $Y' \to Y$ be a morphism. Suppose f is smooth of relative dimension d. We write X' for $Y' \times_Y X$. Take $x' \in X'$ and let x, y and y' be the images of x' in X, Y and Y' respectively. Then we can find an open affine neighbourhood $V = \operatorname{Spec} A$ of y in Y such that $x \in U \simeq \operatorname{Spec} A[T_1, \dots, T_{m+d}]/(f_1, \dots, f_m)$ such that $\operatorname{rank}(a_{ij})|_x = m$. Here $a_{ij} = \partial f_i/\partial T_j$ for $1 \leq i \leq m$ and $1 \leq j \leq m + d$. Take $V' = \operatorname{Spec} B$ be an open affine neighbourhood of y' then $U' = V' \times_V U \simeq \operatorname{Spec} B[T_1, \dots, T_{m+d}]/(f_1, \dots, f_m)$. Note that $a_{ij} \in \kappa(x)$ is contained in $\kappa(x')$, hence $\operatorname{rank}(a_{ij})|_{x'} = \operatorname{rank}(a_{ij})|_x = m$. It follows that $f' : X' \to Y'$ is also smooth of relative dimension d.

(3) Let $f : X \to Y$ and $g : Y \to Z$ be smooth morphisms of relative dimension d and e respectively. By definition, we can reduce to the case that X, Y and Z are all affine. We may assume $X = \operatorname{Spec} C$, $Y = \operatorname{Spec} B$ and $Z = \operatorname{Spec} A$ such that

$$B \simeq A[T_1, \dots, T_{m+d}]/(f_1, \dots, f_m) \quad \text{and} \quad C \simeq B[U_1, \dots, U_{n+e}]/(g_1, \dots, g_n)$$

with $\operatorname{rank}(\partial f_i/\partial T_j)|_y = m$ and $\operatorname{rank}(\partial g_i/\partial U_j)|_x = n$. Here $x \in X$ and $y = f(x)$. After renaming the variables and the functions, we obtain

$$\begin{aligned} C \simeq & A[T_1, \dots, T_{m+d}, U_1, \dots, U_{n+e}]/(f_1, \dots, f_m, g_1, \dots, g_n) \\ \simeq & A[T_1, \dots, T_{m+d+n+e}]/(h_1, \dots, h_{m+n}). \end{aligned}$$

Moreover,

$$\operatorname{rank}(\partial h_i/\partial T_j)|_x = \operatorname{rank}\begin{pmatrix} \frac{\partial f_i}{\partial T_j}(x) & 0 \\ 0 & \frac{\partial g_{i-m}}{\partial U_{j-m-d}}(x) \end{pmatrix} = m + n.$$

We conclude $g \circ f$ is smooth of relative dimension $m + n$. $\square$

Definition 1.2.6. Let $f : X \to Y$ be a morphism of finite type of noetherian schemes. The **smooth locus** of f is the subset

$$X^{\text{smooth}} := \{x \in X \mid f \text{ is smooth at } x\}.$$

Its complement in X is called the singularity locus.

Proposition 1.2.7. *Let $f : X \to Y$ be a morphism of finite type of noetherian schemes. Then the smooth locus of f is open in X.*

Proof. Suppose f is smooth of relative dimension d at $x \in X$. Then there exist an affine open neighbourhood $V = \operatorname{Spec} A$ of $y = f(x)$ and an open neighbourhood

$$U \simeq \operatorname{Spec} A[T_1, \dots, T_{n+d}]/(f_1, \dots, f_n)$$

of x such that the Jacobian matrix $\left(\frac{\partial f_i}{\partial T_j}(x)\right)$ is of rank n. Therefore we can find an $n \times n$ minor (a_{ij}) such that $\det(a_{ij})$ does not vanish at x. It follows that $\det(a_{ij})$ does not vanish in some open neighbourhood U of x. Now U is contained in the smooth locus of f and hence the smooth locus of f is open. $\square$

Definition 1.2.7. A locally noetherian scheme X is regular at $x \in X$ if the local ring $\mathcal{O}_{X,x}$ is a regular local ring. A locally noetherian scheme X is **regular** (or non-singular) if $\mathcal{O}_{X,x}$ is a regular local ring for each $x \in X$.

Remark 1.2.8. Suppose X is a regular scheme. Then for each $x \in X$, the local ring $\mathcal{O}_{X,x}$ is a regular local ring, hence an integral domain. It follows that the scheme X is locally integral. This shows that X is a disjoint union of integral schemes. In particular, a connected regular scheme is integral.

Now we compare these two concepts, namely smoothness and regularity.

Proposition 1.2.9. *Let X be a scheme which is locally of finite type over an arbitrary field k.*
(1) X is smooth over k iff X is geometrically regular.
(2) If X is smooth over k, then X is regular. The converse holds if k is perfect.
(3) Let $x \in X$ be a closed point such that $k(x)|k$ is a separable extension of fields. Then X is smooth at x iff X is regular at x.

Proof. See [2], §2.2, proposition 15. $\square$

Finally, we introduce formally smooth morphisms of schemes. The infinitesimal lifting property will be useful to deduce Hensel's lemma.

Definition 1.2.8. Let $f : X \to Y$ be a morphism of schemes. We say f is **formally smooth** if for each affine scheme $\operatorname{Spec} A$ over Y and for each nilpotent ideal $I \subset A$, the natural map $X(A) \to X(A/I)$ is surjective. This property is also called the **infinitesimal lifting property**.

Proposition 1.2.10. *Let $f : X \to Y$ be a morphism of schemes. Then f is smooth iff f is locally of finite presentation and formally smooth.*

Proof. See [2] §2.2, proposition 6. $\square$

Application: Hensel's lemma

Proposition 1.2.11 (Hensel's lemma)**.** *Let A be a complete noetherian local ring with maximal ideal $\mathfrak{m}$. If $X \to \operatorname{Spec} A$ is smooth, then $X(A) \to X(A/\mathfrak{m})$ is surjective.*

Proof. First we recall a basic fact in algebraic geometry. To give an A-point of X, is the same as to give a point $x \in X$ and a local homomorphism $\varphi : \mathcal{O}_{X,x} \to A$ of local rings. Suppose we are given an A-point of X, say $f : \operatorname{Spec} A \to X$, then we obtain a point $x \in X$ being the image of the closed point of $\operatorname{Spec} A$ and we obtain a local homomorphism $f_x^* : \mathcal{O}_{X,x} \to A_{\mathfrak{m}}$. Since A is local, $A \simeq A_{\mathfrak{m}}$ holds. Conversely, any non-empty open subset of X containing the image of the closed point of $\operatorname{Spec} A$ will contain the image of $\operatorname{Spec} A$, hence we may assume $X = \operatorname{Spec} B$ is affine. Let $\mathfrak{q}$ be the prime ideal corresponding to $x \in X$. Let $B \to B_{\mathfrak{q}} \to A$ be the composition of φ and the canonical homomorphism. Then we obtain a morphism $\operatorname{Spec} A \to X$ sending $\mathfrak{m}$ to x.

If $X \to \operatorname{Spec} A$ is smooth, then by the infinitesimal lifting property, the map

$$X(A/\mathfrak{m}^{n+1}) \to X(A/\mathfrak{m}^n)$$

is surjective for each $n \geq 1$. Now by taking projective limit of $X(A/\mathfrak{m}^{n+1}) \to X(A/\mathfrak{m}^n)$, we obtain a surjective map

$$\varprojlim X(A/\mathfrak{m}^{n+1}) \to \varprojlim X(A/\mathfrak{m}^n)$$

By the above argument, we have

$$X(A/\mathfrak{m}^n) = \{(x, \varphi) \mid x \in X,\ \varphi : \mathcal{O}_{X,x} \to A/\mathfrak{m}^n \text{ local } A\text{-algebra homomorphism}\}$$

for each $n \geq 1$ and it follows that $\varprojlim X(A/\mathfrak{m}^n) = X(\varprojlim A/\mathfrak{m}^n)$. Since A is complete, $A \simeq \varprojlim A/\mathfrak{m}^n$ and therefore $X(A) \to \varprojlim X(A/\mathfrak{m}^n)$ is bijective. For the same reason, $X(A/\mathfrak{m}) \to \varprojlim X(A/\mathfrak{m}^{n+1})$ is bijective. We conclude $X(A) \to X(A/\mathfrak{m})$ is surjective. □

1.3 Grothendieck's topologies

Let T be a topological space. Then we obtain a category whose objects are open subsets of T and morphisms are inclusions. In this section, we generalise the notion of topological spaces to Grothendieck's topologies. We mainly follow Tamme's book [48].

1.3.1 Topologies

Definition 1.3.1. A **topology** (or a **site**) T consists of a category $cat(T)$ and a set $cov(T)$ of coverings, i.e. families $\{\varphi_i : U_i \to U \mid i \in I\}$ of morphisms in $cat(T)$ such that the following properties hold:

T1: for $\{U_i \to U\}$ in $cov(T)$ and a morphism $V \to U$ in $cat(T)$, all fibre products $U_i \times_U V$ exist and $\{U_i \times_U V \to V\}$ is again in $cov(T)$;

T2: given $\{U_i \to U\}$ in $cov(T)$ and a family $\{V_{ij} \to U_i$ in $cov(T)$ for all $i \in I$, the family $\{V_{ij} \to U\}$ obtained by composition of morphisms is also in $cov(T)$;

T3: if $\varphi : U' \to U$ is an isomorphism in $cat(T)$, then $\{\varphi : U' \to U\}$ is in $cov(T)$.

Example 1.3.1. Let T be a topological space. Take $cat(T)$ to be the category of all open subsets of X, and take $cov(T)$ to be families $\{U_i \hookrightarrow U \mid i \in I, \bigcup U_i = U\}$. Suppose $V \to U$ is a morphism in $cat(T)$ and suppose $\bigcup_I U_i = U$. Then $V \subset U$ is an open subset and $U_i \times_V U = U_i \cap V$. This tells us T1 holds. T2 and T3 are obviously true, and hence $cat(T)$ and $cov(T)$ form a topology.

Definition 1.3.2. A morphism $f : T \to T'$ of topologies is a functor $f : cat(T) \to cat(T')$ of the underlying categories with the following two properties:

(1) $\{\varphi_i : U_i \to U\}$ in $cov(T)$ implies $\{f(\varphi_i) : f(U_i) \to f(U)\}$ in $cov(T')$;

(2) for $\{U_i \to U\}$ in $cov(T)$ and a morphism $V \to U$ in $cat(T)$, the canonical morphism

$$f(U_i \times_U V) \to f(U_i) \times_{f(U)} f(V)$$

is an isomorphism for all i.

Example 1.3.2. Let T and T' be topological spaces. If $f : T' \to T$ is a continuous map, then

$$cat(T) \to cat(T'),\ U \mapsto f^{-1}(U)$$

defines a morphism of topologies. Indeed, if $U = \bigcup_I U_i$ is an open covering in T, then $f^{-1}(U) = \bigcup_I f^{-1}(U_i)$ holds. If V is an open subset of U, then $f^{-1}(U_i \times_U V) = f^{-1}(U_i \cap V) = f^{-1}(U_i) \times_{f^{-1}(U)} f^{-1}(V)$. Hence $U \mapsto f^{-1}(U)$ defines a morphism of topologies.

We give several examples in algebraic geometry. Let T be a topology such that each object of $cat(T)$ is a set. We say $\{U_i \to U\}$ in $cov(T)$ is a surjective family if $\bigcup_{i\in I} U_i = U$.

Zariski topologies

Example 1.3.3. Let X be a scheme. We put $cat(X_{Zar})$ to be the category of all Zariski open subsets in X and we put $cov(X_{Zar})$ to be the collection of surjective families of open immersions. Then X_{Zar} is a topology.

Étale topologies

Let X be a fixed scheme. We denote by Et_X the category of étale X-schemes whose objects are étale X-schemes and morphisms are X-morphisms of schemes. A family $\{\varphi_i : U_i \to U \mid i \in I\}$ of morphisms in Et_X is called a surjective family if $U = \bigcup_{i\in I} \varphi_i(U_i)$.

Example 1.3.4. We put $cat(X_{\text{ét}}) = Et_X$ and we put $cov(X_{\text{ét}})$ to be surjective families in Et_X. We verify the axioms T1 to T3 hold. Let $\{U_i \to U\}_{i\in I}$ be a covering and let $V \to U$ be an X-morphism. Then $U_i \times_U V$ exists by general theory and $\{U_i \times_U V \to V\}_{i\in I}$ is a covering since étale morphisms are stable under base change by (1.2.4). This shows T1. T2 and T3 obviously hold. Hence $X_{\text{ét}}$ is indeed a topology and we call it the **étale topology** on X. The category of abelian sheaves on $X_{\text{ét}}$ is denoted by $\mathfrak{Ab}(X_{\text{ét}})$. Sheaves on $X_{\text{ét}}$ are also called **étale sheaves** on X.

Remark 1.3.5. In some literatures, our étale topology is called the **small étale site** on X. The **big étale site** on X has underlying category $\mathfrak{Sch}_X$ being the category of X-schemes and the coverings are the surjective families of étale X-morphisms $\{\varphi_i : U_i \to U \mid i \in I\}$.

Flat topologies

Let X be a scheme. Let $cat(X_{fl})$ be the category of flat X-schemes and let $cov(X_{fl})$ be the collection of surjective families $\{U_i \to U\}_{i\in I}$ of flat X-schemes. Then X_{fl} is a topology by direct verification and (1.2.1).

The fppf topologies

Here fppf is a French abbreviation means faithfully flat and of finite presentation. Let X be a scheme. Suppose $U \to X$ is a flat morphism which is of finite presentation. An fppf covering of U is a surjective family of morphisms $\{\varphi_i : U_i \to U\}_{i\in I}$ of schemes such that each φ_i is flat and locally of finite presentation.

Lemma 1.3.6. *Let U be a scheme.*

(1) If $U' \to U$ is an isomorphism, then $\{U' \to U\}$ is an fppf covering of U.

(2) If $\{U_i \to U\}_{i\in I}$ is an fppf covering and for each i, we have an fppf covering $\{V_{ij} \to U_i\}_{j\in J_i}$, then $\{V_{ij} \to U\}$ is an fppf covering.

(3) If $\{U_i \to U\}_{i\in I}$ is an fppf covering and $U' \to U$ is a morphism of schemes, then $\{U' \times_U U_i \to U'\}_{i\in I}$ is an fppf covering.

Proof. (1) is clear. For (2) and (3), recall that being flat and locally of finite presentation are stable under composition and base change. And the base change of a surjective family of morphisms is still a surjective family. □

Let $cat(X_{\mathrm{fppf}})$ be the category of flat X-schemes of finite presentation and let $cov(X_{\mathrm{fppf}})$ be the collection of surjective families. By the previous lemma, $cat(X_{\mathrm{fppf}})$ and $cov(X_{\mathrm{fppf}})$ forms a topology X_{fppf}.

1.3.2 Sheaves on topologies

A presheaf $\mathcal{F}$ on a topological space T associates each open subset U of T an object $\mathcal{F}(U)$ in some category $\mathfrak{C}$. Note that $\mathcal{F}$ can be viewed as a contravariant functor from the category of open subsets of T to $\mathfrak{C}$. This motivates us to generalise the concept of presheaves on a topological space to presheaves on topologies. Now let T be a topology and let $\mathfrak{C}$ be a category admits products.

Definition 1.3.3. (1) A **presheaf** on T with values in $\mathfrak{C}$ is a contravariant functor $\mathcal{F} : T \to \mathfrak{C}$. A morphism $f : \mathcal{F} \to \mathcal{G}$ of presheaves with values in $\mathfrak{C}$ is defined as a morphism of contravariant functors.

(2) A presheaf $\mathcal{F}$ on T is a **sheaf** if for every covering $\{U_i \to U\}$ in $cov(T)$, the diagram

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

is exact in $\mathfrak{C}$. More explicitly, the first arrow is a monomorphism in $\mathfrak{C}$ and the image of $(F)(U)$ verifies the universal property of kernels of the second two parallel arrows. Morphisms of sheaves are defined as morphisms of presheaves.

(3) Let $\mathfrak{Ab}$ be the category of abelian groups. Presheaves (resp. sheaves) with values in $\mathfrak{Ab}$ are called abelian presheaves (resp. sheaves) on T. We denote by $\mathfrak{Ab}_T^{Pre}$ (resp. $\mathfrak{Ab}_T$) the category of abelian presheaves (resp. sheaves) on T.

Proposition 1.3.7. *Let T be a topology.*

(1) The category $\mathfrak{Ab}_T^{Pre}$ is an abelian category with enough injectives.

(2) A sequence $\mathcal{F}' \to \mathcal{F} \to \mathcal{F}''$ of abelian presheaves on T is exact iff the sequence

$$\mathcal{F}'(U) \to \mathcal{F}(U) \to \mathcal{F}''(U)$$

of abelian groups is exact for all $U \in T$.

Proof. See [48], I, 2.1.1. □

Proposition 1.3.8. *Let T be a topology. Let $\iota : \mathfrak{Ab}_T \to \mathfrak{Ab}_T^{Pre}$, $\mathcal{F} \mapsto \mathcal{F}$ be the inclusion (it is a natural transformation).*

(1) The category $\mathfrak{Ab}_T$ is an abelian category with enough injectives.

(2) The inclusion $\iota : \mathfrak{Ab}_T \to \mathfrak{Ab}_T^{Pre}$ is left exact.

Proof. See [48] I, 3.2.1. □

1.3.3 Cohomology of abelian sheaves on topologies

Let X be a topological space. Then the category $\mathfrak{Ab}_X$ of sheaves of abelian groups on X is an abelian category which has enough injectives. Note that the global section functor $\Gamma(X, -) : \mathfrak{Ab}_X \to \mathfrak{Ab}$ is left exact and hence we can define its derived functors. We denote

$$H^q(X, \mathcal{F}) := R^q\Gamma(X, -)(\mathcal{F})$$

the q-th cohomology group of the sheaf $\mathcal{F}$ of abelian groups on X. This is the cohomology of abelian sheaves in the usual sense. We generalize it to the cohomology of abelian sheaves on topologies now. Let $F : \mathfrak{Ab}_T \to \mathfrak{C}$ be a left exact additive functor where $\mathfrak{C}$ is an abelian category. Then by (1.3.8) the right derived functors R^qF exist. In particular, we consider the section functor

$$\Gamma(U, -) : \mathfrak{Ab}_T \to \mathfrak{Ab},\ \mathcal{F} \mapsto \mathcal{F}(U),$$

which is additive and left exact.

Definition 1.3.4. Let $U \in T$ be a fixed object and let $\mathcal{F}$ be an abelian sheaf on T. We define the **q-th cohomology group of U with values in $\mathcal{F}$** by

$$H^q(U, \mathcal{F}) := R^q\Gamma(U, -)(\mathcal{F}).$$

We will some times write $H^q_T(U, \mathcal{F})$ instead of $H^q(U, \mathcal{F})$ to emphasize the topology T.

Remark 1.3.9. By (1.3.7), the functor $\Gamma(U, -) : \mathfrak{Ab}^{pre}_T \to \mathfrak{Ab}$ is exact. Hence $R^q\Gamma(U, -) = 0$ for each $q \geq 1$. This is the reason why we only study the cohomology group of sheaves.

Example 1.3.10. Let X be a topological space and let T be its topology. Let $\mathcal{F}$ be an abelian sheaf on X. Then the cohomology groups $H^q_T(X, \mathcal{F})$ we just defined, are the usual cohomology groups $H^q(X, \mathcal{F})$.

Étale cohomology groups

Let U be an étale X-scheme. Then we obtain a left exact functor

$$\Gamma(U, -) : \mathfrak{Ab}(X_{\text{ét}}) \to \mathfrak{Ab},\ \mathcal{F} \mapsto \mathcal{F}(U).$$

By (1.3.8), the right derived functors of $\Gamma(U, -)$ exist. Hence we obtain the cohomology groups

$$H^q_{\text{ét}}(U, \mathcal{F}) := R^q\Gamma(U, -)(\mathcal{F})$$

by taking the right derived functors of $\Gamma(U, -)$.

Example 1.3.11. Let X be a scheme. We denote by $\mathbb{G}_m$ the sheaf given by $U \mapsto \Gamma(U, \mathcal{O}_U)^\times$. Then we have

(1) $H^0_{Zar}(X, \mathbb{G}_m) = H^0_{\text{ét}}(X, \mathbb{G}_m) \simeq \Gamma(X, \mathcal{O}_X)^\times$.
(2) $H^1_{Zar}(X, \mathbb{G}_m) = H^1_{\text{ét}}(X, \mathbb{G}_m) \simeq \mathrm{Pic}(X)$.

Proof of (1). By definition, $H^0_{\text{ét}}(X, \mathcal{F}) = R^0(\Gamma(X, -))(\mathcal{F}) = \Gamma(X, \mathcal{F})$ for any abelian étale sheaf $\mathcal{F}$. Hence $H^0_{\text{ét}}(X, \mathbb{G}_m) \simeq \Gamma(X, \mathcal{O}_X)^\times$ holds. $H^0_{Zar}(X, \mathbb{G}_m) = \Gamma(U, \mathcal{O}_U)^\times$ is straightforward. The proof of (2) will use Čech cohomology groups and it will be done later. □

1.3.4 Čech cohomology groups

As in the usual theory of cohomology of sheaves on schemes, the cohomology groups are not easy to compute by definition. One way to reduce the difficulty is to introduce Čech cohomology groups. Thanks to Leray covering theorem, Čech cohomology groups are isomorphic to the cohomology groups defined by derived functors for quasi-compact and separated schemes. Čech cohomology groups really help in computations, for example we can do explicit computation on projective spaces. In this subsection we generalize Čech cohomology groups to abelian presheaves on topologies. Let T be a topology and let $\mathfrak{U} = \{U_i \to U\}_{i \in I}$ be a covering in $cov(T)$. We consider the functor

$$\check{H}^0(\mathfrak{U}, -) : \mathfrak{Ab}^{Pre}_T \to \mathfrak{Ab},$$

which associates each abelian presheaf $\mathcal{F}$ on T the abelian group

$$\check{H}^0(\mathfrak{U}, \mathcal{F}) := \mathrm{Ker}\left(\prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_i \times_U U_j)\right).$$

Then $\check{H}^0(\mathfrak{U}, -)$ is additive and left exact.

Definition 1.3.5. Let $\mathcal{F}$ be an abelian preshef on T. The **q-th Čech cohomology group with values in $\mathcal{F}$ with respect to the covering** $\mathfrak{U} = \{U_i \to U\}$ is defined as

$$\check{H}^q(\mathfrak{U}, \mathcal{F}) := R^q\check{H}^0(\mathfrak{U}, -)(\mathcal{F}).$$

Remark 1.3.12. Let $\mathfrak{U} = \{U_i \to U\}_{i \in I}$ be a covering in $cov(T)$. If $\mathcal{F}$ is an abelian sheaf, then the sequence

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

is exact by definition. Thus $\check{H}^0(\mathfrak{U}, \mathcal{F})$ is identified with $\mathcal{F}(U)$. Moreover, by $\check{H}^0(\mathfrak{U}, \mathcal{F}) = \Gamma(U, \mathcal{F})$ we conclude that $\check{H}^q(\mathfrak{U}, \mathcal{F}) = H^q(U, \mathcal{F})$.

Remark 1.3.13. Note that $\iota : \mathfrak{Ab}_T \to \mathfrak{Ab}_T^{Pre}$ sends injective objects in $\mathfrak{Ab}_T$ to $\check{H}^0(\mathfrak{U}, -)$-acyclic objects in $\mathfrak{Ab}_T^{Pre}$. We obtain for each abelian sheaf $\mathcal{F}$ the spectral sequence

$$\check{H}^p(\mathfrak{U}, R^q\iota(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F}).$$

This spectral sequence describes the relation between Čech cohomology and cohomology with values in abelian sheaves. Here $R^q\iota(\mathcal{F})$ can be identified with the presheaf $\mathcal{H}^q(\mathcal{F})$ which sends U to $H^q(U, \mathcal{F})$.

We omit the discussion of refinement of the coverings in $cov(T)$ for a topology T and we just simply believe the fact that passing to direct limit of all coverings in $cov(T)$ is a well-defined operation. This allows us to give the following:

Definition 1.3.6. Let T be a topology, let $U \in cat(T)$ be an object and let $\mathcal{F}$ be an abelian presheaf on T. For $q \geq 0$, we define the **q-th Čech cohomology group of U with values in $\mathcal{F}$** to be

$$\check{H}^q(U, \mathcal{F}) := \varinjlim_{\mathfrak{U}} \check{H}^q(\mathfrak{U}, \mathcal{F}).$$

It is possible to view $\check{H}^q(U, -)$ as a derived functor. This is guaranteed by the following theorem.

Theorem 1.3.14. *Let T be a topology and let $U \in cat(T)$. The functor*

$$\check{H}^0(U, -) : \mathfrak{Ab}_T^{Pre} \to \mathfrak{Ab}, \ \mathcal{F} \mapsto \check{H}^0(U, \mathcal{F})$$

is left exact and additive. The right derived functors are given by the Čech cohomology groups $\check{H}^q(U, -)$.

Proof. See page 38, theorem 2.2.6 in [48]. □

Theorem 1.3.15 (The spectral sequence for Čech cohomology)**.** *Let T be a topology and let $\mathcal{F}$ be a sheaf of abelian groups on T.*

(1) Let $\mathfrak{U} = \{U_i \to U\}$ be a covering in T. Then there is a spectral sequence

$$\check{H}^p(\mathfrak{U}, \mathcal{H}^q(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F})$$

which is functorial in $\mathcal{F}$.

(2) Let U be an object in T. Then there is a spectral sequence

$$\check{H}^p(U, \mathcal{H}^q(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F})$$

which is functorial in $\mathcal{F}$.

Proof. See page 58, theorem 3.4.4 in [48]. □

Corollary 1.3.16. *Let T be a topology and let $\mathcal{F}$ be a sheaf of abelian groups on T. Then the homomorphisms*

$$\check{H}^q(U, \mathcal{F}) \to H^q(U, \mathcal{F})$$

are bijective for $q = 0, 1$ and injective for $q = 2$.

Proof. The case $q = 0$ follows directly from definition. The terms $\check{H}^0(U, \mathcal{H}^q(\mathcal{F}))$ in the spectral sequence

$$\check{H}^p(U, \mathcal{H}^q(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F})$$

vanish for all $q > 0$. Consider the exact sequence of terms of low degree

$$0 \to \check{H}^1(U, \mathcal{H}^0(\mathcal{F})) \to H^1(U, \mathcal{F}) \to \check{H}^0(U, \mathcal{H}^1(\mathcal{F})) \to \check{H}^2(U, \mathcal{H}^0(\mathcal{F})) \to H^2(U, \mathcal{F}),$$

and note that $\mathcal{H}^0(\mathcal{F}) = \mathcal{F}$, we conclude the assertion. □

We finish this subsection with an example.

Example 1.3.17. Let X be a scheme. Then we have $H^1_{Zar}(X, \mathbb{G}_m) \simeq \mathrm{Pic}(X)$.

Proof. Let $\mathfrak{U} = \{U_i \to X\}$ be an open covering in Zariski topology. Then invertible sheaves on X trivialized by $\mathfrak{U}$ modulo isomorphisms can be identified with $\check{H}^1_{Zar}(X, \mathbb{G}_m)$. We pass to direct limit over all open coverings and then we obtain $\mathrm{Pic}(X) \simeq \check{H}^1_{Zar}(X, \mathbb{G}_m) \simeq H^1_{Zar}(X, \mathbb{G}_m)$. Here the last isomorphism follows from the previous corollary. □

Remark 1.3.18. For the proof of $H^1_{\text{ét}}(X, \mathbb{G}_m) \simeq \mathrm{Pic}(X)$, see [40] page 170.

1.4 Birational maps

In this section we briefly recall rational maps and birational equivalence of varieties. We will need this notion to study the birational invariance of the Brauer groups of schemes and of certain properties of rational points. Then we introduce Hironaka's theorem on resolution of singularities. Finally we study basic properties of del Pezzo surfaces.

1.4.1 Rational maps

Lemma 1.4.1. *Let $f, g : X \to Y$ be two morphisms of schemes with X reduced. Suppose $f(x) = g(x)$ for each $x \in X$. Then $f = g$ as morphisms of schemes.*

Proof. All we need to show is to check f equals to g as morphisms of sheaves, so we may assume $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. By abuse of language, we write $f, g : B \to A$ for the corresponding ring homomorphisms. By assumption, for each $a \in A$, the composition $B \rightrightarrows A \to A_a$ coincides. More explicitly, $f(b)/1 = g(b)/1$ in A_a for each $b \in B$ and hence $a^{n_b}(f(b) - g(b)) = 0$ in A for some integer n_b. We conclude $\mathrm{Im}(f - g) \subset \bigcup \mathrm{Ann}(a^n)$. X is reduced implies that $\operatorname{Spec} A_a$ is dense, but $\operatorname{Spec} A_a \subset V(\mathrm{Ann}(a))$ holds and finally we conclude $\mathrm{Ann}(a^n) = 0$. Consequently, $f, g : B \rightrightarrows A$ coincides and f, g determine the same morphism of schemes. □

Lemma 1.4.2. *Let S be a base scheme. Let X be a reduced scheme over S and let Y be a separated scheme over S. Let f and g be two S-morphisms of X to Y which agree on a non-empty Zariski dense subset of X. Then $f = g$.*

Proof. Suppose $U \subset X$ is the non-empty Zariski dense subset on which f and g coincide. Since $f, g : X \to Y$ are S-morphisms, we obtain an induced morphism $(f, g) : X \to Y \times_S Y$. Y is separated over S implies $\Delta : Y \to Y \times_S Y$ is a closed immersion, and hence $\Delta(Y) \subset Y \times_S Y$ is closed. Since $f|_U = g|_U$, we conclude $(f, g)(U) \subset \Delta(Y)$. This implies the closed subset $(f, g)^{-1}(\Delta(Y))$ of X contains the dense subset U and hence $f = g$ on the underlying topological space of X. But X is reduced, hence $f = g$ as morphisms of schemes. □

Corollary 1.4.3. *Let X and Y be integral varieties over a field k and let f, g be two morphisms from X to Y. Suppose $f|_U = g|_U$ for some non-empty open subset $U \subset X$. Then $f = g$.*

Proof. By assumption X and Y are varieties over k, hence X is reduced and Y is separable over k. Therefore the previous lemma applies and $f = g$ on X. □

Definition 1.4.1. Let X, Y be irreducible schemes over a base scheme S. Let $f : U \to Y$ and $g : V \to Y$ be S-morphisms defined over non-empty open subsets U, V of X. We say f and g are equivalent if $f|_W = g|_W$ for some non-empty subset $W \subset U \cap V$. By the previous lemma, this relation is indeed an equivalent relation. A **rational map** from X to Y over S is an equivalence class of the above equivalent relation.

Definition 1.4.2. Let $f : X \to Y$ be a morphism of schemes. We say f is **dominant** if the image of f is a dense subset in Y.

Remark 1.4.4. In some literature a rational map from X to Y is denoted by $X \dashrightarrow Y$. Dashed arrows are aimed to emphasize that a rational map is not in general a map of the underlying topological spaces. Clearly we can compose dominant rational maps between irreducible schemes, and this leads us to the category whose objects are irreducible schemes and morphisms are dominant rational maps.

Definition 1.4.3. Let X, Y be irreducible schemes over a base scheme S. We say X and Y are **birational** if X and Y are isomorphic in the category of irreducible schemes over S and dominant rational maps over S.

Here is a criterion for birational equivalence.

Lemma 1.4.5. *(1) Let X, Y be irreducible schemes over a base scheme S. Then X, Y are birational iff there are non-empty open subsets $U \subset X$ and $V \subset Y$ such that U, V are isomorphic as S-schemes.*

(2) Let X, Y be integral schemes locally of finite type over a base scheme S. Let x, y be the generic points of X, Y respectively. Then X, Y are birational iff x, y are above the same point $s \in S$ and $\kappa(x) \simeq \kappa(y)$ as extension fields of $\kappa(s)$.

Remark 1.4.6. Let k be a field and let X, Y be integral k-varieties. Then X, Y are birational iff they have isomorphic function fields by (2).

Definition 1.4.4. Let X be an integral variety of dimension n over k.

(1) We say X is k-**rational** or simply **rational**, if X is k-birational to $\mathbb{P}^n_k$.

(2) We say X is **geometrically rational** if there is a field extension $K|k$ such that X_K is integral and K-rational.

1.4.2 Resolution of singularities

We collect some results about resolution of singularities as follows. They will be needed to study unramified Brauer groups of schemes and variants of Brauer-Manin pairing. The main reference is [30].

Theorem 1.4.7 (Hironaka)**.** *Let k be a field of characteristic zero and let X be a smooth variety over k. Let $\mathcal{I}$ be a non-zero ideal sheaf on X. Then there exists a smooth variety X' and a birational and projective morphism $f : X' \to X$ such that*

(1) $f^*\mathcal{I} \subset \mathcal{O}_{X'}$ is a locally principal ideal sheaf on X',

(2) $f : X' \to X$ is an isomorphism over $X - \mathrm{Supp}(\mathcal{O}_X/\mathcal{I})$, and

(3) f is a composition of smooth blowing-ups

$$X' = X_r \to X_{r-1} \to \cdots \to X_1 \to X_0 = X.$$

Proof. See [30], page 136, theorem 3.21. □

Corollary 1.4.8 (Resolution of singularities)**.** *Let k be a field of characteristic zero and let X be a quasi-projective variety over k. Then there is a smooth variety X' and a birational projective morphism $f : X' \to X$.*

Proof. See [30], page 137, corollary 3.22. □

Remark 1.4.9. By the above results and the construction of blowing-up, we can deduce the following assertion. Let X be a smooth geometrically integral variety, then we can find a smooth proper variety X_c containing X as a dense open set. In this case, we say X_c is a smooth proper compactification of X.

1.4.3 Del Pezzo surfaces

Definition 1.4.5. A **del Pezzo surface** over a field k is a smooth geometrically irreducible and proper surface such that $-K_X$ is ample, where K_X is the class of the canonical sheaf ω_X in $\mathrm{Pic}(X)$.

We quote a classification theorem of Iskovskikh to illustrate why del Pezzo surfaces are quite interesting.

Theorem 1.4.10 (Iskovskikh)**.** *Let k be a field. Let X be a smooth projective geometrically rational surface over k. Then X is k-birational to a del Pezzo surface of degree $1 \leq d \leq 9$ or a rational conic bundle surface.*

We need several constructions in general algebraic geometry to define our del Pezzo surfaces.

Definition 1.4.6. Let X be an integral regular variety of dimension n over a field k. We define the **canonical sheaf** of X to be $\omega_X = \bigwedge^n \Omega_{X|k}$, the n-th exterior power of the sheaf of differentials.

The following will be used to describe the exceptional curves on nice surfaces.

Definition 1.4.7. Let X be a projective scheme of dimension n over a field k.
(1) For a coherent sheaf $\mathcal{F}$ on X, we define the **Euler characteristic** of $\mathcal{F}$ by

$$\chi(\mathcal{F}) = \sum (-1)^q \dim_k H^q(X, \mathcal{F}).$$

(2) We define the **arithmetic genus** $p_a(X)$ of X by

$$p_a(X) = (-1)^n(\chi(\mathcal{O}_X) - 1).$$

Then we recall the intersection pairing of the Weil divisor group.

Theorem 1.4.11. *Let X be a regular projective surface over an algebraically closed field k. Then there is a unique pairing*

$$\langle -, - \rangle_X : \mathrm{Div}\, X \times \mathrm{Div}\, X \to \mathbb{Z},\ (C, D) \mapsto C.D,$$

such that
(1) if C and D are regular curves meeting transversally, then $C.D = \mathrm{Card}(C \cap D)$,
(2) it is symmetric: $C.D = D.C$,
(3) it is additive: $(C_1 + C_2).D = C_1.D + C_2.D$, and
(4) it depends only on the linear equivalence classes: if $C_1 \sim C_2$, then $C_1.D = C_2.D$.

When X is a noetherian integral separated locally factorial scheme, there is a natural isomorphism $\mathrm{Cl}\, X \simeq \mathrm{Pic}\, X$. By (4) of the previous theorem, we obtain an intersection pairing

$$\langle -, - \rangle_X : \mathrm{Pic}\, X \times \mathrm{Pic}\, X \to \mathbb{Z}.$$

An **exceptional curve** on a smooth projective surface over k is an irreducible curve $C \subset X_{\overline{k}}$ such that

$$\langle C, C \rangle_X = \langle K_X, C \rangle_X = -1.$$

Definition 1.4.8. The degree of a del Pezzo surface X is the intersection number $\langle K_X, K_X \rangle_X$.

Remark 1.4.12. A smooth exceptional curve has arithmetic genus 0, hence it is $\overline{k}$-isomorphic to $\mathbb{P}^1_{\overline{k}}$.

1.5 An appendix on arithmetic topics

1.5.1 Models over Dedekind schemes

Let X be a scheme over an integral scheme S. Let $\eta \in S$ be the generic point. We obtain a canonical morphism $\operatorname{Spec} \kappa(\eta) \to S$. We call $X_\eta := X \times_S \operatorname{Spec} \kappa(\eta)$ the generic fibre of $X \to S$.

Definition 1.5.1. Let X be a scheme.

(1) We say X is **normal at** $x \in X$ if $\mathcal{O}_{X,x}$ is an integrally closed domain. We say X is **normal** if it is irreducible and normal at each point $x \in X$. In particular, normal schemes are reduced and irreducible hence normal schemes are integral.

(2) We say X a **Dedekind scheme** if X is normal, noetherian and of dimension 1.

Remark 1.5.1. Suppose X is normal at each $x \in X$. Then $\mathcal{O}_{X,x}$ is in particular an integral domain for each $x \in X$. This shows that X is a disjoint union of integral schemes. Here we require the additional condition of irreducibility to guarantee the existence of the function field.

Example 1.5.2. We will use the following examples in the sequel.

(1) Let k be a field. Then $\mathbb{A}_k^n$ and $\mathbb{P}_k^n$ are normal schemes. In particular, $\mathbb{P}_k^1$ is a Dedekind scheme.

(2) Let R be a discrete valuation ring and let K be its fraction field. Then $\operatorname{Spec} R$ is a Dedekind scheme.

Definition 1.5.2. Let S be a Dedekind scheme with function field K. Let X be a scheme of finite type over K.

(1) A **model** for X over S is a flat morphism $\mathcal{X} \to S$ of finite type such that there exists an isomorphism $X \to \mathcal{X}_K = \mathcal{X} \times_S \operatorname{Spec} K$ which identifies X with the generic fibre of $\mathcal{X} \to S$. This can be visualized as the commutative diagram

$$\begin{tikzcd} X \arrow[r, dashed] \arrow[d] & \mathcal{X} \arrow[d] \\ \operatorname{Spec} K \arrow[r] & S \end{tikzcd}$$

which can be identified with a fibred product square.

(2) A morphism $f : \mathcal{X} \to \mathcal{X}'$ of models for X is a morphism $\mathcal{X} \to \mathcal{X}'$ of S-schemes such that the induced morphism

$$X \simeq \mathcal{X}_K \xrightarrow{f \times \mathrm{id}} \mathcal{X}'_K \simeq X$$

is the identity on X.

(3) A model $\mathcal{X}$ for X over S is called a **proper** (resp. **smooth**, etc) model if the structural morphism $\mathcal{X} \to S$ is proper (resp. smooth).

(4) A model $\mathcal{X}$ for X is called a **regular** model if $\mathcal{X}$ is a regular scheme.

Example 1.5.3. Let $S = \operatorname{Spec} A$ be a Dedekind scheme with function field K. Let C be a projective curve over K defined by homogeneous polynomials $F_1, \ldots, F_m \in K[T_0, \ldots, T_n]$. We may assume the F_i have coefficients in A by multiplying the F_i by elements of $A - \{0\}$ if necessary. Let $\mathcal{C} := \operatorname{Proj} A[T_0, \ldots, T_n]/(F_1, \ldots, F_m)$, then we have

$$\operatorname{Proj} K[T_0, \ldots, T_n]/(F_1, \ldots, F_m) \simeq \operatorname{Proj} A[T_0, \ldots, T_n]/(F_1, \ldots, F_m) \times_{\operatorname{Spec} A} \operatorname{Spec} K.$$

Thus $\mathcal{C}$ is a model for C over S.

1.5.2 Reductions

Let X be a scheme over a base scheme S. For $s \in S$, we write $\kappa(s)$ for the residue field of the local ring $\mathcal{O}_{S,s}$. Then we obtain a natural morphism $\operatorname{Spec}\kappa(s) \to S$. We denote by X_s the fibred product $X \times_S \operatorname{Spec}\kappa(s)$. Now let $S = \operatorname{Spec} A$ and let $\mathfrak{p} \subset A$ be a non-zero prime ideal in A. Let $X \to \operatorname{Spec} A$ be a scheme over A. We call

$$X_{\mathfrak{p}} := X \times_A \operatorname{Spec}\kappa(\mathfrak{p})$$

the **reduction of X modulo $\mathfrak{p}$**. We would like to pass to $X_{\mathfrak{p}}$ to study properties of X.

Now suppose X is a scheme over $\mathbb{Q}$. In this case there are no non-trivial homomorphisms $\mathbb{Q} \to \mathbb{F}_p$, hence we can not study X by base change to $\operatorname{Spec}\mathbb{F}_p$. One possible way is considering the canonical projection $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$. If we view the $\mathbb{Q}$-scheme X as a $\mathbb{Z}$-scheme by $X \to \operatorname{Spec}\mathbb{Q} \to \operatorname{Spec}\mathbb{Z}$, then the only non-trivial fibre is the fibre above the generic point. This motivates us to extend X to $\operatorname{Spec}\mathbb{Z}$ such that other fibres are non-trivial. If this is done, then we can base change to $\operatorname{Spec}\mathbb{F}_p$ to study arithmetic properties of X.

Definition 1.5.3. Let S be a Dedekind scheme and let K be the function field of S. Let X be a scheme of finite type over K and let $\mathcal{X}$ be a model for X over S.

(1) Let $s \in S$ be a closed point. The fibre $\mathcal{X}_s$ of $\mathcal{X}$ above s is called **the reduction of X at s**. This can be visualized by the following two fibred product squares:

$$\begin{tikzcd} X \arrow[r, dashed] \arrow[d] & \mathcal{X} \arrow[d] \\ \operatorname{Spec} K \arrow[r] & S \end{tikzcd} \qquad \begin{tikzcd} \mathcal{X}_s \arrow[r] \arrow[d] & \mathcal{X} \arrow[d] \\ \operatorname{Spec}\kappa(s) \arrow[r] & S. \end{tikzcd}$$

(2) We say X has **good reduction** at a closed point $s \in S$ if X admits a smooth and proper model over $\operatorname{Spec}\mathcal{O}_{S,s}$. Note that in this case X is proper and smooth over K and $\mathcal{X} \times_{\mathcal{O}_{S,s}} \kappa(s)$ is proper and smooth over $\kappa(s)$. This can be visualized by the following fibred product square:

$$\begin{tikzcd} X \arrow[r, dashed] \arrow[d] & \mathcal{X} \arrow[d] \\ \operatorname{Spec} K \arrow[r] & \operatorname{Spec}\mathcal{O}_{S,s}. \end{tikzcd}$$

Example 1.5.4. Let $p \neq 3$ be a prime number. Then the curve

$$C = \operatorname{Proj}\mathbb{Q}[X,Y,Z]/(X^3 + Y^3 + p^3 Z^3)$$

admits a model $\mathcal{C}$

$$\operatorname{Proj}\mathbb{Z}[X,Y,W]/(X^3 + Y^3 + W^3)$$

where $W = pZ$ and the fibre $\mathcal{C}_p$ is smooth over p. Hence C has good reduction at p.

Remark 1.5.5. Let k be a number field and let $S = \operatorname{Spec}\mathcal{O}_k$. Suppose X is a smooth projective variety over k. We choose a closed immersion $i : X \to \mathbb{P}^n_k$. Note that $\mathbb{P}^n_k$ is the generic fibre of $\mathbb{P}^n_S \to S$, so the Zariski closure $\mathcal{X}$ of the image of $i(X)$ in $\mathbb{P}^n_S$ is projective over S. Then $\mathcal{X}$ is a model for X over S. $\mathcal{X}$ may have bad special fibres, but we can prove X has good reductions at all but finitely many points.

1.5.3 Passage to limit

Let k be a field and let $\mathbb{P}^1_k$ be the projective line over k. Suppose a k-variety X is endowed with a dominant morphism $\pi : X \to \mathbb{P}^1_k$. Let X_η be the generic fibre of π. We want to show that if X_η has some property $\mathcal{P}$, then all but finitely many fibres of π satisfy the property $\mathcal{P}$.

Let S_0 be a scheme. Let I be a directed set. Let $(\mathcal{A}_i, \varphi_{ij})$ be a direct system, where $\mathcal{A}_i$ is a quasi-coherent $\mathcal{O}_{S_0}$-algebra for each i and $\varphi_{ij} : \mathcal{A}_i \to \mathcal{A}_j$ for $i \leq j$ is a morphism of $\mathcal{O}_{S_0}$-algebras. Let $\mathcal{A} = \varinjlim_I \mathcal{A}_i$ and let $\varphi_i : \mathcal{A}_i \to \mathcal{A}$ be the canonical morphism for each $i \in I$. For each i we construct a scheme $S_i = \mathbf{Spec}\mathcal{A}_i$ which is affine over S_0. Let $\varphi_{ij}^* : S_j \to S_i$ be the S_0-morphism induced by φ_{ij}.

Proposition 1.5.6. *Let $S = \mathbf{Spec}\mathcal{A}$. Then S is the inverse limit of the inverse system (S_i, φ_{ij}^*) in the category of schemes.*

Proof. Step 1. We show that S is the inverse limit of (S_i, φ_{ij}^*) in the category of S_0-schemes. Let X be an S_0-scheme and let $f : X \to S_0$ be its structural morphism. By construction of **Spec**, we have

$$\mathrm{Hom}_{S_0}(X, S_i) \simeq \mathrm{Hom}_{\mathcal{O}_{S_0}}(\mathcal{A}_i, f_*\mathcal{O}_X),$$
$$\mathrm{Hom}_{S_0}(X, S) \simeq \mathrm{Hom}_{\mathcal{O}_{S_0}}(\mathcal{A}, f_*\mathcal{O}_X).$$

Since $\mathcal{A} = \varinjlim_I \mathcal{A}_i$ and $\mathrm{Hom}_{\mathcal{O}_{S_0}}(-, f_*\mathcal{O}_X)$ is left exact, the canonical map

$$\mathrm{Hom}_{\mathcal{O}_{S_0}}(\mathcal{A}, f_*\mathcal{O}_X) \to \varprojlim_I \mathrm{Hom}_{\mathcal{O}_{S_0}}(\mathcal{A}_i, f_*\mathcal{O}_X)$$

is bijective. Hence the canonical map

$$\mathrm{Hom}_{S_0}(X, S) \to \varprojlim_I \mathrm{Hom}_{S_0}(X, S_i)$$

is bijective and S is the inverse limit in the category of S_0-schemes.

Step 2. Now we conclude. Let X be a scheme and let $f \in \mathrm{Hom}_{\mathfrak{Sch}}(X, S_0)$. Then f defines an S_0-scheme structure on X. For an S_0-scheme Y, we denote by $\mathrm{Hom}_f(X, Y)$ the set of S_0-morphisms with respect to the S_0-scheme structure on X defined by f. Therefore we have

$$\mathrm{Hom}_{\mathfrak{Sch}}(X, S_i) = \bigcup_{f \in \mathrm{Hom}_{\mathfrak{Sch}}(X, S_0)} \mathrm{Hom}_f(X, S_i)$$
$$\mathrm{Hom}_{\mathfrak{Sch}}(X, S) = \bigcup_{f \in \mathrm{Hom}_{\mathfrak{Sch}}(X, S_0)} \mathrm{Hom}_f(X, S).$$

By step 1, the canonical map

$$\mathrm{Hom}_f(X, S) \to \varprojlim_I \mathrm{Hom}_f(X, S_i)$$

is bijective and hence the canonical map

$$\mathrm{Hom}_{\mathfrak{Sch}}(X, S) \to \varprojlim_I \mathrm{Hom}_{\mathfrak{Sch}}(X, S_i)$$

is bijective, as required. $\square$

Proposition 1.5.7. *Let S_0 be a quasi-compact and quasi-separated scheme. Let $f_0 : X_0 \to S_0$ be a morphism of finite presentation. If the morphism $f : X_0 \times_{S_0} S \to S$ obtained by base change is proper, then for all but finitely many $i \in I$, the morphism $f_i : X_0 \times_{S_0} S_i \to S_i$ obtained by base change is proper.*

Proof. See [18], proposition 1.10.10. $\square$

Remark 1.5.8. The previous proposition is still true if we replace proper by open immersion, closed immersion, separated, finite, affine, surjective and quasi-finite. All these properties are also proved in [18], proposition 1.10.10.

Example 1.5.9. Let k be a field and let $p : X \to \mathbb{A}^1_k$ be a dominant morphism of schemes. Let η be the generic point of $\mathbb{A}^1_k$. Since p is dominant, the generic fibre X_η is non-empty. Suppose the generic fibre X_η is proper, then by the previous proposition, all but finitely many fibres of $p : X \to \mathbb{A}^1_k$ are proper.

The following is a variant version of passage to limit. It asserts under some condition that properties of the generic fibre will also hold for an open neighbourhood of the generic point.

Proposition 1.5.10. *Let S be an integral scheme and let K be its function field. Suppose X is a scheme of finite presentation over K. Then there exist a dense open subscheme $U \subset S$ and a scheme $\mathcal{X}$ of finite presentation over U such that X can be identified with the generic fibre $\mathcal{X}_K$. This can be visualized as the following fibred product square:*

$$\begin{tikzcd} X \arrow[r, dashed] \arrow[d, "\text{f.p.}"'] & \mathcal{X} \arrow[d, "\text{f.p.}"] \\ \operatorname{Spec} K \arrow[r] & U. \end{tikzcd}$$

Proof. Let $\operatorname{Spec} R$ be a non-empty affine open neighbourhood of the generic point of S. Then K is the fraction field of R and $\operatorname{Spec} R$ is dense in S. Since X is of finite presentation over K, $X = X_1 \cup \cdots \cup X_r$ with $X_i \simeq \operatorname{Spec} K[T_{i1}, \ldots, T_{in_i}]/(f_{i1}, \ldots, f_{im_i})$. $X \to \operatorname{Spec} K$ is of finite presentation (hence quasi-separated) implies that $X_i \cap X_j$ is covered by finitely many affine open subsets X_{ijk} where X_{ijk} is of finite presentation over K. Hence the gluing data of gluing X_i along $X_i \cap X_j$ is given by finitely many polynomials g_l with coefficients in K. We write each coefficient of these f_{ij} and g_l as a fraction of elements of R for $j = 1, \ldots, m_i$, $i = 1, \ldots, r$ and l, and we let Σ denote the set of all the inverse of the appeared denominators. Let R_Σ be the localization of R with respect to the multiplicatively closed subset generated by Σ. We put $U = \operatorname{Spec} R_\Sigma$. By construction, X_i is a scheme of finite presentation over U for each $i = 1, \ldots, r$, and the gluing data will also glue X_i over U. Summing up, the resulting scheme $\mathcal{X}$ is as required. $\square$

Theorem 1.5.11. *Let S be an integral scheme and let K be its function field. We write $\mathcal{P}$ for the following properties of morphisms: affine, open immersion, closed immersion, flat, étale, smooth, separated, proper, projective and geometrically integral.*

(1) Suppose $\mathcal{X} \to S$ is a morphism of finite type and $\mathcal{X}_K \to K$ satisfies $\mathcal{P}$. Then there exists a dense open subscheme $U \subset S$ such that $\mathcal{X}_U \to U$ satisfies $\mathcal{P}$.

(2) Suppose $\mathcal{X}$ and $\mathcal{X}'$ are schemes of finite presentation over S and suppose $f : \mathcal{X}_K \to \mathcal{X}'_K$ is a K-morphism. Then there exists a dense open subscheme $U \subset S$ such that f extends to a U-morphism $\mathcal{X}_U \to \mathcal{X}'_U$.

(3) Suppose $f : \mathcal{X} \to \mathcal{X}'$ is an S-morphism between schemes of finite presentation over S. If $f : \mathcal{X}_K \to \mathcal{X}'_K$ satisfies $\mathcal{P}$, then there exists a dense open subscheme $U \subset S$ such that $f_U : \mathcal{X}_U \to \mathcal{X}'_U$ satisfies $\mathcal{P}$.

Proof. See [40], theorem 3.2.1. $\square$

1.5.4 Adelic points on varieties over number fields

Let X be a variety over a number field k. Let $\mathbb{A}_k$ be the associated ring of adeles and let $k_\Omega = \prod_{v \in \Omega} k_v$. In this section we consider relevant topologies and the relations between $X(\mathbb{A}_k)$ and $X(k_\Omega)$.

v-adic topology on $X(k_v)$

Let X be a variety over a number field k and let k_v be the completion of k with respect to the place v. We define the **v-adic topology** of $X(k_v)$ for $v \in \Omega$ as follows.

(1) If $X = \mathbb{A}^n_k$ is the affine space of dimension n, then we have $\mathbb{A}^n_k(k_v) = \prod_{i=1}^n k_v$. Hence $\mathbb{A}^n_k(k_v)$ is naturally endowed with the product topology obtained from the v-adic topology of k_v. If $X \subset \mathbb{A}^n_k$ is a closed subscheme, then we give $X(k_v) \subset \prod_{i=1}^n k_v$ the subspace topology.

(2) In general, $X = X_1 \cup \cdots \cup X_r$ where

$$X_\alpha \simeq \operatorname{Spec} k[T_{\alpha 1}, \ldots, T_{\alpha s_\alpha}]/I_\alpha \text{ for some ideal } I_\alpha$$

and hence X_α is identified with a closed subscheme of $\mathbb{A}_k^{s_\alpha}$ for each $\alpha = 1, \ldots, r$. Then we need to glue $X_1(k_v), \ldots, X_r(k_v)$ together. Suppose $X_1, \ldots, X_r$ are glued via Zariski open subsets $U_{\alpha\beta} \subset X_\alpha$ and $\varphi_{\alpha\beta} : U_{\alpha\beta} \to U_{\beta\alpha}$ for each $\alpha \neq \beta$. We obtain a homeomorphism

$$\phi_{\alpha\beta} : U_{\alpha\beta}(k_v) \to U_{\beta\alpha}(k_v),\ u_{\alpha\beta} \mapsto \varphi_{\alpha\beta} \circ u_{\alpha\beta}.$$

Then we have $\phi_{\beta\alpha} = \phi_{\alpha\beta}^{-1}$, $\phi_{\alpha\beta}(U_{\alpha\beta}(k_v) \cap U_{\alpha\gamma}(k_v)) = U_{\beta\alpha}(k_v) \cap U_{\beta\gamma}(k_v)$ and $\phi_{\alpha\gamma} = \phi_{\beta\gamma} \circ \phi_{\alpha\beta}$. Therefore the gluing data of $X_1, \ldots, X_r$ will also glue $X_1(k_v), \ldots, X_r(k_v)$ together. We call the resulting topology on $X(k_v)$ the v-adic topology of X.

Remark 1.5.12. Suppose k is a topological field. Let X be a variety over k. Then the above construction also works for $X(k)$. The resulting topology is called the **analytic topology** on $X(k)$. In general, the analytic topology is different from the Zariski topology.

Adelic topology on $X(\mathbb{A}_k)$

Let X be a variety over a number field k. We define the **adelic topology** on $X(\mathbb{A}_k)$ as follows. X admits a model $\mathcal{X}$ that is separated and of finite type over $\operatorname{Spec} \mathcal{O}_k$. If $v \in \Omega_f$, then we give $\mathcal{X}(\mathcal{O}_v) \subset \mathcal{X}(k_v)$ the subspace topology. We equip the set $X(\mathbb{A}_k)$ of all adelic points on X with the restricted topological product with respect to $X(k_v)$ for $v \in \Omega_\infty$ and $\mathcal{X}(\mathcal{O}_v)$ for $v \in \Omega_f$. By definition, an open base for topology is of the form

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{X}(\mathcal{O}_v),$$

where S is a finite subset of Ω containing the set all the archimedean places Ω_∞ and U_v is an open subset of $X(k_v)$ for each $v \in S$.

Remark 1.5.13. Of course we can view $X(\mathbb{A}_k) = \operatorname{Hom}_{\mathfrak{Sch}_k}(\operatorname{Spec} \mathbb{A}_k, X)$ as the set of all k-morphisms from $\operatorname{Spec} \mathbb{A}_k$ to X, but in this way the topology of $X(\mathbb{A}_k)$ is not clear. We thus consider a model over $\mathcal{O}_k$ to construct explicitly an open base for topology. We will see later that the adelic topology on $X(\mathbb{A}_k)$ does not depend on the choice of the model $\mathcal{X}$.

Adelic points on varieties

Let X be a scheme over a field k. We make the following remarks to give the explicit relations between k-points, adelic points and k_Ω-points on X.

(0) First of all, $k \subset k_v$ induces a map $X(k) \to X(k_v)$. This means each k-point gives rise to a k_v-point. By (1.4.1), we can view $X(k)$ as a subset of $X(k_v)$.

(1) By the diagonal embedding $k \hookrightarrow \mathbb{A}_k$, we obtain an induced map $X(k) \to X(\mathbb{A}_k)$. This means each k-point on X induces an adelic point on X.

(2) By construction we have $\mathbb{A}_k \subset k_\Omega$, we obtain a map $X(\mathbb{A}_k) \to \prod_{v \in \Omega} X(k_v) = X(k_\Omega)$. This means each adelic point on X gives rise to a k_Ω-point on X.

(3) By the canonical projection $k_\Omega \to k_v$, we obtain a map $X(k_\Omega) \to X(k_v)$. This tells us each k_Ω-point on X induces a k_v-point for each $v \in \Omega$. In particular, each adelic point on X gives rise to a k_v-point for each $v \in \Omega$ via $X(\mathbb{A}_k) \to X(k_\Omega) \to X(k_v)$.

Proposition 1.5.14. *Let k be a number field and let X be a k-scheme. Then the canonical map $X(k) \to X(\mathbb{A}_k)$ is injective.*

Proof. Suppose x_1 and x_2 have the same image in $X(\mathbb{A}_k)$. Then $x_1 \circ \Delta^* = x_2 \circ \Delta^* : \operatorname{Spec} \mathbb{A}_k \to X$ as morphisms of schemes, where Δ^* denotes the morphism induced by the diagonal embedding $k \to \mathbb{A}_k$. Then Δ^* is surjective implies that $x_1 = x_2$ as a map between topological spaces and let $x \in X(\mathbb{A}_k)$ be their image in X. Now we consider the homomorphisms $\varphi_i : \mathcal{O}_{X,x} \to k$ induced by x_i for $i = 1, 2$. Since $x_1 \circ \Delta^* = x_2 \circ \Delta^*$, we conclude $\Delta \circ \varphi_1 = \Delta \circ \varphi_2$. Note that $\Delta : k \to \mathbb{A}_k$ is injective, therefore $\varphi_1 = \varphi_2$ holds. It follows that $x_1 = x_2$ as morphisms of schemes. $\square$

Consequently, we can view $X(k)$ as a subset of $X(\mathbb{A}_k)$.

Proposition 1.5.15. *Let k be a number field and let X be a separated k-scheme. Then the sequence $(x_v) \in \prod_{v\in\Omega} X(k_v)$ determines the corresponding adelic point (if it exists) uniquely.*

Proof. Let $\pi_v : \mathbb{A}_k \to k_v$ be the canonical projection to the v-component. It is clear that the image of the canonical morphism $\operatorname{Spec} k_v \to \operatorname{Spec} \mathbb{A}_k$ is $\pi_v^{-1}(0) = \{(a_w) \in \mathbb{A}_k \mid a_v = 0\}$. We can therefore identify $\operatorname{Spec} k_v$ with its image in $\operatorname{Spec} \mathbb{A}_k$ and we claim $\bigcup_{v\in\Omega} \operatorname{Spec} k_v \subset \operatorname{Spec} \mathbb{A}_k$ is Zariski dense. Indeed, let $0 \neq a \in \mathbb{A}_k$ be an arbitrary adele, then $a_v \neq 0$ for some $v \in \Omega$. By construction, $\operatorname{Spec} k_v \subset D(a)$ holds. Recall that $\{D(a) \mid 0 \neq a \in \mathbb{A}_k\}$ is an open base for topology, thus we are done.

Suppose $x_1, x_2 : \operatorname{Spec} \mathbb{A}_k \to X$ induce the same element in $\prod_{v\in\Omega} X(k_v)$. This means that x_1 and x_2 coincide on $\bigcup_{v\in\Omega} \operatorname{Spec} k_v$. Now X is separable, $\operatorname{Spec} \mathbb{A}_k$ is integral hence reduced, and x_1, x_2 coincide on a dense subset of $\operatorname{Spec} \mathbb{A}_k$. Therefore $x_1 = x_2$ by (1.4.2). ☐

Remark 1.5.16. We obtain $X(\mathbb{A}_k) \subset X(k_\Omega)$ by (1.5.15), hence each adelic point on X can be represented by a family $(x_v) \in \prod_{v\in\Omega} X(k_v)$. Moreover, $X(\mathbb{A}_k)$ can be endowed with the subspace topology of $X(k_\Omega)$ by $X(\mathbb{A}_k) \subset X(k_\Omega)$. The resulting topology is called the **product topology** of $X(\mathbb{A}_k)$.

Suppose $\mathcal{X}$ is a separated scheme of finite type over $\operatorname{Spec} \mathcal{O}_k$ with generic fibre $X = \mathcal{X} \times_{\mathcal{O}_k} k$. Next we introduce a criterion which tells us that whether a k_Ω-point on X comes from an adelic point on X. Note that $\mathcal{X}(\mathcal{O}_v) \subset \mathcal{X}(k_v)$ by the valuation criterion of separated morphisms, and direct verification tells us $X(k_v)$ can be identified with a subset of $\mathcal{X}(k_v)$.

Proposition 1.5.17. *Let k be a number field and let $\mathcal{O}_k$ be the ring of algebraic integers in k. Let $\mathcal{X}$ be a separated $\mathcal{O}_k$-scheme of finite type over $\mathcal{O}_k$ and let $X = \mathcal{X} \times_{\mathcal{O}_k} k$ be the generic fibre. Then a k_Ω-point $(x_v) \in \prod_{v\in\Omega} X(k_v)$ is induced by an adelic point iff all but finitely many x_v are also $\mathcal{O}_v$-points on $\mathcal{X}$.*

Proof. Let $\Omega_\infty \subset S \subset \Omega$ be a finite set of places containing all Archimedean places of k. Let $(x_v) \in \prod_{v\in\Omega} X(k_v)$ be a k_Ω-point such that $x_v \in \mathcal{X}(\mathcal{O}_v)$ for $v \notin S$ and $x_v \in \mathcal{X}(k_v)$ for $v \in S$. We need to show $(x_v) \in X(\mathbb{A}_k)$.

To simplify the notation, we write $R_v = \mathcal{O}_v$ for $v \notin S$ and $R_v = k_v$ for $v \in S$. Now we have $x_v \in \mathcal{X}(R_v)$ for each $v \in \Omega$. Let $R = \prod_{v\in\Omega} R_v$. Suppose there is a morphism $\operatorname{Spec} R \to \mathcal{X}$ induced by (x_v). Now $\prod R_v = \prod_{v\in S} k_v \times \prod_{v\notin S} \mathcal{O}_v \subset \mathbb{A}_k$ will induce a canonical morphism $\operatorname{Spec} \mathbb{A}_k \to \operatorname{Spec} R$. Therefore (x_v) is induced by an adelic point.

Now we show that there is a morphism $\operatorname{Spec} R \to \mathcal{X}$. If $\mathcal{X} = \operatorname{Spec} A$ is affine, then

$$\operatorname{Hom}_{\mathfrak{Sch}}(\operatorname{Spec} R, \operatorname{Spec} A) \simeq \operatorname{Hom}_{\mathfrak{Ring}}(A, \prod R_v) \simeq \prod \operatorname{Hom}_{\mathfrak{Ring}}(A, R_v) \neq \emptyset.$$

Here $\mathfrak{Ring}$ denotes the category of commutative rings with neutral elements. In general, note that $\mathcal{X}$ is of finite type over $\operatorname{Spec} \mathcal{O}_k$ and hence $\mathcal{X}$ is quasi-compact. We cover $\mathcal{X}$ by finitely many open affine subsets $\mathcal{X}_i = \operatorname{Spec} A_i$ for $i = 1, \dots, n$. Each R_v is a local ring, so the image of $\operatorname{Spec} R_v$ is contained in one and only one of $\mathcal{X}_i$ for $i = 1, \dots, n$. Let

$$S_i = \{v \in \Omega \mid \text{the image of } \operatorname{Spec} R_v \to \mathcal{X} \text{ lies in } \mathcal{X}_i\}$$

and then $\Omega = \bigsqcup_{i=1}^n S_i$. Now $\operatorname{Spec} R_v \to \mathcal{X}_i$ for $v \in S_i$ gives rise to a morphism $\operatorname{Spec} \prod_{v\in S_i} R_v \to \mathcal{X}_i \subset \mathcal{X}$. Note that $\bigsqcup_{i=1}^n \operatorname{Spec} \prod_{v\in S_i} R_v \simeq \operatorname{Spec} \prod_{v\in\Omega} R_v = \operatorname{Spec} R$ since the left hand side is a finite disjoint union. Therefore we obtain a morphism $\operatorname{Spec} R \to \bigsqcup_{i=1}^n \operatorname{Spec} \prod_{v\in S_i} R_v \to \bigcup \mathcal{X}_i = \mathcal{X}$. By construction, the image of $\operatorname{Spec} R$ in $\mathcal{X}$ is contained in the generic fibre and hence we obtain an adelic point on X.

Conversely, let $(x_v) \in \prod X(k_v)$ be an adelic point on X. We cover $\mathcal{X}$ by open affine subsets $\mathcal{X}_i$ for $i = 1, \dots, n$ with $\mathcal{X}_i \simeq \operatorname{Spec} \mathcal{O}_k[T_1^{(i)}, \dots, T_{r_i}^{(i)}]/\mathfrak{a}_i$. The adelic point (x_v) induces homomorphisms of $\mathcal{O}_k$-algebras

$$\varphi_i : \mathcal{O}_k[T_1^{(i)}, \dots, T_{r_i}^{(i)}]/\mathfrak{a}_i \to (\mathbb{A}_k)_{f_i}$$

for some $f_i \in \mathbb{A}_k$ such that $(f_1, \ldots, f_n) = (1)$. We fix adeles $g_1, \ldots, g_n \in \mathbb{A}_k$ such that $f_1 g_1 + \cdots + f_n g_n = 1$ and let $\varphi_i(T_j^{(i)}) = h_{ij}/f_i^{e_{ij}}$ with $h_{ij} \in \mathbb{A}_k$ and $e_{ij} \in \mathbb{Z}_{\geq 0}$. Let S be the union of Ω_∞ and the places $v \in \Omega_f$ such that not all the adeles g_i and h_{ij} are integral at v. Then S is a finite set of places. Take $v \notin S$. Then

$$1 = |(f_1 g_1 + \cdots + f_n g_n)_v|_v \leq \max |(f_i g_i)_v|_v \leq \max |(f_i)_v|_v$$

implies that $|(f_i)_v|_v \geq 1$ for some i. By construction $|(h_{ij})_v|_v \leq 1$ and therefore $(\varphi_i(T_j^{(i)}))_v \in \mathcal{O}_v$ for each j. It follows that φ_i induces a morphism $\operatorname{Spec} \mathcal{O}_v \to \mathcal{X}_i \subset \mathcal{X}$. $\square$

Comparing adelic topology with product topology

As we have seen, $X(\mathbb{A}_k) \subset X(k_\Omega)$ can be endowed with the subspace topology.I n general, the adelic topology of $X(\mathbb{A}_k)$ is different from the product topology of $X(\mathbb{A}_k)$. Now we compare these two topologies on $X(\mathbb{A}_k)$ for a proper variety X over k.

Proposition 1.5.18. *Let X be a proper variety over k, then $X(\mathbb{A}_k) = \prod_{v \in \Omega} X(k_v)$.*

Proof. First X is proper hence separated, it follows that $X(\mathbb{A}_k) \subset X(k_\Omega)$. Conversely, we can find a scheme $\mathcal{X}$ which is proper over $\mathcal{O}_{k,S}$ for some finite subset $\Omega_\infty \subset S \subset \Omega$ such that the generic fibre can be identified with X. By construction $\mathcal{O}_{k,S} \subset \mathcal{O}_v$ for $v \notin S$, then we obtain an induced map $\operatorname{Spec} \mathcal{O}_v \to \operatorname{Spec} \mathcal{O}_{k,S}$. Finally, $x_v \in X(k_v)$ will give rise to a morphism $\operatorname{Spec} k_v \to \mathcal{X}$. We obtain a commutative diagram

$$\begin{tikzcd} \operatorname{Spec} k_v \arrow[r] \arrow[d] & \mathcal{X} \arrow[d] \\ \operatorname{Spec} \mathcal{O}_v \arrow[r] \arrow[ur, dashed] & \operatorname{Spec} \mathcal{O}_{k,S}. \end{tikzcd}$$

The image of $\operatorname{Spec} k_v$ in $\operatorname{Spec} \mathcal{O}_{k,S}$ via $\operatorname{Spec} \mathcal{O}_v$ is the generic point, hence the image of $\operatorname{Spec} k_v$ in $\mathcal{X}$ lies in the generic fibre X, i.e. $\mathcal{X}(k_v) = X(k_v)$ holds for $v \notin S$. We conclude that for the places $v \notin S$, we have $\mathcal{X}(\mathcal{O}_v) = \mathcal{X}(k_v)$ by the valuation criterion of proper morphisms. Hence $X(k_v) = \mathcal{X}(\mathcal{O}_v)$ for each $v \notin S$. It follows that $(x_v) \in X(\mathbb{A}_k)$ by (1.5.17) and this implies $X(k_\Omega) \subset X(\mathbb{A}_k)$. $\square$

An open base for the product topology (resp. adelic topology) is of the form

$$\prod_{v \in S} U_v \times \prod_{v \notin S} X(k_v) \quad (\text{resp. } \prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{X}(\mathcal{O}_v)).$$

We have seen that $X(k_v) = \mathcal{X}(\mathcal{O}_v)$ and therefore the adelic topology and the product topology are equivalent when X is proper over k.

1.5.5 Implicit function theorem

The inverse function theorem and the implicit function theorem are well-known over $\mathbb{R}$ and $\mathbb{C}$. For arithmetic concerning, we will consider the v-adic implicit function theorem where v is a place of a number field. We begin with generalizing analytic functions to fields endowed with a non-trivial absolute value. The main reference is chapter II in [42].

Let k be a complete field with respect to a non-trivial absolute value $|-|$ (archimedean or ultrametric). For $\boldsymbol{x} \in k^n$ and $\boldsymbol{r} \in \mathbb{R}_{>0}^n$, we define $|\boldsymbol{x}| \leq \boldsymbol{r}$ (resp. $|\boldsymbol{x}| < \boldsymbol{r}$) $\iff$ $|x_i| \leq r_i$ (resp. $|x_i| < r_i$) for $i = 1, \ldots, n$. We put

$$\overline{P}_{\boldsymbol{r}}(\boldsymbol{x}) = \{\boldsymbol{y} \mid |\boldsymbol{y} - \boldsymbol{x}| \leq \boldsymbol{r}\} \quad (\text{resp. } P_{\boldsymbol{r}}(\boldsymbol{x}) = \{\boldsymbol{y} \mid |\boldsymbol{y} - \boldsymbol{x}| < \boldsymbol{r}\})$$

to be the polydisk (resp. strict polydisk) of radius $\boldsymbol{r}$ and center $\boldsymbol{x}$. Thanks to the absolute value on k, we can define convergent power series with coefficients in k.

Definition 1.5.4. Let $f = \sum a_I \boldsymbol{X}^I$ be a formal power series with $a_I \in k$. Here I denotes multi-index $(i_1, \ldots, i_n)$ and $\boldsymbol{X}^I = X_1^{i_1} \ldots X_n^{i_n}$.

(1) We say f is convergent in $\overline{P}_{\boldsymbol{r}}(0)$ if $\sum |a_I| \boldsymbol{r}^I < \infty$.

(2) We say f is convergent in $P_{\boldsymbol{r}}(0)$ if f is convergent in $\overline{P}_{\boldsymbol{r}'}(0)$ for each $\boldsymbol{r}' < \boldsymbol{r}$.

Then it is possible to define analytic functions and analytic maps.

Definition 1.5.5. (1) Let $U \subset k^n$ be an open subset and let $\varphi : U \to k$ be a function. Then we say φ is analytic in U if for each $\boldsymbol{x} \in U$, there is a formal power series f and a radius $\boldsymbol{r} > 0$ such that $P_{\boldsymbol{r}}(\boldsymbol{x}) \subset U$ and f converges in $P_{\boldsymbol{r}}(\boldsymbol{x})$ and for $\boldsymbol{h} \in P_{\boldsymbol{r}}(\boldsymbol{x})$, $\varphi(\boldsymbol{x} + \boldsymbol{h}) = f(\boldsymbol{h})$.

(2) Let $U \subset k^n$ be an open subset and let $\varphi = (\varphi_1, \ldots, \varphi_m) : U \to k^m$ be a continuous map. Then we say φ is analytic if φ_i is analytic for $i = 1, \ldots, m$.

Theorem 1.5.19 (v-adic inverse function theorem)**.** *Let $U \subset k^n$ be an open subset and let $f : U \to k^n$ be an analytic map such that $f(0) = 0$. If $Df(0) : k^n \to k^n$ is a linear isomorphism, then f is a local analytic isomorphism.*

Proof. See [42], chapter II. ∎

As usual, we can prove the v-adic implicit function theorem by applying the v-adic inverse function theorem.

Theorem 1.5.20 (v-adic implicit function theorem)**.** *Let*

$$F : k^{n+m} \to k^m, \ (\boldsymbol{x}, \boldsymbol{y}) \mapsto (F_1(\boldsymbol{x}, \boldsymbol{y}), \ldots, F_m(\boldsymbol{x}, \boldsymbol{y}))$$

be an analytic map such that $F_i(\boldsymbol{0}, \boldsymbol{0}) = \boldsymbol{0}$ for each $i = 1, \ldots, m$ and $\det\left(\frac{\partial F_i}{\partial y_j}(\boldsymbol{0}, \boldsymbol{0})\right) \neq 0$. Then there exists a unique analytic map

$$f : k^n \to k^m, \ \boldsymbol{x} \mapsto (f_1(\boldsymbol{x}), \ldots, f_m(\boldsymbol{x}))$$

such that $f_i(\boldsymbol{0}) = \boldsymbol{0}$ satisfying $F(\boldsymbol{x}, f(\boldsymbol{x})) = 0$.

Chapter 2

Brauer groups and Brauer-Manin obstruction

The first goal of this chapter is to introduce the Brauer groups of schemes. We begin with the Brauer group of a field by group cohomology and then we compare it with the classical definition by central simple algebras. Then we generalize this definition to the Brauer group of a local ring by replacing central simple algebras over a field with Azumaya algebras over a local ring. Later we study the Brauer group of a scheme in terms of étale cohomology and we end up with the unramified Brauer group of a variety. The next goal is to introduce the Hasse principle, weak approximation, and strong approximation for varieties over a number field k. We will find a closed subset of $X(\mathbb{A}_k)$ containing $X(k)$ defined by the Brauer-Manin pairing. Then we are in a position to state several slightly different Brauer-Manin obstructions to the Hasse principle and weak approximation. Finally we briefly introduce some technical results.

2.1 Brauer groups of fields

2.1.1 The Brauer group

Cohomological description

Let $L|K$ be a finite Galois extension of any fields and let

$$H^2(L|K) = H^2(\mathrm{Gal}(L|K), L^\times).$$

Let $(L_i)_{i\in I}$ be the family of all finite Galois extensions of K. Suppose L_i and L_j are two finite Galois extensions of K, then we can always find a finite Galois extension L_k containing the composite $L_i.L_j$. Hence the family $(L_i)_{i\in I}$ forms a directed set. Then we can define the **Brauer group** of K to be

$$\mathrm{Br}(K) := \varinjlim_{i\in I} H^2(L_i|K).$$

We can write more explicitly that $\mathrm{Br}(K) = \bigcup_{i\in I} H^2(L_i|K)$ because for each $L_i \subset L_j$, the homomorphism $H^2(L_i|K) \to H^2(L_j|K)$ is injective by (1.1.15).

By infinite Galois theory, we have

$$\mathrm{Gal}(K_s|K) \simeq \varprojlim_{I} \mathrm{Gal}(K_s|K)/\,\mathrm{Gal}(K_s|L_i) \simeq \varprojlim_{I} \mathrm{Gal}(L_i|K)$$

where K_s is the separable closure of K, $L_i|K$ runs through all finite Galois extensions and

$\mathrm{Gal}(K_s|L_i)$ runs through all open and normal subgroups of $\mathrm{Gal}(K_s|K)$. Hence we conclude

$$\begin{aligned} H^2(\mathrm{Gal}(K_s|K), K_s^\times) &\simeq \varinjlim_I H^2\big(\mathrm{Gal}(K_s|K)/\mathrm{Gal}(K_s|L_i), (K_s^\times)^{\mathrm{Gal}(K_s|L_i)}\big) \\ &\simeq \varinjlim_I H^2(\mathrm{Gal}(L_i|K), L_i^\times) = \varinjlim_I H^2(L_i|K). \end{aligned}$$

Therefore we have the identification

$$H^2(K_s|K) := H^2(\mathrm{Gal}(K_s|K), K_s^\times) \simeq \mathrm{Br}(K).$$

Central simple algebras

Now we introduce central simple algebras and then we study another equivalent description of the Brauer group over a field K. For any ring A, we denoted by $M_n(A)$ the ring of all $n \times n$ matrices with all entries in A.

Proposition 2.1.1. *Let K be a field and let A be a finite dimensional K-algebra. The following are equivalent:*

(1) A has no non-trivial two-sided ideal, and the center of A is K.

(2) $A \otimes_K \overline{K} \simeq M_n(\overline{K})$ for some positive integer n, where $\overline{K}$ is an algebraic closure of K.

(3) There exists a finite Galois extension $L|K$ such that $A \otimes_K L \simeq M_n(L)$ for some positive integer n.

(4) $A \simeq M_n(D)$ for some positive integer n, where D is a division algebra with center K.

Proof. For a proof, see Bourbaki, Algebra, chapter VIII, §§5, 10. □

Definition 2.1.1. (1) Suppose A is a K-algebra that satisfies conditions (1) to (4) above. Then A is called a **central simple** K-algebra.

(2) Let A and A' be two central simple K-algebras. Then $A \simeq M_n(D)$ and $A' \simeq M_{n'}(D')$ for some division K-algebras D and D'. We say A is similar to A' over K if $D \simeq D'$ as K-algebras. Note that this is an equivalent relation.

(3) We denote by $\mathrm{Br}_{\mathrm{Az}}(K)$ the set of similarity classes of central simple algebras over K.

Remark 2.1.2. Let A and A' be two central simple K-algebras of the same dimension. Then to say A is similar to A' is equivalent to say they are K-isomorphic.

Remark 2.1.3 (Group structure)**.** We give $\mathrm{Br}_{\mathrm{Az}}(K)$ a group structure as follows. Take $[A], [A'] \in \mathrm{Br}_{\mathrm{Az}}(K)$. By definition we have $A \simeq M_n(D)$, $A' \simeq M_{n'}(D')$ for some division algebra D and D' over K. Since

$$A \otimes_K A' \simeq M_n(D) \otimes_K M_{n'}(D') \simeq M_{nn'}(D \otimes_K D')$$

is a central simple algebra, we can define

$$\mathrm{Br}_{\mathrm{Az}}(K) \times \mathrm{Br}_{\mathrm{Az}}(K) \to \mathrm{Br}_{\mathrm{Az}}(K),\ ([A], [A']) \mapsto [A \otimes_K A'].$$

Then we have $[A][K] = [A]$ and $[A][A^{\mathrm{op}}] = [K]$. Thus the tensor product makes $\mathrm{Br}_{\mathrm{Az}}(k)$ into an abelian group, and $[K] = [M_n(K)]$ for any positive n is the neutral element. This is the **classical Brauer group**.

Remark 2.1.4 (Covariant functor)**.** Let $L|K$ be a field extension, then we obtain a group homomorphism

$$\mathrm{Br}_{\mathrm{Az}}(K) \to \mathrm{Br}_{\mathrm{Az}}(L),\ A \mapsto A \otimes_K L.$$

It's easy to check that $\mathrm{Br}_{\mathrm{Az}}(-)$ forms a covariant functor from the category of fields to the category of groups.

The equivalence of two constructions

The aim of this subsection is to show $\mathrm{Br}_{\mathrm{Az}}(K) \simeq \mathrm{Br}(K)$. Let $L|K$ be a field extension. We denote by

$$\mathrm{Br}_{\mathrm{Az}}(L|K) := \mathrm{Ker}(\mathrm{Br}_{\mathrm{Az}}(K) \to \mathrm{Br}_{\mathrm{Az}}(L))$$

the kernel of the restriction homomorphism.

Take $A \in \mathrm{Br}_{\mathrm{Az}}(K)$, then by (3) in (2.1.1) we obtain $A \otimes_K L \simeq M_n(L)$ for some finite Galois extension L of K. This tells us $\mathrm{Br}_{\mathrm{Az}}(K)$ is the union of $\mathrm{Br}_{\mathrm{Az}}(L|K)$ as L runs through all the finite Galois extensions of K. Hence it will be sufficient to construct isomorphisms

$$\mathrm{Br}_{\mathrm{Az}}(L_i|K) \to H^2(L_i|K)$$

for each finite Galois extension $L_i|K$ that compatible with the injections

$$\mathrm{Br}_{\mathrm{Az}}(L_i|K) \to \mathrm{Br}_{\mathrm{Az}}(L_j|K) \text{ and } H^2(L_i|K) \to H^2(L_j|K),$$

for field extension $L_j|L_i$.

Let $\mathrm{Br}_{\mathrm{Az}}(n, L|K)$ be the set of similarity classes of K-algebras A such that $A \otimes_K L \simeq M_n(L)$. Then the group $\mathrm{Br}_{\mathrm{Az}}(L|K) = \bigcup_{n \geq 1} \mathrm{Br}_{\mathrm{Az}}(n, L|K)$.

Proposition 2.1.5. *Let $L|K$ be a finite Galois extension. Then the canonical map*

$$\theta_n : \mathrm{Br}_{\mathrm{Az}}(n, L|K) \to H^1(\mathrm{Gal}(L|K), \mathrm{PGL}_n(L))$$

is bijective.

Proof. See [43] page 158, proposition 8. □

On the other hand, we have a short exact sequence $1 \to L^\times \to \mathrm{GL}_n(L) \to \mathrm{PGL}_n(L) \to 1$ with $L^\times$ contained in the center of $\mathrm{GL}_n(L)$. The short exact sequence defines a coboundary operator

$$\Delta_n : H^1(\mathrm{Gal}(L|K), \mathrm{PGL}_n(L)) \to H^2(\mathrm{Gal}(L|K), L^\times)$$

of pointed sets (see [44], section 5.7). Composing θ_n and Δ_n gives a map

$$\delta_n : \mathrm{Br}_{\mathrm{Az}}(n, L|K) \to H^2(\mathrm{Gal}(L|K), L^\times) = H^2(L|K).$$

We want these $\{\delta_n\}_{n \geq 1}$ to be compatible so that we will have a homomorphism

$$\delta : \mathrm{Br}_{\mathrm{Az}}(L|K) \to H^2(L|K).$$

This is guaranteed by the following:

Lemma 2.1.6. *For $C \in \mathrm{Br}_{\mathrm{Az}}(n, L|K)$ and $C' \in \mathrm{Br}_{\mathrm{Az}}(n', L|K)$, then*

$$\delta_{nn'}(C \otimes_K C') = \delta_n(C) + \delta_{n'}(C').$$

Moreover, $\delta_n(C) = 0$ iff C is a matrix algebra.

Proof. See [43] page 158, lemma 1. □

Now we can conclude.

Proposition 2.1.7. *(1) If $n = [L : K]$, then the map $\delta_n : \mathrm{Br}_{\mathrm{Az}}(n, L|K) \to H^2(L|K)$ is surjective.*

(2) The homomorphism $\delta : \mathrm{Br}_{\mathrm{Az}}(L|K) \to H^2(L|K)$ is bijective. In particular, $\mathrm{Br}_{\mathrm{Az}}(K) \simeq H^2(K_s|K) = \mathrm{Br}(K)$.

Proof. A proof is in [43], page 158. □

2.1.2 Cyclic algebras

We construct explicitly a representative for each similarity class in $\mathrm{Br}(K)$. Let $L|K$ be a cyclic extension of fields of degree n with Galois group G. Let $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ be a group homomorphism. Note that χ is surjective if and only if χ is an isomorphism. This is also equivalent to choose a generator $\sigma \in G$ such that $\chi(\sigma) = 1 \in \mathbb{Z}/n\mathbb{Z}$. Take $a \in K^\times$, we construct a K-algebra (χ, a) as follows.

(1) As an additive abelian group, (χ, a) is an n-dimensional L-vector space with basis $1, e, \dots, e^{n-1}$. We put $(\chi, a) := L \oplus Le \oplus \cdots \oplus Le^{n-1}$.

(2) Let $\lambda, \mu \in L$ and $\sigma \in G$, we define

$$\lambda e^i \cdot \mu e^j = \begin{cases} \lambda\sigma(\mu)e^{i+j} & \text{if } i+j<n \\ a\lambda\sigma(\mu)e^{i+j-n} & \text{if } i+j \geq n \end{cases}$$

and extend L-bilinearly to (χ, a).

Thus we obtain an associated K-algebra which is called the **cyclic algebra** associated to the character χ and $a \in K^\times$. Since $\dim_L(\chi, a) = n$, $[L : K] = n$, we conclude $\dim_K(\chi, a) = n^2$.

Theorem 2.1.8. *Let $L|K$ be a cyclic extension of degree n. Take $a \in K^\times$ and let $\chi : G \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ be a surjective character. Then*

$$(\chi, a) \otimes_K L \simeq M_n(L).$$

Proof. Let σ be a generator of G such that $\chi(\sigma) = 1$. Suppose as an L-vector space, $(\chi, a) \simeq \bigoplus_{i=0}^{n-1} Le^i$. We define a homomorphism

$$\varphi : (\chi, a) \otimes_K L \to M_n(L)$$

of L-algebras by

$$\varphi(\lambda \otimes 1) = \sum_{i=1}^{n} \sigma(\lambda)^{i-1} E_{ii} \quad \text{and} \quad \varphi(e \otimes 1) = aE_{n1} + \sum_{i=2}^{n} E_{i,i-1},$$

for $\lambda \in L$ and e as above, where E_{ij} is the $n \times n$ matrix with the (i, j)-entry equals to 1 and others equal to 0. Then φ is a well-defined homomorphism of L-algebras. Since

$$\dim_L \big((\chi, a) \otimes_K L\big) = n^2 = \dim_L M_n(L),$$

it will be sufficient to show φ is surjective.

Suppose $L = K(\alpha)$ for some $\alpha \in L$. For $\lambda \in L$, we can find $g \in K[t]$ such that $\lambda = g(\alpha)$. Then by the lemma below, $\lambda \otimes 1$ is sent to $(\alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)) \in L^{\oplus n}$. Hence we have

$$\begin{aligned} \varphi(L \otimes_K L) &= \bigoplus_{i=1}^{n} LE_{ii} \\ \varphi(Le \otimes_K L) &= LE_{n1} \oplus \bigoplus_{i=2}^{n} LE_{i,i-1} \\ \varphi(Le^2 \otimes_K L) &= LE_{n-1,1} \oplus LE_{n,2} \oplus \bigoplus_{i=3}^{n} LE_{i,i-2}, \text{ etc.} \end{aligned}$$

It follows that $\mathrm{Im}\,\varphi = M_n(L)$. □

Lemma 2.1.9. *Let $L|K$ be a Galois extension of degree n with Galois group G. Then we have an isomorphism of L-algebras:*

$$L \otimes_K L \simeq \mathrm{Hom}_{\mathfrak{Set}}(G, L), \ a \otimes b \mapsto (\sigma \mapsto \sigma(a)b).$$

Proof. Write $G = \{\sigma_1, \ldots, \sigma_n\}$. Finite separable extensions are simple extensions, so $L = K(\alpha)$ for some $\alpha \in L$. Let $P(t) = \prod_{i=1}^n (t - \sigma_i(\alpha))$ be the minimal polynomial of α. We view $L \otimes_K L$ as an L-algebra via the second entry. Then

$$L \otimes_K L \simeq \big(K[t]/P(t)\big) \otimes_K L \simeq L[t]/P(t).$$

By Chinese remainder theorem, we conclude

$$L[t]/P(t) \simeq \prod_{i=1}^n L(t)/(t - \sigma_i\alpha) = \mathrm{Hom}_{\mathfrak{Set}}(G, L),$$

as required. □

Definition 2.1.2. Let A be a central simple algebra over K. $L|K$ is called a splitting field for A if

$$A \otimes_K L \simeq M_n(L)$$

for some positive integer n. In this case we say that L splits A.

Theorem 2.1.10. *Let $L|K$ be a cyclic extension of degree n with Galois group G.*

(1) By the identification $H^1(G, \mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$, we can view a surjective character $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ as an element of $H^1(G, \mathbb{Z}/n\mathbb{Z})$. From the exact sequence

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

of trivial G-modules, we obtain a connecting homomorphism

$$\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}).$$

Then for any $a \in K^\times$, we get

$$a \cup \delta(\chi) \in H^2(G, L^\times) = H^2(L|K)$$

equals to the class of the opposite of the cyclic algebra (χ, a).

(2) A central simple algebra A over K is similar to a cyclic algebra iff there exists a cyclic extension of K splitting A, i.e. $A \otimes_K L \simeq M_n(L)$ where $n = [L : K]$.

(3) In $\mathrm{Br}(K)$, we have

$$[(\chi, a_1)] + [(\chi, a_2)] = [(\chi, a_1 a_2)] \quad \textit{and} \quad [(\chi_1, a)] + [(\chi_2, a)] = [(\chi_1 + \chi_2, a)]$$

for any $a_1, a_2 \in K^\times$ and $\chi_1, \chi_2 \in H^1(G, \mathbb{Z}/n\mathbb{Z})$.

Proof. (1) This is done by explicit computation.

(2) Suppose a central simple algebra A over K is similar to a cyclic algebra (χ, a), where $\chi : \mathrm{Gal}(L|K) \to \mathbb{Z}/n\mathbb{Z}$ is a surjective character for some cyclic extension $L|K$ of degree n. Then $(\chi, a) \otimes_K L \simeq M_n(L)$ for some $n > 0$, and hence A is also splitting by the cyclic extension $L|K$. Conversely, suppose $L|K$ is a cyclic extension of degree n splitting A. Then $[A] \in \mathrm{Br}_{\mathrm{Az}}(L|K) \simeq H^2(L|K)$. Let $\chi \in \mathrm{Hom}(\mathrm{Gal}(L|K), \mathbb{Z}/n\mathbb{Z})$ be a surjective character. The we have an isomorphism of Tate cohomology groups

$$K^\times / N_{L|K}(L^\times) = \widehat{H}^0(\mathrm{Gal}(L|K), L^\times) \xrightarrow{-\cup\delta(\chi)} \widehat{H}^2(\mathrm{Gal}(L|K), L^\times) = H^2(L|K).$$

In particular, $[A] = \overline{a} \cup \delta(\chi)$ for some $a \in K^\times$. This shows that A is a cyclic algebra over K by (1).

(3) These formulas hold by the bilinearity of cup product. □

2.1.3 The local invariants

We say a field K is a local field, if K is endowed with a discrete valuation v such that K is complete with respect to v and the residue field κ is finite.

Theorem 2.1.11. *Let K be a local field.*
(1) If K is of characteristic 0, then K is a finite extension of $\mathbb{Q}_p$ for some prime number p.
(2) If K is of characteristic $p > 0$, then K is a finite extension of $\mathbb{F}_p((t))$ where $\mathbb{F}_p$ denotes the finite field with p elements.

Proof. See [39], page 135, proposition 5.2. □

Example 2.1.12. Let k be a number field with $\mathcal{O}_k$ the ring of algebraic integers and let $v \in \Omega$ be a finite place of k. Then k_v is a local field. Indeed, each finite place v is above some prime ideal $(p) \subset \mathbb{Z}$ and hence the residue field $\kappa(v)$ is a finite extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. This shows that in particular $\kappa(v)$ is finite.

Let K be a local field and we may assume the discrete valuation v is normalized which means that $v : K^\times \to \mathbb{Z}$ is surjective. We take $U_K = \{x \in K^\times \mid v(x) = 0\}$ to be the group of units in the valuation ring $\{x \in K^\times \mid v(x) \geq 0\}$ of v. Let K_s be the separable closure of K and let K_{nr} be the maximal unramified subextension of $K_s|K$. Recall that the residue field of K_{nr} is $\overline{\kappa}$, the algebraic closure of κ. Moreover, $\mathrm{Gal}(K_{nr}|K) = \mathrm{Gal}(\overline{\kappa}|\kappa)$ holds. Recall that

$$\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) \to \mathbb{Z}/n\mathbb{Z},\ F_n \mapsto \overline{1}$$

is an isomorphism for each positive integer n where F_n is the Frobenius element. Passing to the projective limit we obtain an isomorphism $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q) \simeq \widehat{\mathbb{Z}}$. In our case, the κ is a finite field and hence $\mathrm{Gal}(\overline{\kappa}|\kappa) \simeq \widehat{\mathbb{Z}}$. From now on, we may identify $\widehat{\mathbb{Z}}$ with $\mathrm{Gal}(K_{nr}|K)$ by $v \mapsto F^v$, here F is the Frobenius element in $\mathrm{Gal}(K_{nr}|K)$.

Lemma 2.1.13. *Let G be a finite group and let M be a G-module. Let*

$$M = M^0 \supseteq M^1 \supseteq \cdots \supseteq M^i \supseteq \dots$$

be a descending chain of G-submodules. Suppose the natural map $M \to \varprojlim M/M^i$ is a bijection. If there exists some q such that $H^q(G, M^i/M^{i+1}) = 0$ for all $i \geq 0$, then $H^q(G, M) = 0$.

Proof. Let f be any q-cocycle with values in M. We show that f is also a q-coboundary. $H^q(G, M/M^1) = 0$ implies there is a $(q-1)$-cochain ψ_1 with values in M such that $f = \delta\psi + f_1$ where f_1 is a q-cocyle with values in M^1. Similarly, there exists ψ_2 such that $f_1 = \delta\psi_2 + f_2$ with f_2 a q-cocycle with values in M^2. We construct in this way a sequence (ψ_n, f_n) where ψ_n is a $(q-1)$-cochain with values in M^{n-1}, f_n is a q-cocycle with values in M^n and $f_n = \delta\psi_{n+1} + f_{n+1}$. Set $\psi = \psi_1 + \psi_2 + \dots$ By assumption $M \simeq \varprojlim M/M^i$, hence the series converges and thus defines a $(q-1)$-cochain on G with values in M. Finally $f = \delta\psi_1 + f_1 = \delta(\psi_1 + \psi_2) + f_2 = \cdots = \delta\psi$. □

Proposition 2.1.14. *Let $L|K$ be an unramified extension of degree n with Galois group G. Then for all $q \in \mathbb{Z}$, we have*
(1) $H^q(G, U_L) = 0$,
(2) $v : H^q(G, L^\times) \to H^q(G, \mathbb{Z})$ is an isomorphism.

Proof. From the exact sequence $1 \to U_L \to L^\times \to \mathbb{Z} \to 0$ with trivial G-actions, we obtain a long exact sequence

$$\cdots \to H^q(G, U_L) \to H^q(G, L^\times) \to H^q(G, \mathbb{Z}) \to H^{q+1}(G, U_L) \to \dots$$

If $H^q(G, U_L) = 0$ for each q, then $H^q(G, L^\times) \to H^q(G, \mathbb{Z})$ is an isomorphism for each $q \in \mathbb{Z}$, hence it will be sufficient to show (1).

Let $\pi \in K$ be a uniformizor. Since $L|K$ is unramified, $U_L^{(i)} = 1 + \pi^i \mathcal{O}_L$ indeed forms a descending chain of open subsets of U_L. Then $U_L \simeq \varprojlim U_L/U_L^{(i)}$. To apply the previous lemma, we need the following two facts.

(A) We have isomorphisms $U_L/U_L^{(1)} \simeq \kappa_L^\times$ and $U_L^{(i)}/U_L^{(i+1)} \simeq (\kappa_L, +)$ that are compatible with the action of the Galois group.

Take $a \in U_L$, we put $U_L \to \kappa_L^\times$, $a \mapsto \overline{a}$. Since $U_L^{(1)} = 1 + \pi\mathcal{O}_L$, $\overline{a} = 1$ iff $a \in U_L^{(1)}$. Hence we have $U_L/U_L^{(1)} \simeq \kappa_L^\times$. For $a \in U_L^{(i)}$, then $a = 1 + \pi^i b$ for some $b \in \mathcal{O}_L$. We define $\varphi : U_L^{(i)}/U_L^{(i+1)} \to (k_L, +)$ by $a \mapsto \overline{b} \in k_L$. Clearly $\operatorname{Ker}\varphi \simeq U_L^{(i+1)}$, hence $U_L^{(i)}/U_L^{(i+1)} \simeq (\kappa_L, +)$ holds for $i \geq 1$.

(B) For all $q \in \mathbb{Z}$, we have

$$\begin{cases} H^q(G, U_L^{(i)}/U_L^{(i+1)}) = 0 & \text{if } i \geq 1 \\ H^q(G, U_L^{(i)}/U_L^{(i+1)}) = H^q(G, L^\times) & \text{if } i = 0 \end{cases}$$

$q = 1$, we apply Hilbert's theorem 90. $q = 2$, $|L^\times| < \infty$ and G is cyclic imply the Herbrand quotient $h(L^\times) = 1$ by (1.1.8). Hence $H^2(G, U_L^{(i)}/U_L^{(i+1)}) = 0$. For other q we use the periodicity.

Take $M = U_L$ and $M_i = U_L^{(i)}$ for $i \geq 1$. Then for any q and all $i \geq 0$, $H^q(G, M^i/M^{i+1}) = 0$ by (B). Hence $H^q(G, M) = 0$ by the previous lemma. □

Since $K_{nr}|K$ is unramified, the valuation $v : K^\times \twoheadrightarrow \mathbb{Z}$ extends uniquely to the valuation $v : K_{nr}^\times \twoheadrightarrow \mathbb{Z}$. This valuation map induces a homomorphism $H^2(K_{nr}|K) \to H^2(\operatorname{Gal}(K_{nr}|K), \mathbb{Z})$. This leads us to the following theorem.

Theorem 2.1.15. *The valuation map $v : K_{nr}^\times \twoheadrightarrow \mathbb{Z}$ defines an isomorphism*

$$H^2(K_{nr}|K) \to H^2(\widehat{\mathbb{Z}}, \mathbb{Z}).$$

Proof. We have seen $H^q(\operatorname{Gal}(K_{nr}|K), K_{nr}^\times) \to H^q(\operatorname{Gal}(K_{nr}|K), \mathbb{Z})$ is an isomorphism. Note that $\operatorname{Gal}(K_{nr}|K) \simeq \widehat{\mathbb{Z}}$, we conclude $H^2(K_{nr}|K) \to H^2(\widehat{\mathbb{Z}}, \mathbb{Z})$. □

Then we compute $H^2(\widehat{\mathbb{Z}}, \mathbb{Z})$. More generally, let G be a profinite group and consider the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ of G-modules with trivial actions. $\mathbb{Q}$ is an injective $\mathbb{Z}$-module, hence $\mathbb{Q}$ has trivial cohomology groups. Hence $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ is an isomorphism by the long exact sequence. Since $\mathbb{Q}/\mathbb{Z}$ is a trivial G-module, $H^1(G, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z})$. Summing up, we get $\delta : \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z}) \simeq H^2(G, \mathbb{Z})$.

In particular, we take $G = \widehat{\mathbb{Z}}$. Hence we get a chain of maps:

$$H^2(K_{nr}|K) \xrightarrow{v} H^2(\widehat{\mathbb{Z}}, \mathbb{Z}) \xrightarrow{\delta^{-1}} \operatorname{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z}$$

where v is induced from $v : K_{nr}^\times \to \mathbb{Z}$ and $\gamma : \varphi \mapsto \varphi(1)$. We take

$$\operatorname{inv}_K = \gamma \circ \delta^{-1} \circ v,$$

then we obtain an isomorphism, the so-called **local invariants**:

$$\operatorname{inv}_K : \operatorname{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

Proposition 2.1.16. *Let K be a local field, let $L|K$ be a finite separable extension of degree n and let L_{nr}, K_{nr} be the maximal unramified extensions of L, K respectively, so that $K_{nr} \subset L_{nr}$. Then the following diagram is commutative:*

$$\begin{tikzcd} H^2(K_{nr}|K) \arrow[r, "\operatorname{res}"] \arrow[d, "\operatorname{inv}_K"'] & H^2(L_{nr}|L) \arrow[d, "\operatorname{inv}_L"] \\ \mathbb{Q}/\mathbb{Z} \arrow[r, "n"'] & \mathbb{Q}/\mathbb{Z}. \end{tikzcd}$$

Proof. We write $\Gamma_K = \mathrm{Gal}(K_{nr}|K)$ for short and we denote by F_K the Frobenius element in the Galois group Γ_K. Γ_L and F_L are defined similarly. Then we have a homomorphism

$$\Gamma_L \to \Gamma_K,\ \sigma \mapsto j^{-1} \circ \sigma \circ j$$

where $j : K_{nr} \to L_{nr}$ is the inclusion, and $\sigma \circ j(K_{nr}) \subset j(K_{nr})$ holds implies that j^{-1} makes sense. This homomorphism between Galois groups induces the restriction homomorphism

$$\mathrm{res} : H^2(K_{nr}|K) \to H^2(L_{nr}|L).$$

Let κ_K and κ_L be the residue field of K and L respectively. Suppose $f = [\kappa_L : \kappa_K]$, then $F_L = (F_K)^f$. Let e be the ramification index of $L|K$. We consider the following diagram

$$\begin{tikzcd}
H^2(K_{nr}|K) \arrow[r, "v_K"] \arrow[d, "\mathrm{res}"'] & H^2(\Gamma_K, \mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "e\cdot\mathrm{res}"'] & \mathrm{Hom}(\Gamma_K, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\gamma_K"] \arrow[d, "e\cdot\mathrm{res}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "n"'] \\
H^2(L_{nr}|L) \arrow[r, "v_L"'] & H^2(\Gamma_L, \mathbb{Z}) \arrow[r, "\delta^{-1}"'] & \mathrm{Hom}(\Gamma_L, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\gamma_L"'] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Here $\gamma_K(\varphi) = \varphi(F_K)$ for $\varphi \in \mathrm{Hom}(\Gamma_K, \mathbb{Q}/\mathbb{Z})$ and $\gamma_L(\psi) = \psi(F_L)$ for $\psi \in \mathrm{Hom}(\Gamma_L, \mathbb{Q}/\mathbb{Z})$. The left square commutes since $v_L = e \cdot v_K$ on $K_{nr}^\times$. The middle square commutes is obvious. The right square commutes since $F_L = (F_K)^f$ and $n = ef$. This completes the proof. $\square$

2.2 Brauer groups of schemes

2.2.1 Brauer groups of local rings

Let R be a commutative local ring with maximal ideal $\mathfrak{m}$ and residue field $\kappa = R/\mathfrak{m}$. Let A be an R-algebra (not necessarily commutative) with 1_A. Suppose the homomorphism $R \to A$, $r \mapsto r \cdot 1_A$ identifies R with a subring of $Z(A)$, the center of A. We write A^{op} for the opposite algebra of A.

Definition 2.2.1. A is called an **Azumaya algebra** over R if
(1) A is an free R-module of finite rank,
(2) the map $A \otimes_R A^{\mathrm{op}} \to \mathrm{End}_R(A)$, $a \otimes a' \mapsto (x \mapsto axa')$ is an isomorphism.

Lemma 2.2.1. *Let M and N be finitely generated R-modules with N free. If $\varphi : M \to N$ is a homomorphism of R-modules such that $\overline{\varphi} : \overline{M} \to \overline{N}$ is injective, then φ has a section. If $\overline{\varphi}$ is an isomorphism, then so is φ. Here for any R-module M, we write $\overline{M}$ for $M \otimes_R (R/\mathfrak{m})$.*

Proof. See [37] lemma 1.11. $\square$

Proposition 2.2.2. *(1) If A is an Azumaya algebra over R and R' is a commutative local R-algebra ($R \to R'$ need not be a local homomorphism), then $A \otimes_R R'$ is an Azumaya algebra over R'.*

(2) If A is free of finite rank as an R-module, and $A \otimes_R (R/\mathfrak{m})$ is an Azumaya algebra over $R/\mathfrak{m}$, then A is an Azumaya algebra over R.

Proof. (1) A is a free R-module of finite rank implies that $A \otimes_R R'$ is a free R'-module of finite rank. By the isomorphisms

$$(A \otimes_R R') \otimes_{R'} (A \otimes_R R')^{\mathrm{op}} \simeq (A \otimes_R A^{\mathrm{op}}) \otimes_R R' \simeq \mathrm{End}_R(A) \otimes_R R' \simeq \mathrm{End}_{R'}(A \otimes_R R'),$$

we conclude that $A \otimes_R R'$ is an Azumaya algebra over R'.

(2) All we need to show is $A \otimes_R A^{\mathrm{op}} \simeq \mathrm{End}_R(A)$. Since $\overline{A} = A \otimes_R (R/\mathfrak{m})$ is an Azumaya algebra over $R/\mathfrak{m}$, we have an isomorphism $\overline{A} \otimes_{R/\mathfrak{m}} \overline{A}^{\mathrm{op}} \simeq \mathrm{End}_{R/\mathfrak{m}}(\overline{A})$ of $R/\mathfrak{m}$-algebras. This gives rise to $(A \otimes_R A^{\mathrm{op}}) \otimes_R (R/\mathfrak{m}) \simeq \mathrm{End}_R(A) \otimes_R (R/\mathfrak{m})$. A is a free R-module, hence the lemma applies. Consequently, $A \otimes_R A^{\mathrm{op}} \simeq \mathrm{End}_R(A)$ holds and therefore A is an Azumaya algebra over R. $\square$

Corollary 2.2.3. *(1) If A and A' are Azumaya algebras over R, then $A \otimes_R A'$ is an Azumaya algebra over R.*

(2) The matrix ring $M_n(R)$ is an Azumaya algebra over R.

Proof. (1) Now A and A' are free R-modules of finite rank, hence $A \otimes_R A'$ is also a free R-module of finite rank. By (2.2.2), $\overline{A}$ and $\overline{A'}$ are Azumaya algebra over $\kappa = R/\mathfrak{m}$, we have

$$(\overline{A} \otimes_\kappa \overline{A'}) \otimes_\kappa (\overline{A} \otimes_\kappa \overline{A'})^{\mathrm{op}} \simeq (\overline{A} \otimes_\kappa \overline{A}^{\mathrm{op}}) \otimes_\kappa (\overline{A'} \otimes_\kappa \overline{A'}^{\mathrm{op}}) \simeq \mathrm{End}_\kappa(\overline{A}) \otimes_\kappa \mathrm{End}_\kappa(\overline{A'}) \simeq \mathrm{End}_\kappa(\overline{A} \otimes_\kappa \overline{A'}).$$

It follows that $\overline{A} \otimes_\kappa \overline{A'}$ is an Azumaya algebra over $R/\mathfrak{m}$ and by (2.2.2) we conclude $A \otimes_R A'$ is an Azumaya algebra over R.

(2) $M_n(R)$ is a free R-algebra of finite rank and $M_n(R) \otimes_R (R/\mathfrak{m}) \simeq M_n(R/\mathfrak{m})$ is an Azumaya algebra over $R/\mathfrak{m}$. Thus by (2.2.2) we know that $M_n(R)$ is an Azumaya algebra over R. □

We say two Azumaya algebras A and A' over R are similar if

$$A \otimes_R M_n(R) \simeq A' \otimes_R M_{n'}(R)$$

holds for some n and n'. Similarity is obvious flexible and symmetric. It's easy to show it is transitive by the fact $M_n(R) \otimes_R M_{n'}(R) \simeq M_{nn'}(R)$. Hence similarity is an equivalence relation.

Definition 2.2.2. We define the **Brauer group** of R, denoted by $\mathrm{Br}_{\mathrm{Az}}(R)$, to be the group of similarity classes of Azumaya algebras over R.

Remark 2.2.4. Note that if A_1 is similar to A'_1 and A_2 to A'_2, then $A_1 \otimes_R A_2$ is similar to $A'_1 \otimes_R A'_2$ by the fact $M_n(R) \otimes_R M_{n'}(R) \simeq M_{nn'}(R)$. Hence $[A][A'] = [A \otimes_R A']$, $[A]^{-1} = [A^{\mathrm{op}}]$ and the neutral element $[R]$ make $\mathrm{Br}_{\mathrm{Az}}(R)$ into a group.

Let R be a local ring with residue field κ. Take $a \in R$ and $f \in R[T]$, then we write $\overline{a} \in \kappa$ and $\overline{f} \in \kappa[T]$ for their images under the canonical projection. We say R is **Henselian** if for each monic polynomial $f \in R[T]$ and each simple root a_0 of $\overline{f}$ in κ, there exists an $a \in R$ such that $f(a) = 0$ and $\overline{a} = a_0$. We say a Henselian local ring R is **strictly Henselian** if κ is separably algebraically closed. We collect some results about the Brauer group of a local ring in the following.

Proposition 2.2.5. *If R is a Henselian local ring with residue field κ, then the canonical map $\mathrm{Br}_{\mathrm{Az}}(R) \to \mathrm{Br}_{\mathrm{Az}}(\kappa)$ is injective. Moreover, if R is a strict Henselian local ring, then $\mathrm{Br}_{\mathrm{Az}}(R) = 0$.*

Proof. See [37], page 138-139. □

Proposition 2.2.6. *Let R be a Henselian local ring with residue field κ. Then the homomorphism*

$$H^q_{\text{ét}}(\mathrm{Spec}\, R, \mathbb{G}_m) \to H^q_{\text{ét}}(\mathrm{Spec}\, \kappa, \mathbb{G}_m)$$

is an isomorphism for each $q \geq 1$.

Proof. See [37], page 116, remark 3.11(a). □

2.2.2 Brauer groups of schemes

Let X be a scheme and let $\mathcal{O}_X$ be the structure sheaf on X.

Definition 2.2.3. An $\mathcal{O}_X$-module $\mathcal{A}$ is called an **Azumaya algebra** over X if

(1) $\mathcal{A}$ is a coherent $\mathcal{O}_X$-module,

(2) for all closed points $x \in X$, $\mathcal{A}_x$ is an Azumaya algebra over the local ring $\mathcal{O}_{X,x}$.

Note that the assumption (2) implies that $\mathcal{A}$ is locally free of finite rank as an $\mathcal{O}_X$-module. Moreover, for each point $x \in X$ (not necessarily closed), $\mathcal{A}_x$ is an Azumaya algebra over $\mathcal{O}_{X,x}$.

Proposition 2.2.7. *Let $\mathcal{A}$ be an $\mathcal{O}_X$-algebra of finite type. The following are equivalent:*

(1) $\mathcal{A}$ is an Azumaya algebra over X,

(2) $\mathcal{A}$ is locally free as an $\mathcal{O}_X$-module and $\mathcal{A}_x \otimes_{\mathcal{O}_{X,x}} k(x)$ is a central simple algebra over $k(x)$ for all $x \in X$,

(3) $\mathcal{A}$ is locally free as an $\mathcal{O}_X$-module and the canonical homomorphism $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{A}^{\mathrm{op}} \to \mathcal{E}nd_{\mathcal{O}_X}(\mathcal{A})$ is an isomorphism,

(4) there is a covering $\{U_i \to X\}$ for the étale topology on X such that for all i, there exists r_i such that $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \simeq M_{r_i}(\mathcal{O}_{U_i})$,

(5) there is a covering $\{U_i \to X\}$ for the flat topology on X such that for all i, there exists r_i such that $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \simeq M_{r_i}(\mathcal{O}_{U_i})$.

Proof. See [37], page 141, proposition 2.1. □

We say two Azumaya algebras $\mathcal{A}$ and $\mathcal{A}'$ over X are similar, if there exist two locally free $\mathcal{O}_X$-modules $\mathcal{E}$ and $\mathcal{E}'$ of finite rank on X, such that

$$\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{E}nd_{\mathcal{O}_X}(\mathcal{E}) \simeq \mathcal{A}' \otimes_{\mathcal{O}_X} \mathcal{E}nd_{\mathcal{O}_X}(\mathcal{E}').$$

The similarity relation is an equivalence relation, because

$$\mathcal{E}nd_{\mathcal{O}_X}(\mathcal{E}) \otimes_{\mathcal{O}_X} \mathcal{E}nd_{\mathcal{O}_X}(\mathcal{E}') \simeq \mathcal{E}nd_{\mathcal{O}_X}(\mathcal{E} \otimes_{\mathcal{O}_X} \mathcal{E}').$$

This leads us to the following:

Definition 2.2.4. We define the **Brauer group** of X, denoted by $\mathrm{Br}_{\mathrm{Az}}(X)$, to be the similarity classes of Azumaya algebras over X.

Remark 2.2.8. (1) $\mathrm{Br}_{\mathrm{Az}}(X)$ is indeed a group. We define an operation

$$\mathrm{Br}_{\mathrm{Az}}(X) \times \mathrm{Br}_{\mathrm{Az}}(X) \to \mathrm{Br}_{\mathrm{Az}}(X),\ [\mathcal{A}][\mathcal{A}'] = [\mathcal{A} \otimes \mathcal{A}'].$$

Of course $\mathcal{O}_X$ itself is an Azumaya algebra over X hence it defines a class $[\mathcal{O}_X]$ in $\mathrm{Br}_{\mathrm{Az}}(X)$. Then its easy to see $[\mathcal{A}][\mathcal{O}_X] = [\mathcal{A}]$ and $[\mathcal{A}][\mathcal{A}^{\mathrm{op}}] = [\mathcal{O}_X]$. We conclude $[\mathcal{O}_X]$ is the neutral element and $[\mathcal{A}]^{-1} = [\mathcal{A}^{\mathrm{op}}]$.

(2) $\mathrm{Br}_{\mathrm{Az}}(-) : \mathfrak{Sch} \to \mathfrak{Ab}$ is a contravariant functor. Suppose $f : X \to Y$ is a morphism of schemes, then we can define

$$f^* : \mathrm{Br}_{\mathrm{Az}}(Y) \to \mathrm{Br}_{\mathrm{Az}}(X),\ \mathcal{A} \mapsto f^*\mathcal{A}.$$

Here $f^*\mathcal{A}$ is the sheaf associated to the presheaf $f^{-1}\mathcal{A} \otimes_{f^{-1}\mathcal{O}_Y} \mathcal{O}_X$. Let $x \in X$ and $y = f(x)$, then $(f^*\mathcal{A})_x = \mathcal{A}_y \otimes_{\mathcal{O}_{Y,y}} \mathcal{O}_{X,x}$ is a free $\mathcal{O}_{X,x}$-algebra. $f_x^* : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ induces a homomorphism $\kappa(y) \hookrightarrow \kappa(x)$ and hence $(f^*\mathcal{A})_x \otimes_{\mathcal{O}_{X,x}} \kappa(x) \simeq \mathcal{A}_y \otimes_{\mathcal{O}_{Y,y}} \kappa(x)$ is a central simple algebra over $\kappa(x)$.

Definition 2.2.5. Let X be a scheme. We put

$$\mathbb{G}_m : X_{\text{ét}} \to \mathfrak{Ab},\ U \mapsto \Gamma(U, \mathcal{O}_U)^\times,$$

and then $\mathbb{G}_m$ is an abelian sheaf on $X_{\text{ét}}$. We define the **cohomological Brauer group** of X, denoted by $\mathrm{Br}(X)$, to be $H^2_{\text{ét}}(X, \mathbb{G}_m)$.

Theorem 2.2.9. *Let X be a scheme. There is a canonical injective homomorphism*

$$\mathrm{Br}_{\mathrm{Az}}(X) \to \mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m).$$

Proof. See [37], page 142, theorem 2.5. □

Corollary 2.2.10. *Let X be a regular integral scheme with function field $K(X)$. Then the canonical map $\mathrm{Br}_{\mathrm{Az}}(X) \to \mathrm{Br}(X) \hookrightarrow \mathrm{Br}(K(X))$ is injective.*

Proof. See [37], page 145, corollary 2.6. □

Finally, we give some special cases when the canonical homomorphism is surjective.

Proposition 2.2.11. *Suppose R is a Henselian local ring. Let $X = \operatorname{Spec} R$. Then $\mathrm{Br}_{\mathrm{Az}}(X) = \mathrm{Br}(X)$.*

Proof. See [37], page 148, corollary 2.12. □

Proposition 2.2.12. *Suppose X is a regular quasi-compact and separated scheme endowed with an ample invertible sheaf $\mathcal{L}$. Then $\mathrm{Br}_{\mathrm{Az}}(X) = \mathrm{Br}(X)$.*

Proof. This is an unpublished result of Gabber. One proof is contained in [15]. □

2.2.3 Residue homomorphisms

We begin with a few discussion on the vanishing of the Brauer groups of fields and then we construct the residue homomorphisms.

Vanishing of Brauer groups

Proposition 2.2.13. *For a given field K, the following are equivalent:*

(1) Let $L|K$ be any finite separable extension of fields. Then $\mathrm{Br}(L) = 0$.

(2) Let $L|K$ be a finite extension and let $M|L$ be a finite Galois extension. Then the $\mathrm{Gal}(M|L)$-module $M^\times$ is cohomologically trivial.

(3) Let $L|K$ be a finite extension and let $M|L$ be a finite Galois extension. Then the norm map $N_{M|L} : M^\times \to L^\times$ is surjective.

Proof. For a proof, see [43], chapter X, proposition 11. □

Let A be a complete discrete valuation ring with fraction field K and perfect residue field κ. Let $K_{nr}|K$ be the maximal unramified extension of K. Then (3) in the proposition holds by [43], chapter V, proposition 7, and hence K_{nr} has trivial Brauer group.

Remark 2.2.14. The fact $\mathrm{Br}(K_{nr}) = 0$ can also be deduced from a more difficult fact that K_{nr} is a C_1 field which is proved by Lang in [31].

In fact, it is convenient to use the theory of cohomological dimension for profinite groups to study fields with vanishing Brauer group. We briefly introduce some basic definitions and results as follows. For an abelian group A and for a prime number p, we write $A[p]$ for the p-primary torsion subgroup of A, that is the subgroup of elements of p-power order.

Definition 2.2.6. Let G be a profinite group and let p be a prime number.

(1) We say that G has **p-cohomological dimension** $\leq n$, if $H^q(G, A) = 0$ for each $q > n$ and for each continuous torsion G-module A.

(2) We define the **p-cohomological dimension of** G, denoted by $\mathrm{cd}_p(G)$, to be the smallest positive integer n for which G has cohomological dimension $\leq n$. If such n does not exist, we say $\mathrm{cd}_p(G) = \infty$.

By construction, $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ is a profinite group. We consider the p-cohomological dimension of $\widehat{\mathbb{Z}}$ as an example.

Proposition 2.2.15. *Let p be a prime number. Then we have $\mathrm{cd}_p(\widehat{\mathbb{Z}}) = 1$.*

Proof. See [19], page 136, proposition 6.1.3. □

Let K be a field and then the Galois group $\mathrm{Gal}(K_s|K)$ is a profinite group. This leads us to the following:

Definition 2.2.7. Let K be a field and let K_s be a separable closure of K.

(1) The **p-cohomological dimension** $\mathrm{cd}_p(K)$ of K is the p-cohomological dimension of the absolute Galois group $\mathrm{Gal}(K_s|K)$.

(2) The **cohomological dimension** $\mathrm{cd}(K)$ of K is the supremum of the $\mathrm{cd}_p(K)$ for all prime numbers p.

Now we can see that fields of p-cohomological dimension 1 can be characterized by the Brauer group. The following result can be compared with (2.2.13).

Theorem 2.2.16. *Let K be a field and let p be a prime number not equal to the characteristic of K. Then the following are equivalent:*

(1) The p-cohomological dimension of K is less or equal to 1, i.e. $\mathrm{cd}_p(K) \leq 1$.

(2) For each separable algebraic extension $L|K$, we have $\mathrm{Br}(L)[p] = 0$.

(3) The norm homomorphism $N_{M|L} : M^\times \to L^\times$ is surjective for each separable algebraic extension $L|K$ and each Galois extension $M|L$ with $\mathrm{Gal}(M|L) \simeq \mathbb{Z}/p\mathbb{Z}$.

Proof. See [19], page 138, theorem 6.1.8. □

We have the following complement:

Proposition 2.2.17. *Let K be a field of characteristic $p > 0$. Then $\mathrm{cd}_p(K) \leq 1$.*

Proof. See [19], page 139, proposition 6.1.9. □

Residue homomorphisms

Since $K_s|K$ is a Galois extension containing the Galois extension $K_{nr}|K$, we have an exact sequence

$$0 \to H^2(K_{nr}|K) \to H^2(K_s|K) \to H^2(K_s|K_{nr})$$

by (1.1.15). Note that $H^2(K_s|K_{nr}) = \mathrm{Br}(K_{nr}) = 0$, we conclude the map

$$H^2(\mathrm{Gal}(K_{nr}|K), K_{nr}^\times) \to H^2(\mathrm{Gal}(K_s|K), K_s^\times) = \mathrm{Br}(K)$$

induced by $\mathrm{Gal}(K_s|K) \to \mathrm{Gal}(K_{nr}|K)$ and $K_{nr}^\times \hookrightarrow K_s^\times$ is an isomorphism. Since $K_{nr}|K$ is unramified, the valuation v_A of K extends uniquely to K_{nr}. For each $\sigma \in \mathrm{Gal}(K_{nr}|K)$, we have

$$v_A(N_{K_{nr}|K}(\sigma.x)) = v_A(\sigma.N_{K_{nr}|K}(x)) = v_A(N_{K_{nr}|K}(x))$$

for each $x \in K_{nr}^\times$ since $N_{K_{nr}|K}(x) \in K^\times$. Therefore the valuation map $K_{nr}^\times \to \mathbb{Z}$ is Galois-equivariant hence it induces a map

$$H^2(\mathrm{Gal}(K_{nr}|K), K_{nr}^\times) \to H^2(\mathrm{Gal}(K_{nr}|K), \mathbb{Z}).$$

Note that $\mathrm{Gal}(K_{nr}|K) \simeq \mathrm{Gal}(\overline{\kappa}|\kappa)$, hence $H^2(\mathrm{Gal}(K_{nr}|K), \mathbb{Z}) \simeq H^2(\mathrm{Gal}(\overline{\kappa}|\kappa), \mathbb{Z})$. From the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, we obtain $H^2(\mathrm{Gal}(\overline{\kappa}|\kappa), \mathbb{Z}) \simeq H^1(\mathrm{Gal}(\overline{\kappa}|\kappa), \mathbb{Q}/\mathbb{Z})$. We therefore construct a homomorphism

$$\partial_A : \mathrm{Br}(K) \to H^1(\mathrm{Gal}(\overline{\kappa}|\kappa), \mathbb{Q}/\mathbb{Z})$$

by the composition

$$\mathrm{Br}(K) \xrightarrow{\sim} H^2(K_{nr}|K) \xrightarrow{v} H^2(\mathrm{Gal}(K_{nr}|K), \mathbb{Z}) \xrightarrow{\sim} H^2(\mathrm{Gal}(\overline{\kappa}|\kappa), \mathbb{Z}) \xrightarrow{\sim} H^1(\mathrm{Gal}(\overline{\kappa}|\kappa), \mathbb{Q}/\mathbb{Z}).$$

When A is not complete, we replace A by its completion which does not change the residue field κ, then apply the above construction.

Proposition 2.2.18. *Let X be a regular noetherian integral scheme of dimension 1. Let η be the generic point on X. Suppose for each $x \in X^{(1)}$, the residue field $\kappa(x)$ is perfect. Then we have an exact sequence*

$$0 \to H^2(X, \mathbb{G}_m) \to H^2(\operatorname{Spec} \kappa(\eta), \mathbb{G}_m) \to \bigoplus_{x \in X^{(1)}} H^1(\operatorname{Spec} \kappa(x), \mathbb{Q}/\mathbb{Z})$$

by [23], III, page 93, proposition 2.1.

Remark 2.2.19. Let A be a discrete valuation ring with fraction field K and residue field κ. Then there is an exact sequence

$$0 \to \mathrm{Br}(A) \to \mathrm{Br}(K) \to H^1(\kappa, \mathbb{Q}/\mathbb{Z}).$$

We can show that $\mathrm{Br}(A)$ can be identified with the kernel of the residue homomorphism $\partial_A : \mathrm{Br}(K) \to H^1(\kappa, \mathbb{Q}/\mathbb{Z})$ by [14], §1.1.

Proposition 2.2.20. *Let k be a field. Let $A \subset B$ be two discrete valuation rings containing k with fraction fields $K \subset L$ and perfect residue fields κ_A, κ_B. Let $e = e_{B|A}$ be the ramification index of B over A. Then the diagram commutes:*

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\partial_A"] \arrow[d, "\mathrm{res}"'] & H^1(\mathrm{Gal}(\overline{\kappa}_A|\kappa_A), \mathbb{Q}/\mathbb{Z}) \arrow[d, "e\cdot\mathrm{res}"] \\
\mathrm{Br}(L) \arrow[r, "\partial_B"'] & H^1(\mathrm{Gal}(\overline{\kappa}_B|\kappa_B), \mathbb{Q}/\mathbb{Z}).
\end{tikzcd}$$

Proof. We have seen in the proof of (2.1.16), the diagram

$$\begin{tikzcd}
H^2(K_{nr}|K) \arrow[r, "v_A"] \arrow[d, "\mathrm{res}"'] & H^2(\mathrm{Gal}(K_{nr}|K), \mathbb{Z}) \arrow[d, "e\cdot\mathrm{res}"] \\
H^2(L_{nr}|L) \arrow[r, "v_B"'] & H^2(\mathrm{Gal}(L_{nr}|L), \mathbb{Z})
\end{tikzcd}$$

is commutative. Hence the required square commutes by construction. □

Proposition 2.2.21. *Let A be a discrete valuation ring with fraction field K and perfect residue field κ. Let $L|K$ be a finite separable extension of fields. Let $B \subset L$ be the integral closure of A in L. B is a semi-local Dedekind ring. Let $\mathfrak{p}_i$, $i \in I$ be the non-zero prime ideals of B. Let $\kappa_i = B/\mathfrak{p}_i$ which we assume to be separable extensions of κ. The following diagram commutes:*

$$\begin{tikzcd}
\mathrm{Br}(L) \arrow[r, "\sum_i \partial_i"] \arrow[d, "\mathrm{cores}_{L|K}"'] & \bigoplus_{i \in I} H^1(\mathrm{Gal}(\overline{\kappa}_i|\kappa_i), \mathbb{Q}/\mathbb{Z}) \arrow[d, "\sum_i \mathrm{cores}_{\kappa_i|\kappa}"] \\
\mathrm{Br}(K) \arrow[r, "\partial_A"'] & H^1(\mathrm{Gal}(\overline{\kappa}|\kappa), \mathbb{Q}/\mathbb{Z}).
\end{tikzcd}$$

We briefly illustrate how these arrows go as follows. Since $L|K$ is a finite separable extension of fields, we obtain $L \subset K_s$ and hence we can identify $\mathrm{Br}(L)$ with $H^2(K_s|L)$. Moreover, $\mathrm{Gal}(K_s|L) \subset \mathrm{Gal}(K_s|K)$ is a subgroup of finite index $\mathrm{Card}(\mathrm{Gal}(L|K))$. Therefore we obtain a corestriction homomorphism

$$\mathrm{cores}_{L|K} : H^2(K_s|L) \to H^2(K_s|K).$$

Let v_i be the valuation of L associated to $\mathfrak{p}_i$ extending the valuation v_A and let $L_{i,nr}$ be the maximal unramified extension of L with respect to v_i contained in K_s. Therefore we obtain a residue homomorphism

$$\partial_i : \mathrm{Br}(L) \to H^1(\mathrm{Gal}(\overline{\kappa}_i|\kappa_i), \mathbb{Q}/\mathbb{Z})$$

for each i. Finally, $\kappa_i|\kappa$ is a finite separable extension, so $\overline{\kappa}$ is also an algebraic closure of κ_i. Moreover, $\mathrm{Gal}(\overline{\kappa}|\kappa_i)$ is a subgroup of $\mathrm{Gal}(\overline{\kappa}|\kappa)$ of finite index, and the corestriction homomorphism

$$\mathrm{cores}_{\kappa_i|\kappa} : H^1(\mathrm{Gal}(\overline{\kappa}|\kappa_i), \mathbb{Q}/\mathbb{Z}) \to H^1(\mathrm{Gal}(\overline{\kappa}|\kappa), \mathbb{Q}/\mathbb{Z})$$

is defined as usual.

Proposition 2.2.22. *Let A be a discrete valuation ring with perfect residue field κ. Let K be its fraction field and let $v_A : K^\times \to \mathbb{Z}$ be the associated valuation. Take $\xi \in H^1_{\text{ét}}(A, \mathbb{Q}/\mathbb{Z})$. Let $\overline{\xi}$ be the image of ξ under the reduction map*

$$H^1_{\text{ét}}(A, \mathbb{Q}/\mathbb{Z}) \to H^1_{\text{ét}}(\kappa, \mathbb{Q}/\mathbb{Z}),$$

and let ξ_K be the image of $H^1_{\text{ét}}(A, \mathbb{Q}/\mathbb{Z})$ in $H^1_{\text{ét}}(K, \mathbb{Q}/\mathbb{Z})$. For any $a \in K^\times$, we have

$$\partial_A((\xi_K, a)) = v_A(a) \cdot \overline{\xi} \in H^1(\kappa, \mathbb{Q}/\mathbb{Z}).$$

Proof. For a proof, see [8], proposition 1.3. $\square$

2.2.4 Unramified Brauer groups

There are two equivalent ways to define the unramified Brauer group of a variety X over a field k. We first briefly recall the birational invariance of the Brauer group $\mathrm{Br}(X)$. More detailed arguments are contained in [23], III, section 7.

Proposition 2.2.23. *Let $f : X \to Y$ be a birational morphism of integral smooth proper varieties over a field of characteristic zero. Then the induced map $\mathrm{Br}(Y) \to \mathrm{Br}(X)$ of the Brauer groups is an isomorphism.*

Let X be an integral smooth proper variety over a field k and let $k(X)$ be the function field of X. Let A be a discrete valuation ring of rank one such that $k \subset A$ and $k(X)$ is the fraction field of A, and let κ_A be the residue field. We have constructed the residue homomorphism $\partial_A : \mathrm{Br}(k(X)) \to H^1(\kappa_A, \mathbb{Q}/\mathbb{Z})$. Let $x \in X^{(1)}$ be a point of codimension 1, then the above construction applies to the local ring $\mathcal{O}_{X,x}$. Since X is regular, there is an injection $\mathrm{Br}(X) \to \mathrm{Br}(k(X))$. Similarly, for each $x \in X$, we have an injection $\mathrm{Br}(\mathcal{O}_{X,x}) \to \mathrm{Br}(k(X))$. We have the well-known

Theorem 2.2.24. *Let k be a field of characteristic zero and let X be an integral smooth proper variety over k. Let $k(X)$ be the function field of X. For an element $\alpha \in \mathrm{Br}(k(X))$, the following are equivalent:*

(1) α lies in $\mathrm{Br}(X)$.

(2) For any $x \in X$, α lies in $\mathrm{Br}(\mathcal{O}_{X,x})$.

(3) For any $x \in X^{(1)}$, α lies in $\mathrm{Br}(\mathcal{O}_{X,x})$; equivalently, the residue of α at x vanishes.

(4) For any discrete valuation ring $A \subset k(X)$ containing k and with fraction field $k(X)$, α lies in $\mathrm{Br}(A)$; equivalently, the residue $\partial_A(\alpha)$ vanishes.

If these conditions are fulfilled, and if Y is an integral smooth proper variety over k which is k-birationally equivalent to X, then

(5) α lies in $\mathrm{Br}(Y)$.

(6) For any $y \in Y$, α lies in $\mathrm{Br}(\mathcal{O}_{Y,y})$.

Proof. First of all, suppose all of (1) to (4) hold. Then (5) holds since $\mathrm{Br}(X)$ is isomorphic to $\mathrm{Br}(Y)$ and (6) holds by the equivalence of (1) and (2). Now we only need to prove the equivalence of (1) to (4).

(1)⇒(2). For any $x \in X$, we have a morphism $\mathrm{Spec}\,\mathcal{O}_{X,x} \to X$ and it induces $\mathrm{Br}(X) \to \mathrm{Br}(\mathcal{O}_{X,x})$. Both groups are contained in $\mathrm{Br}(k(X))$ and hence $\mathrm{Br}(X) \to \mathrm{Br}(\mathcal{O}_{X,x})$ is an injection.

(2)⇒(3). This is trivial.

(3)⇒(1). By assumption for each $x \in X^{(1)}$, $\alpha \in \mathrm{Br}(\mathcal{O}_{X,x})$ and it follows that

$$\alpha \in \mathrm{Ker}\left(\mathrm{Br}(k(X)) \to H^1(\kappa(x), \mathbb{Q}/\mathbb{Z})\right).$$

Recall that we have an exact sequence

$$0 \to \mathrm{Br}(X) \to \mathrm{Br}(k(X)) \to \bigoplus_{x \in X^{(1)}} H^1(\kappa(x), \mathbb{Q}/\mathbb{Z}),$$

we conclude α lies in the kernel of the third arrow, i.e. $\alpha \in \mathrm{Br}(X)$. □

Definition 2.2.8. The elements of $\mathrm{Br}(k(X))$ satisfying conditions (1) to (4) above form a group, denoted by $\mathrm{Br}_{nr}(k(X)|k)$ or $\mathrm{Br}_{nr}(X)$. We call it **the unramified Brauer group** of the field $k(X)$ over k.

Remark 2.2.25. Let k be a field of characteristic zero and let X be a smooth geometrically integral variety over k. We can embed X into a smooth and proper variety X_c by Hironaka's theorem on resolution of singularities. It is possible to identify $\mathrm{Br}_{nr}(X)$ with the Brauer group $\mathrm{Br}(X_c)$ of X_c. The unramified Brauer group $\mathrm{Br}_{nr}(X)$ also provides an easier way to compute $\mathrm{Br}(X_c)$ by residue homomorphisms.

2.3 Hasse principle, weak and strong approximation

In this section we introduce the Hasse principle, weak approximation and strong approximation for varieties over number fields. Let k be a number field and let Ω be the set of places of k. The main reference of this section is [47], §5.1.

2.3.1 Hasse principle, weak and strong approximation

Definition 2.3.1. A class of geometrically integral varieties over a number field k satisfies the **Hasse principle** if for every variety X in this class, the condition $X(k_v) \neq \emptyset$ for all places $v \in \Omega$ implies $X(k) \neq \emptyset$.

The Hasse principle is also called the **local-global principle**. We say a k-variety X is a counter-example to the Hasse principle if $X(k_v) \neq \emptyset$ for each place v, but $X(k) = \emptyset$.

Here is a list of some classical and more recent results on the Hasse principle. All cubics are assumed to be geometrically integral, non-conical (can not be reduced to a lesser number of variables by a linear transformation), and of codimension 1. For more detailed illustrations, see [47], page 99.

Theorem 2.3.1. *The following classes of geometrically integral varieties over a number field k satisfy the Hasse principle:*

(1) smooth projective quadrics (Minkowski and Hasse);

(2) Severi-Brauer varieties (Châtelet);

(3) smooth projective cubics in $\mathbb{P}^n_{\mathbb{Q}}$ for $n \geq 9$ (Hooley);

(4) principal homogeneous spaces under simply conncected, or adjoint semisimple groups (Kneser, Harder and Chernousov).

Next, we suppose $X(k_v) \neq \emptyset$ for each $v \in \Omega$. Then we have the diagonal embedding $X(k) \to X(k_\Omega)$. It is natural to ask the density of the image of $X(k)$ in $\prod_{v\in\Omega} X(k_v)$ with respect to the product topology.

Definition 2.3.2. Let X be a geometrically integral smooth variety over a number field k.

(1) We say X satisfies **weak approximation** if the image under the diagonal embedding of $X(k)$ is dense in $X(k_\Omega)$ with respect to the product topology.

(2) Let $S \subset \Omega$ be a subset. We say X satisfies **weak approximation away from** S if $X(k)$ is dense in $\prod_{v\in\Omega - S} X(k_v)$ with respect to the product topology.

The following proposition is useful when we study weak approximation because it allows us to approximate only finitely many places.

Proposition 2.3.2. *Let k be a number field and let X be a k-variety. Suppose $X(k_v) \neq \emptyset$ for each $v \in \Omega$. Then X satisfies weak approximation iff for any finite set $S \subset \Omega$, $X(k)$ is dense in $\prod_{v \in S} X(k_v)$.*

Proof. Suppose X satisfies weak approximation. Let $(P_v) \in \prod_{v \in S} X(k_v)$ be the point we need to approximate. Take any $(Q_v) \in \prod_{v \in \Omega} X(k_v)$ with $Q_v = P_v$ for $v \in S$, then we can find $Q \in X(k)$ arbitrarily close to (Q_v). In particular, Q is also arbitrarily close to P_v for $v \in S$. Conversely, let Z be the closure of $X(k)$ in $\prod_{v \in \Omega} X(k_v)$. By construction of the Tychonoff topology, an open base for topology is of the form

$$\Big\{ \prod_{v \in S} U_v \times \prod_{v \notin S} X(k_v) \mid \text{for any finite subset } S \subset \Omega \Big\}.$$

Here $U_v \subset X(k_v)$ is an open subset for each $v \in S$. Now let $S \subset \Omega$ be any finite subset. By assumption $X(k)$ is dense in $\prod_{v \in S} X(k_v)$, hence

$$Z \bigcap \big(\prod_{v \in S} U_v \times \prod_{v \notin S} X(k_v) \big) \neq \emptyset.$$

This implies that Z meets every non-empty open subsets of $\prod_{v \in \Omega} X(k_v)$ and hence $Z = \prod_{v \in \Omega} X(k_v)$, as required. □

Remark 2.3.3. (1) We should take care of the extreme case $\prod_{v \in \Omega} X(k_v) = \emptyset$. In this case, we say X satisfies weak approximation by convention.

(2) Suppose $\prod_{v \in \Omega} X(k_v) \neq \emptyset$. If X satisfies the weak approximation, then in particular $X(k)$ is non-empty and hence X satisfies the Hasse principle.

Definition 2.3.3. Let X be a geometrically integral smooth variety over a number field k.

(1) We say X satisfies **strong approximation** if $X(k)$ is dense in $X(\mathbb{A}_k)$ with respect to the adelic topology.

(2) We say X satisfies **strong approximation** away from S, if $X(k)$ is dense in $X(\mathbb{A}_k^S)$ with respect to the adelic topology.

Suppose X is a proper, smooth and geometrically integral variety over a number field k. Applying (1.5.18), we obtain $X(\mathbb{A}_k) = X(k_\Omega)$. Moreover, the adelic topology and the product topology are equivalent for proper varieties. Therefore weak approximation and strong approximation are equivalent in this case.

2.3.2 Birational invariance

Roughly speaking, the existence of k-points and satisfying weak approximation are stable under birational maps.

Lemma 2.3.4. *Let k be a number field and let k_v be its completion with respect to a place $v \in \Omega$. Let X be a smooth integral variety over k_v. Let $U \subset X$ be a non-empty Zariski open subset. Then the set $U(k_v)$ is dense in $X(k_v)$ with respect to the v-adic topology. In particular, if $X(k_v)$ is non-empty, then $U(k_v)$ is also non-empty.*

Proof. Suppose X is of dimension n. Let $P \in X(k_v)$ be the k_v-point we need to approximate. Since P is a smooth point on X, we can find a Zariski open neighbourhood V such that

$$V \simeq \operatorname{Spec} \frac{k_v[T_1, \dots, T_{n+m}]}{(F_1, \dots, F_m)} \quad \text{and} \quad \operatorname{rank} \big(\frac{\partial F_i}{\partial T_j}(P) \big) = m.$$

Note that the map

$$F : k_v^{n+m} \to k_v^m, \ (\boldsymbol{x}, \boldsymbol{y}) \mapsto (F_1(\boldsymbol{x}, \boldsymbol{y}), \dots, F_m(\boldsymbol{x}, \boldsymbol{y}))$$

satisfying
$$\det\big(\frac{\partial F_i}{\partial T_{n+j}}(P)\big) \neq 0,$$
hence by implicit function theorem we obtain a map
$$f : k_v^n \to k_v^m,\ \boldsymbol{x} \mapsto (f_1(\boldsymbol{x}), \ldots, f_m(\boldsymbol{x}))$$
such that $F(\boldsymbol{x}, f(\boldsymbol{x})) = 0$. Therefore there exists open subsets $\Omega_1 \subset V(k_v)$ and $\Omega_2 \subset k_v^n$ such that $P \in \Omega_1$ and the map $\theta : \Omega_1 \to \Omega_2$ induced by $\varphi : V \to \mathbb{A}^n_{k_v}$ is a homeomorphism. Moreover, the Zariski closure G of $\varphi(U^c \cap V)$ in $\mathbb{A}^n_k$ is of dimension strictly smaller than n. We can therefore take the points in $\Omega_2 - G$ arbitrarily close to $\varphi(P)$. Its inverse image by θ^{-1} is not in U^c and arbitrarily close to P. □

Proposition 2.3.5. *Let X, Y be two smooth geometrically integral and birationally equivalent varieties over a number field k. Then X satisfies weak approximation if and only if Y satisfies the weak approximation. In particular, k-rational geometrically integral smooth varieties over k satisfy weak approximation.*

Proof. It will be sufficient to prove the proposition in the case $Y = X - W$ where $W \subset X$ is a proper closed sub-variety of X, i.e. Y is a dense open set of X. Then if X satisfies weak approximation, then so does Y by definition of induced topology. Conversely, by the v-adic implicit function theorem, $Y(k_v)$ is dense in $X(k_v)$ by (2.3.4). Suppose Y satisfies weak approximation and let $(x_v) \in \prod_v X(k_v)$ be the given point we need to approximate. Choose $(y_v) \in \prod_v Y(k_v) \subset \prod_v X(k_v)$ arbitrarily close to (x_v) with respect to the product topology. By hypothesis, there is a rational point $y \in Y(k)$ whose image in $\prod_v Y(k_v)$ is arbitrarily close to (y_v). Hence y is also close to (x_v), i.e. X satisfies weak approximation. □

The Zariski density of rational points also follows from weak approximation.

Corollary 2.3.6. *Let k be a number field and let X be a smooth geometrically integral variety over k. Suppose $X(k) \neq \emptyset$ and X verifies weak approximation. Then $X(k)$ is Zariski dense in X.*

Proof. Let $P \in X$ be any point. We need to show for any non-empty open neighbourhood U of P, $U \cap X(k)$ is non-empty. Indeed, U is open dense in X and hence U satisfies weak approximation. In particular, $U(k) = U \cap X(k)$ is non-empty. □

Finally, we prove the existence of a k-point is stable under birational maps for proper varieties. This also shows that satisfying the Hasse principle is stable under birational maps for proper varieties.

Lemma 2.3.7 (Lang-Nishimura)**.** *Let k be a field and let $f : Y \to X$ be a rational map of schemes over k. Assume that Y has a smooth k-point and X is proper. Then $X(k) \neq \emptyset$.*

Proof. We do induction on $n = \dim Y$. $n = 0$ is clear. For $n > 0$, let y be a smooth k-point of Y. Consider the blow-up $\mathrm{Bl}_y Y$ of Y at y with exceptional divisor $E \simeq \mathbb{P}^{n-1}_k$ and the composition $\mathrm{Bl}_y Y \to Y \to X$. By the valuation criterion of properness, this composition is defined outside a set of codimension at least 2, so the restricting to E, we obtain a rational map $E \to X$. Now $X(k) \neq \emptyset$. □

2.4 The Brauer-Manin obstruction

Recall that for a number field k, the local invariant of the Brauer group of k_v is a homomorphism
$$\mathrm{inv}_v : \mathrm{Br}(k_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$
It is an isomorphism for each finite place v. If v is a real place, then inv_v identifies $\mathrm{Br}(\mathbb{R})$ with $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. If v is a complex place, then $\mathrm{Br}(\mathbb{C}) = 0$. We will frequently use the following short exact sequence.

Proposition 2.4.1 (Albert-Brauer-Hasse-Noether)**.** *Let k be a number field, then we have an exact sequence of abelian groups*

$$0 \to \operatorname{Br}(k) \to \bigoplus_{v\in\Omega} \operatorname{Br}(k_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Here the second arrow is the natural diagonal map and the third arrow is the sum of local invariants $\operatorname{inv}_v : \operatorname{Br}(k_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}$*.*

2.4.1 Brauer-Manin pairing

Lemma 2.4.2. *Let X be a variety over a number field k. Let $A \in \operatorname{Br}(X)$. For any finite subset $S \subset \Omega$, there exist a scheme $\mathcal{X}$ of finite type over $\mathcal{O}_{k,S}$, an element $\mathcal{A} \in \operatorname{Br}(\mathcal{X})$ and a morphism $X \hookrightarrow \mathcal{X}$ identifying X with the generic fibre of $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_{k,S}$ such that $\operatorname{Br}(\mathcal{X}) \to \operatorname{Br}(X)$ sends $\mathcal{A}$ to A.*

Proof. Now $\operatorname{Spec} \mathcal{O}_k$ is an integral scheme and the field k is its function field. X is a variety, hence $X \to \operatorname{Spec} k$ is of finite presentation. Applying (1.5.10) we obtain a dense open subscheme U of $\operatorname{Spec} \mathcal{O}_k$ and a scheme $\mathcal{X}$ of finite presentation over U such that $X \simeq \mathcal{X}_k$. We may shrinking U to an affine open subscheme $\operatorname{Spec} \mathcal{O}_{k,S_0}$ for some finite set $S_0 \subset \Omega$. Now we consider $\{\mathcal{X}_{\mathcal{O}_{k,T}}\}$ where T runs through all finite subsets of Ω containing S_0 and it forms a filtrated inverse system and $\varprojlim \mathcal{X}_{\mathcal{O}_{k,T}} \simeq X$. This implies $\operatorname{Br}(X) \simeq \varinjlim \operatorname{Br}(\mathcal{X}_{\mathcal{O}_{k,T}})$ (Cf. [40], proposition 6.6.10). Hence $A \in \operatorname{Br}(X)$ comes from an element of $\operatorname{Br}(\mathcal{X}_{\mathcal{O}_{k,S}})$ for some finite set $S \supseteq S_0$. The scheme $\mathcal{X}_{\mathcal{O}_{k,S}}$ is as required. ☐

Proposition 2.4.3 (Brauer-Manin pairing)**.** *Let X be a smooth and geometrically integral variety over a number field k. Then we have a well-defined pairing*

$$\operatorname{Br}(X) \times X(\mathbb{A}_k) \to \mathbb{Q}/\mathbb{Z},\ \ (A, (x_v)) \mapsto \sum_{v\in\Omega} \operatorname{inv}_v(A(x_v)).$$

Proof. (1) If x_v is a k_v-point of X, then apply $\operatorname{Br}(-)$ we obtain a map $\operatorname{Br}(x_v) : \operatorname{Br}(X) \to \operatorname{Br}(k_v)$ induced by x_v. We define $A(x_v)$ to be the image of A under this induced map. Hence $\operatorname{inv}_v(A(x_v))$ indeed lies in $\mathbb{Q}/\mathbb{Z}$.

(2) Then we claim the sum is finite. By (2.4.2), we can find a scheme $\mathcal{X}$ over $\mathcal{O}_{k,S}$ and a morphism $\operatorname{Br}(\mathcal{X}) \to \operatorname{Br}(X)$ sending $\mathcal{A}$ to A. We may assume $x_v \in \mathcal{X}(\mathcal{O}_v)$ for all $v \notin S$ by enlarging S. Note that (x_v) is an adelic point, so S is still a finite set. Then it follows $A(x_v) = \mathcal{A}(x_v) \in \operatorname{Br}(\mathcal{O}_v)$. Since the Brauer group of a valuation ring of a local field is trivial, it follows that $\operatorname{Br}(\mathcal{O}_v) = 0$ and $A(x_v) = 0$ for almost all v. ☐

Notation 2.4.1. Let $\Sigma \subset \operatorname{Br}(X)$ be a subset. Then we write

$$X(\mathbb{A}_k)^{\Sigma} = \{(x_v) \in X(\mathbb{A}_k) \mid \sum_{v\in\Omega} \operatorname{inv}_v(A(x_v)) = 0,\ \forall A \in \Sigma\}.$$

In particular, we obtain a subset $X(\mathbb{A}_k)^{\operatorname{Br}(X)}$ of $X(\mathbb{A}_k)$ and this is just the right kernel of the Brauer-Manin pairing.

Lemma 2.4.4. *Let X be a smooth and geometrically integral variety over a number field k. Recall that* $\operatorname{Br}_0(X) = \operatorname{Im}(\operatorname{Br}(k) \to \operatorname{Br}(X))$*. Then* $X(\mathbb{A}_k)^{\operatorname{Br}_0(X)} = X(\mathbb{A}_k)$ *and hence the pairing* $\operatorname{Br}(X) \times X(\mathbb{A}_k) \to \mathbb{Q}/\mathbb{Z}$ *can be considered as a pairing*

$$\big(\operatorname{Br}(X)/\operatorname{Br}_0(X)\big) \times X(\mathbb{A}_k) \to \mathbb{Q}/\mathbb{Z}.$$

Proof. Indeed, let $p : X \to \operatorname{Spec} k$ be the structral morphism and let $p^* : \operatorname{Br}(k) \to \operatorname{Br}(X)$ be the induced map. Let A be an element in $\operatorname{Br}_0(X)$, then $A = p^*(\alpha)$ for some $\alpha \in \operatorname{Br}(k)$. Take any $(x_v) \in X(\mathbb{A}_k)$ and we write $x_v^* : \mathrm{Br}(X) \to \mathrm{Br}(k_v)$ for the homomorphism induced by the k-morphism $x_v : \mathrm{Spec}\, k_v \to X$. By construction, we have

$$\sum_{v\in\Omega} \mathrm{inv}_v \big(p^*(\alpha)(x_v)\big) = \sum_{v\in\Omega} \mathrm{inv}_v \big((x_v^* \circ p^*)(\alpha)\big) = (\sum_{v\in\Omega} \mathrm{inv}_v) \circ \Delta(\alpha) = 0$$

by the reciprocity law (2.4.1), where Δ denotes the diagonal embedding $\mathrm{Br}(k) \to \bigoplus \mathrm{Br}(k_v)$. $\square$

Lemma 2.4.5. *Let us write $\Delta : X(k) \to X(\mathbb{A}_k)$ for the diagonal embedding. If $x \in X(k)$ is a k-point on X, then $\sum_{v\in\Omega} \mathrm{inv}_v \big(A(x)\big) = 0$ for each $A \in \mathrm{Br}(X)$. Here we view $x \in X(k)$ as an element in $X(k_v)$. In other words, we have $\Delta(X(k)) \subset X(\mathbb{A}_k)^{\mathrm{Br}(X)}$.*

Proof. Let $A \in \mathrm{Br}(X)$ and let $x \in X(k)$. We write $x^* : \mathrm{Br}(X) \to \mathrm{Br}(k)$ for the homomorphism induced by $x \in X(k)$. Then we define the evaluation map

$$ev_A : X(k) \to \mathrm{Br}(k),\ x \mapsto x^*(A).$$

Similarly we can defined the evaluation map

$$ev_A : X(\mathbb{A}_k) \to \bigoplus \mathrm{Br}(k_v),\ (x_v) \mapsto (x_v^*(A)).$$

Note that $x_v^*(A) \in \mathrm{Br}(\mathcal{O}_v) = 0$ for all but finitely many places v, hence the map $ev_A : X(\mathbb{A}_k) \to \bigoplus \mathrm{Br}(k_v)$ is well-defined. Now we obtain the following commutative diagram

$$\begin{tikzcd}
 & X(k) \arrow[r] \arrow[d] & X(\mathbb{A}_k) \arrow[d] & & \\
0 \arrow[r] & \mathrm{Br}(k) \arrow[r] & \bigoplus \mathrm{Br}(k_v) \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0,
\end{tikzcd}$$

with exact bottom row. The Brauer-Manin pairing is the map obtained via $X(\mathbb{A}_k)$ and it is 0 by commutativity and exactness of the bottom row. $\square$

Remark 2.4.6 (Functionality of the kernel)**.** Let k be a number field, let X and Y be two k-varieties and let $f : Y \to X$ be a k-morphism. We denote by $f^* : \mathrm{Br}(X) \to \mathrm{Br}(Y)$ the homomorphism induced by f. Take $(y_v) \in Y(\mathbb{A}_k)$ and $A \in \mathrm{Br}(X)$. Then

$$\sum_{v\in\Omega} \mathrm{inv}_v \big((f^*A)(y_v)\big) = \sum_{v\in\Omega} \mathrm{inv}_v \big((y_v^* \circ f^*)(A)\big) = \sum_{v\in\Omega} \mathrm{inv}_v \big(A(f \circ y_v)\big).$$

It follows that $(f \circ y_v) \in X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ as soon as $(y_v) \in Y(\mathbb{A}_k)^{\mathrm{Br}(Y)}$ and thus we have a well-defined map

$$f : Y(\mathbb{A}_k)^{\mathrm{Br}(Y)} \to X(\mathbb{A}_k)^{\mathrm{Br}(X)},\ (y_v) \mapsto (f \circ y_v).$$

In particular, $X(\mathbb{A}_k)^{\mathrm{Br}(X)} = \emptyset$ implies $Y(\mathbb{A}_k)^{\mathrm{Br}(Y)} = \emptyset$.

Lemma 2.4.7. *Let k be a number field and let X be a smooth and geometrically integral k-variety. Let $A \in \mathrm{Br}(X)$.*

(1) The map $ev_A : X(k_v) \to \mathrm{Br}(k_v)$, $x_v \mapsto A(x_v)$ is locally constant with respect to the v-adic topology for each place $v \in \Omega$.

(2) The map $X(\mathbb{A}_k) \to \mathbb{Q}/\mathbb{Z}$, $(x_v) \mapsto \sum_{v\in\Omega} \mathrm{inv}_v(A(x_v))$ is locally constant and $X(\mathbb{A}_k)^A$ is open and closed in $X(\mathbb{A}_k)$.

Proof. See [40], page 209, proposition 8.2.9. $\square$

Corollary 2.4.8. *Let k be a number field and let X be a smooth and geometrically integral k-variety. Then $X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ is a closed subset of $X(\mathbb{A}_k)$.*

Proof. By the previous lemma, it is clear that the complement of $X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ in $X(\mathbb{A}_k)$ is open. It follows that $X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ is a closed subset of $X(\mathbb{A}_k)$. $\square$

The product Brauer-Manin pairing

Proposition 2.4.9 (The product Brauer-Manin pairing)**.** *Let X be a smooth and geometrically integral variety over a number field k. We write $k_\Omega = \prod_{v\in\Omega} k_v$ as usual. Then we have a well-defined pairing*

$$\mathrm{Br}_{nr}(X) \times X(k_\Omega) \to \mathbb{Q}/\mathbb{Z},\ (A, (x_v)) \mapsto \sum_{v\in\Omega} \mathrm{inv}_v(A(x_v)).$$

Proof. By Hironaka's theorem (1.4.7), we can find a smooth proper variety X_c containing X as a dense open subset. The elements of $\mathrm{Br}_{nr}(X)$ uniquely extend to elements of $\mathrm{Br}(X_c)$. Note that $X(k_\Omega) \subset X_c(k_\Omega) = X_c(\mathbb{A}_k)$ and hence $\sum_{v\in\Omega} \mathrm{inv}_v(A(x_v))$ is a finite sum by the Brauer-Manin pairing. □

Notation 2.4.2. Let us put

$$X(k_\Omega)^{\mathrm{Br}_{nr}(X)} = \{(x_v) \in X(k_\Omega) \mid \sum_{v\in\Omega} \mathrm{inv}_v(A(x_v)) = 0,\ \forall A \in \mathrm{Br}_{nr}(X)\}$$

to be the right kernel of the product Brauer-Manin pairing.

Remark 2.4.10. We have seen $\mathrm{Br}(X_c) \subset \mathrm{Br}(X)$ and hence $\mathrm{Br}_{nr}(X) \subset \mathrm{Br}(X)$ by $\mathrm{Br}_{nr}(X) = \mathrm{Br}(X_c)$. We conclude that $X(\mathbb{A}_k)^{\mathrm{Br}(X)} \subset X(k_\Omega)^{\mathrm{Br}_{nr}(X)}$. For a fixed $A \in \mathrm{Br}_{nr}(X)$, the function $\sum_{v\in\Omega} \mathrm{inv}_v(A(x_v))$ is locally constant in the product topology. Thus $X(k_\Omega)^{\mathrm{Br}_{nr}(X)} \subset X(k_\Omega)$ is closed.

2.4.2 The Brauer-Manin obstruction

Now we can view $X(k)$ as a subset of $X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ via the diagonal embedding. Therefore $X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ potentially obstructs the existence of k-points on X.

Definition 2.4.3. Let X be a variety over a number field k.

(1) We say X has a **Brauer-Manin obstruction** to the Hasse principle if $X(\mathbb{A}_k)^{\mathrm{Br}(X)} = \emptyset$ and $X(\mathbb{A}_k) \neq \emptyset$.

(2) We say the Brauer-Manin obstruction is the **only obstruction** to the Hasse principle for X if $X(\mathbb{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$ implies $X(k) \neq \emptyset$.

(3) We say there is **no** Brauer-Manin obstruction to the Hasse principle if $X(\mathbb{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$.

Suppose $X(k_\Omega)^{\mathrm{Br}_{nr}(X)} \subsetneq X(k_\Omega)$. Then $X(k) \subset X(k_\Omega)^{\mathrm{Br}_{nr}(X)}$ and $X(k_\Omega)^{\mathrm{Br}_{nr}(X)} \subset X(k_\Omega)$ being closed imply $X(k)$ cannot be dense in $X(k_\Omega)$. This means $X(k_\Omega) \neq X(k_\Omega)^{\mathrm{Br}_{nr}(X)}$ is an obstruction to weak approximation for X.

Definition 2.4.4. Let X be a smooth and geometrically integral variety over a number field k.

(1) We say $X(k_\Omega) \neq X(k_\Omega)^{\mathrm{Br}_{nr}(X)}$ is the **Brauer-Manin obstruction to weak approximation** for X.

(2) We say the Brauer-Manin obstruction is the **only obstruction** to the weak approximation if $X(k)$ is dense in $X(k_\Omega)^{\mathrm{Br}_{nr}(X)}$, i.e. $\overline{X(k)} = X(k_\Omega)^{\mathrm{Br}_{nr}(X)}$.

(3) We say that there is **no** Brauer Manin obstruction to weak approximation if $X(k_\Omega) = X(k_\Omega)^{\mathrm{Br}_{nr}(X)}$.

In practice we will frequently in the situation that X is projective. In this case the Brauer-Manin obstruction has an easier expression.

Definition 2.4.5. Let X be a proper, smooth and geometrically integral variety over a number field k. Then $X(\mathbb{A}_k) = X(k_\Omega)$ and $\mathrm{Br}(X) = \mathrm{Br}_{nr}(X)$ are fulfilled.

(1) We say $X(\mathbb{A}_k) \neq X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ is the **Brauer-Manin obstruction to weak approximation** for X.

(2) We say the Brauer-Manin obstruction is the **only obstruction** to the weak approximation if $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}(X)}$.

2.4.3 Harari's formal lemma

We will use the following result in the sequel. More information is contained in [24].

Definition 2.4.6. Let X be an integral variety over a number field k and let $k(X)$ be its function field. Take $A_1, \dots, A_r \in \mathrm{Br}(k(X))$. Let $\langle A_1, \dots, A_r\rangle$ be the subgroup of $\mathrm{Br}(k(X))$ generated by these A_i and let $\Gamma = \mathrm{Br}(X) \cap \langle A_1, \dots, A_r\rangle$.

(1) We say there exists **Brauer-Manin obstruction to the Hasse principle associated to** Γ if for each adelic point $(P_v) \in X(\mathbb{A}_k)$ and an element $A \in \Gamma$ such that $\sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) \neq 0$ in $\mathbb{Q}/\mathbb{Z}$.

(2) We say there exists **Brauer-Manin obstruction to weak approximation associated to** Γ if there exists an adelic point $(P_v) \in X(\mathbb{A}_k)$ and an element $A \in \Gamma$ such that $\sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) \neq 0$ in $\mathbb{Q}/\mathbb{Z}$.

Theorem 2.4.11. *Let X be a smooth, projective and geometrically integral variety over k. Take $\alpha \in \mathrm{Br}(k(X))$ which is not in $\mathrm{Br}(X)$. Let $U \subset X$ be a non-empty Zariski open subset such that $\alpha \in \mathrm{Br}(U)$. Then there exist infinitely many places v of k such that $U(k_v) \to \mathrm{Br}(k_v)$ induced by α takes a non-zero value.*

Proof. See [24], Thm 2.1.1. □

Lemma 2.4.12 (Harari)**.** *Let k be a number field and let Ω be the set of all places of k. Let X be a smooth, projective and geometrically integral k-variety. Suppose $X(k_v) \neq \emptyset$ for all $v \in \Omega$. Let $A_1, \dots, A_r \in \mathrm{Br}(k(X))$ and let Γ be as above. Let U be a non-empty Zariski open subset of X such that $A_i \in \mathrm{Br}(U)$ for all i. Let $S \subset \Omega$ be a finite subset.*

(1) If there is no Brauer-Manin obstruction to the Hasse principle associated to Γ for X, then there exists a finite set $T \supset S$ and a family $(P_v) \in \prod_{v\in T} U(k_v)$ such that

$$\sum_{v\in T} \mathrm{inv}_v(A_i(P_v)) = 0, \quad i = 1, \dots, r.$$

(2) If there is no Brauer-Manin obstruction to weak approximation associated to Γ for X, then for all family $(P_v) \in \prod_{v\in S} U(k_v)$, there exists a finite set $T \supset S$ and a family $(P_v) \in \prod_{v\in T-S} U(k_v)$ such that

$$\sum_{v\in T} \mathrm{inv}_v(A_i(P_v)) = 0, \quad i = 1, \dots, r.$$

Proof. We write multiplicatively the group law of $\mathrm{Br}(k(X))$. Let n_i be the order of A_i in $\mathrm{Br}(k(X))$ for all i. Since the Brauer-Manin pairing $\mathrm{Br}(U) \times U(k_v) \to \mathbb{Q}/\mathbb{Z}$ is additive in the first variable, $\mathrm{inv}_v(A_i(P_v)) \in \mathbb{Z}/n_i\mathbb{Z}$ for all i and all $P_v \in U(k_v)$. For $v \in \Omega$, we write E_v for the subset

$$E_v = \big\{(\mathrm{inv}_v(A_i(P'_v)) \in \textstyle\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \mid P'_v \in U(k_v)\big\}$$

of $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$. Let Γ be the subgroup of $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ generated by

$$\big\{h = (h_i) \in \textstyle\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \mid h \in E_v \text{ for infinitely many } v \in \Omega\big\}.$$

By construction of Γ, there exists a finite set $S' \subset \Omega$ such that for all $v \notin S'$ and for all $P'_v \in U(k_v)$, we have $(\mathrm{inv}_v(A_i(P'_v)))_{1\le i\le r} \in \Gamma$. Take $(P_v) \in \prod_{v\in\Omega} U(k_v)$. Let $S \subset \Omega$ be a finite subset containing S' and take

$$W_S = \big(\sum_{v\in S} \mathrm{inv}_v(A_i(P_v))\big)_{1\le i\le r} \in \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}.$$

(1) If $W_S \in \Gamma$, we have $-W_S = W_1 + \cdots + W_n$ where $W_l \in E_v$, $1 \le l \le n$ for infinitely many v. Thus there exist pairwise distinct places $v_1, \dots, v_n$ not in S, such that $W_l \in E_{v_l}$ for $1 \le l \le n$. Write $S'' = \{v_1, \dots, v_n\}$, and take $T = S \cup S''$. Since $W_l \in E_{v_l}$, we can find $P_{v_l} \in U(k_{v_l})$

such that $(\mathrm{inv}_v(A_i(P_{v_l})))_{1\leq i\leq r} = W_l$ for $1 \leq l \leq n$. Then we have $\sum_{v\in T} \mathrm{inv}_v(A_i(P_v)) = 0$ by $W_S + \sum_{l=1}^{n} W_l = 0$.

(2) If $W_S \notin \Gamma$, there exists a character $\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ which vanishes on Γ, but does not vanish at W_S. Explicitly, there exist integers α_i for $1 \leq i \leq r$ such that for any element $(h_1, \ldots, h_r) \in \Gamma$, we have $\sum_{i=1}^{r} \alpha_i h_i = 0$ in $\mathbb{Q}/\mathbb{Z}$ while $\sum_{v\in S} \mathrm{inv}_v(\prod_{i=1}^{r} A_i^{\alpha_i}(P_v)) \neq 0$ in $\mathbb{Q}/\mathbb{Z}$. But for all $v \notin S'$ and $P'_v \in U(k_v)$, we have $(\mathrm{inv}_v(A_i(P'_v)))_{1\leq i\leq r} \in \Gamma$ which implies that $\mathrm{inv}_v(\prod_{i=1}^{r} A_i^{\alpha_i}(P'_v)) = 0$ in $\mathbb{Q}/\mathbb{Z}$. By (2.4.11), we conclude $A = \prod_{i=1}^{r} A_i^{\alpha_i} \in \mathrm{Br}(k(X))$ is in fact lies in $\mathrm{Br}(X)$ because $\mathrm{inv}_c(A(P'_v)) \neq 0$ holds potentially for $v \in S'$ which is finite. We have $\sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) = \sum_{v\in S'} \mathrm{inv}_v(A(P_v)) \neq 0$ in $\mathbb{Q}/\mathbb{Z}$ since $\sum_{v\in S} \mathrm{inv}_v(\prod_{i=1}^{r} A_i^{\alpha_i}(P_v)) \neq 0$.

Now, there's no Brauer-Manin obstruction to the Hasse principle associated to $(A_1, \ldots, A_r)$ for X, we can take $(P_v) \in \prod_{v\in\Omega} U(k_v)$ such that for all $B \in \mathrm{Br}(X)$, $\sum_{v\in\Omega} \mathrm{inv}_v(B(P_v)) = 0$ holds. Hence the case (2) above can not happen and the assertion follows from the case (1). Similarly, there's no Brauer-Manin obstruction to weak approximation, it is known for every element $(P_v) \in \prod_{v\in\Omega} U(k_v)$, we are in the above case. □

Chapter 3

Torsors and descent obstruction

3.1 Definition of torsors

3.1.1 Group schemes

Let X be a base scheme. Before the main topic of this section, we briefly recall the notion of X-group scheme and the action of an X-group scheme on an X-scheme.

Definition 3.1.1. Let X be a scheme and let G be an X-scheme. We say G is an X-**group scheme** if there exists morphisms

$$\mu : G \times_X G \to G, \quad e : X \to G \ \text{ and } \ \mathrm{inv} : G \to G,$$

such that μ, e and inv satisfy the group axioms for group operation, neutral element and inverse element respectively. More precisely, these can be visualized as the following commutative diagrams.

(1) Associativity:

$$\begin{tikzcd}
G \times_X G \times_X G \arrow[r, "\mu\times\mathrm{id}"] \arrow[d, "\mathrm{id}\times\mu"'] & G \times_X G \arrow[d, "\mu"] \\
G \times_X G \arrow[r, "\mu"'] & G.
\end{tikzcd}$$

(2) Left neutral element and right neutral element:

$$\begin{tikzcd}
X \times_X G \arrow[r, "e\times\mathrm{id}"] \arrow[dr] & G \times_X G \arrow[d, "\mu"] & G \times_X X \arrow[l, "\mathrm{id}\times e"'] \arrow[dl] \\
& G. &
\end{tikzcd}$$

(3) Inverse:

$$\begin{tikzcd}
G \arrow[r, "\mathrm{inv}\times\mathrm{id}"] \arrow[d] & G \times_X G \arrow[d, "\mu"'] & G \arrow[l, "\mathrm{id}\times\mathrm{inv}"'] \arrow[d] \\
X \arrow[r, "e"'] & G & X \arrow[l, "e"]
\end{tikzcd}$$

Definition 3.1.2. Let X be a scheme, let G be an X-group scheme and let Y be an X-scheme. A right G-action on Y is given by a morphism $\rho : Y \times_X G \to Y$ such that the composition

$$Y \simeq Y \times_X X \xrightarrow{\mathrm{id}\times e} Y \times_X G \xrightarrow{\rho} Y$$

is the identity on Y, and such that the diagram

$$\begin{tikzcd}
Y \times_X G \times_X G \arrow[r, "\rho\times\mathrm{id}"] \arrow[d, "\mathrm{id}\times\mu"'] & Y \times_X G \arrow[d, "\rho"] \\
Y \times_X G \arrow[r, "\rho"'] & Y
\end{tikzcd}$$

is commutative.

Remark 3.1.1. Let T be an X-scheme. Then the action $\rho : Y \times_X G \to Y$ induces a map

$$\rho_T : Y(T) \times_{X(T)} G(T) \to Y(T).$$

The first request says $\rho_T(y, \mathrm{id}) = y$ for each $y \in Y(T)$ where $\mathrm{id} \in G(T)$ is the neutral element. And the second request says $\rho_T(y, gh) = \rho_T(\rho_T(y, h), g)$ for any $g, h \in G(T)$. Hence we obtain the action by the group $G(T)$ on the set $Y(T)$ in the usual sense. We will denote this action by $(y, g) \mapsto y.g$.

3.1.2 Torsors over schemes

Definition 3.1.3. Let X be a scheme and let G be an fppf X-group scheme. Let $f : Y \to X$ be an X-scheme endowed with a G-action $\rho : Y \times_X G \to Y$ such that the diagram

$$\begin{tikzcd}
Y \times_X G \arrow[r, "\rho"] \arrow[d, "f\times\mathrm{id}_G"'] & Y \arrow[d, "f"] \\
X \times_X G \arrow[r, "pr_1"'] & X
\end{tikzcd}$$

commutes. We say Y is an X-**torsor** under G (or a G-**torsor** over X) if $f : Y \to X$ satisfies the following equivalent properties:

(1) the morphism $p : Y \to X$ is fppf, and the morphism $Y \times_X G \to Y \times_X Y$ induced by

$$\begin{tikzcd}
Y \times_X G \arrow[dr, dashed] \arrow[drr, bend left, "\rho"] \arrow[ddr, bend right, "pr_1"'] & & \\
& Y \times_X Y \arrow[r] \arrow[d] & Y \arrow[d] \\
& Y \arrow[r] & X
\end{tikzcd}$$

is an isomorphism;

(2) there exists a covering $\{U_i \to X\}_{i\in I}$ in the flat topology such that for each $i \in I$, $Y_{U_i} = Y \times_X U_i$ with the action of $G_{U_i} = G \times_X U_i$ is isomorphic to G_{U_i} with the right action of G_{U_i} on itself.

Remark 3.1.2. If we apply the functor of points, the morphism obtained in (1) can be described as follows. Let T an X-scheme, then we obtain a bijection of sets

$$Y(T) \times_{X(T)} G(T) \to Y(T) \times_{X(T)} Y(T),\ (y, g) \mapsto (y, \rho(y, g))$$

for $y \in Y(T)$ and $g \in G(T)$. In particular, for any $y, z \in Y(T)$, there exists unique $g \in G(T)$ such that $\rho(y, g) = z$, i.e. the $G(T)$-action on $Y(T)$ is simply transitive. In the sequel, we will simply denote this morphism by $(y, g) \mapsto (y, y.g)$.

Remark 3.1.3. We briefly sketch the equivalence of (1) and (2). (1) implies (2) since $Y \to X$ is a covering in the flat topology. Conversely, let $U = \bigsqcup U_i$ be the disjoint union of all the U_i. Then $U \to X$ is faithfully flat and locally of finite type. By assumption, we have $Y_{U_i} \simeq G_{U_i}$ and it follows that $Y_U \simeq G_U$. Hence $Y_U \to U$ verifies the property of (1). $Y \to X$ verifies (1) follows from descent with respect to morphisms which are faithfully flat and locally of finite type.

Let G be an fppf X-scheme. Then in particular, $G \to X$ is an X-torsor under G. By the compatibility assumption of an X-torsor, the right G-action on X is trivial. For this reason, the torsor $G \to X$ with the right G-action is called the **trivial** torsor.

Definition 3.1.4. Let Y_1 and Y_2 be two X-torsors under G. A morphism $\varphi : Y_1 \to Y_2$ of X-torsors under G is a morphism $\varphi : Y_1 \to Y_2$ of X-schemes such that the diagram

$$\begin{tikzcd}
Y_1 \times_X G \arrow[r, "\varphi\times\mathrm{id}"] \arrow[d, "\rho_1"'] & Y_2 \times_X G \arrow[d, "\rho_2"] \\
Y_1 \arrow[r, "\varphi"'] & Y_2
\end{tikzcd}$$

commutes. Here ρ_i denotes the G-action on Y_i for $i = 1, 2$. If we apply the functor of points, the compatibility of G-actions can be read as $\rho_2(\varphi(y_1), g) = \varphi(\rho_1(y_1, g))$.

Lemma 3.1.4. *Let G be an fppf group scheme over X. An X-torsor $Y \to X$ under G is trivial iff the structural morphism $f : Y \to X$ has a section $s : X \to Y$.*

Proof. Let $Y \to X$ be a trivial X-torsor under G. Note that $Y \to X$ is fppf and hence $Y \to X$ is surjective. Then each fibre Y_x over $x \in X$ is non-empty and is isomorphic to the group G_x, where G_x stands for the fibre of $G \to X$ at x. Now we obtain a section $s : X \to Y$, $x \to 1_{Y_x}$ where 1_{Y_x} is the unique element corresponding to the neutral element of G_x.

Conversely, let $s : X \to Y$ be a section of $f : Y \to X$ and let $\rho : Y \times_X G \to Y$ be the right G-action on Y. Since $Y \to X$ is an X-torsor under G, the morphism $\pi : Y \times_X G \to Y \times_X Y$ induced by p_1 and ρ is an isomorphism. Then we obtain an isomorphism

$$G \simeq X \times_Y Y \times_X G \xrightarrow{\mathrm{id}_X \times \pi} X \times_Y Y \times_X Y \simeq Y$$

where the existence of $X \times_Y Y \times_X G$ and $X \times_Y Y \times_X Y$ are given by the base change of $Y \times_X G \to Y$ and $Y \times_X Y \to Y$ to the morphism $s : X \to Y$. □

Proposition 3.1.5. *The category of X-torsors under G is a groupoid. More precisely, any morphism $Y_1 \to Y_2$ compatible with canonical projections to X and the action of G is an isomorphism.*

Proof. Let $f : Y_1 \to Y_2$ be a morphism of X-torsors under G. By definition, there are coverings $\{U_{ij} \to X\}_{i\in I_j, j=1,2}$ of X in the flat topology over X such that $Y_j \times_X U_{ij} \simeq G \times_X U_{ij}$. We can therefore take a common refinement $\{V_j \to X\}_{j\in J}$ of $\{U_{i1} \to X\}_{i\in I_1}$ and $\{U_{i2} \to X\}_{i\in I_2}$, such that $Y_i \times_X V_j \simeq G \times_X V_j$ for $i = 1, 2$ and for each $j \in J$. We take $V = \bigsqcup_J V_j$ and we obtain an fppf morphism $V \to X$. Then $Y_i \times_X V$ is a trivial V-torsor under G_V for $i = 1, 2$ and it follows that $Y_1 \times_X V \simeq Y_2 \times_X V$. By descent theory by fppf morphisms, $Y_1 \to Y_2$ is also an isomorphism. □

3.2 Torsors over fields

Let k be a field and let k_s be an algebraic closure of k. Let Σ be a set endowed with an action of the Galois group $\mathrm{Gal}(k_s|k)$. Then we denote by $(g, \sigma) \mapsto {}^g\sigma$ for the action of $g \in \mathrm{Gal}(k_s|k)$ on $\sigma \in \Sigma$. Let G be an algebraic group defined over k. The left action of G on itself is denoted by $(s, x) \mapsto s.x$, and the right action is denote by $(s, x) \mapsto x.s$. For an arbitrary scheme X over

k, we write $\overline{X}$ for $X \times_k k_s$. We have an action of $\mathrm{Gal}(k_s|k)$ on $\overline{X}$ which can be visualized as follows

$$\begin{tikzcd} X \times_k k_s \arrow[r, "\mathrm{id}_X \times g^*"] \arrow[d, equal] & X \times_k k_s \arrow[d, equal] \\ \overline{X} & \overline{X}, \end{tikzcd}$$

where $g^* : \operatorname{Spec} k_s \to \operatorname{Spec} k_s$ is the morphism induced by $g \in \mathrm{Gal}(k_s|k)$. The G-actions on G are compatible with the action of $\mathrm{Gal}(k_s|k)$: for $s_1, s_2 \in G(k_s)$, $g \in \mathrm{Gal}(k_s|k)$, we have

$$^g(s_1 s_2) = {}^g s_1 \cdot {}^g s_2.$$

Let X be a variety over a field k. Then X is of finite type over k implies that X is noetherian. The structure sheaf $\mathcal{O}_X$ is a free coherent $\mathcal{O}_X$-module. These two facts show that $\mathcal{O}_X$ is flat over X and consequently X is fppf over k. In particular, algebraic groups over k are also fppf over k. Hence we can obtain $\operatorname{Spec} k$-torsors under G from the previous section and we will say k-torsors to simplify the notation.

Definition 3.2.1. Let X be a variety over k and let G be an algebraic group over k.

(1) A k-**torsor** under G is a non-empty k-variety X equipped with a right action $X \times_k G \to X$ of G, denoted by $(x, g) \mapsto x.g$, such that the morphism

$$X \times_k G \to X \times_k X, \ (x, g) \mapsto (x, x.g)$$

is a k-isomorphism. A left k-**torsor** under G is a non-empty k-variety X equipped with a left action of G such that the morphism $G \times_k X \to X \times_k X$ is a k-isomorphism. Unless otherwise stated, a torsor will always mean a right torsor.

(2) A morphism $\varphi : X_1 \to X_2$ of k-torsors under G is a morphism of k-varieties such that the diagram

$$\begin{tikzcd} X_1 \times_k G \arrow[r, "\varphi \times \mathrm{id}"] \arrow[d, "\rho_1"'] & X_2 \times_k G \arrow[d, "\rho_2"] \\ X_1 \arrow[r, "\varphi"'] & X_2 \end{tikzcd}$$

commutes, where $\rho_i : X_i \times_k G \to X_i$ is the action of G for $i = 1, 2$. An isomorphism of k-torsors under G is an isomorphism of k-varieties compatible with the G-actions.

Remark 3.2.1. Let X be a k-torsor under G. Then we obtain a bijective map

$$X(k_s) \times G(k_s) \to X(k_s) \times X(k_s), \ (x, g) \mapsto (x, x.g).$$

This tells us that the right $G(k_s)$-action on $X(k_s)$ is simply transitive. More precisely, for any $x_1, x_2 \in X(k_s)$, there exists a unique $g \in G(k_s)$ such that $x_2 = x_1.g$.

Theorem 3.2.2. *Let k be a field. Then k-torsors are quasi-projective. More generally, this also holds with* $\operatorname{Spec} k$ *replaced by the spectrum of a Dedekind domain.*

Proof. See theorem 6.4.1 in [2]. □

3.2.1 Twisting by Galois descent

Let F be a **quasi-projective** k-variety endowed with an action of G. Suppose $\mathrm{Gal}(k_s|k)$ is endowed with its natural profinite topology and $G(k_s)$ is endowed with discrete topology. Let $\sigma : \mathrm{Gal}(k_s|k) \to G(k_s)$ be a continuous 1-cocycle with respect to the group cohomology. Then we have $\sigma(g_1 g_2) = \sigma(g_1) \cdot ({}^{g_1}\sigma(g_2))$ by the standard resolution. We define the **twisted action** of $\mathrm{Gal}(k_s|k)$ on $\overline{F}$ by

$$\rho : \mathrm{Gal}(k_s|k) \times \overline{F} \to \overline{F}, \quad (g, s) \mapsto \sigma(g).{}^g s,$$

where $g \in \mathrm{Gal}(k_s|k)$ and $s \in \overline{F}$. Take $g_1, g_2 \in \mathrm{Gal}(k_s|k)$, then we have

$$\begin{aligned}\rho(g_1g_2, s) &= \sigma(g_1g_2).^{g_1g_2}s = \big(\sigma(g_1)\cdot {}^{g_1}\sigma(g_2)\big).^{g_1g_2}s \\ &= \sigma(g_1).^{g_1}\rho(g_2, s) = \rho(g_1, \rho(g_2, s)),\end{aligned}$$

hence $\rho : (g, s) \mapsto \sigma(g).^{g}s$ is a well-defined $\mathrm{Gal}(k_s|k)$-action on $\overline{F}$.

Definition 3.2.2. Let F be a quasi-projective k-variety endowed with a G-action. Let σ : $\mathrm{Gal}(k_s|k) \to G(k_s)$ be a continuous 1-cocycle. By Weil's theorem on descent of the base field, the quotient of $\overline{F}$ by the twisted action of $\mathrm{Gal}(k_s|k)$ exists (a proof is contained in chapter 6 of [2]). We call the quotient the **twist** of F by σ, and we denote it by F^σ.

Remark 3.2.3. Replacing σ by a cohomologous cocycle $g \mapsto \big(c^{-1}\cdot\sigma(g)\cdot {}^{g}c\big)$ for $c \in G(k_s)$ gives rise to an isomorphic variety. The isomorphism depends on the choice of $c \in G(k_s)$ and hence the isomorphism is not canonical.

3.2.2 Classification of k-torsors

Let $\varphi : G \to G$ be an automorphism of G such that $\varphi(x.s) = \varphi(x).s$ for any $x, s \in G$. Then we claim φ can be identified with L_g the multiplication of some element $g \in G$ on the left. Indeed, we can take $g = \varphi(1_G)$, then $\varphi(x) = \varphi(1_G.x) = \varphi(1_G).x = L_g(x)$. Thus the group G acting on itself on the left is the automorphism group of the pair (G, the right action of G on G). Let $\sigma : \mathrm{Gal}(k_s|k) \to G(k_s)$ be a continuous 1-cocycle. Thus the corresponding twisted variety of G by σ is equipped with the right action of G making it into a right torsor under G. We shall denote this torsor by G^σ.

Conversely, any k-torsor X under G can be obtained in this way: choose a k_s-point $\overline{x}_0 \in X(k_s)$, then for any $g \in \mathrm{Gal}(k_s|k)$ there is a unique element $\sigma(g) \in G(k_s)$ such that ${}^{g}\overline{x}_0 = \overline{x}_0.\sigma(g)$ by the simple transitivity. Then we obtain a continuous map $\sigma : \mathrm{Gal}(k_s|k) \to G(k_s)$, $g \mapsto \sigma(g)$. Note that

$$\overline{x}_0\sigma(g_1g_2) = {}^{g_1g_2}\overline{x}_0 = {}^{g_1}(\overline{x}_0\sigma(g_2)) \overset{*}{=} {}^{g_1}\overline{x}_0{}^{g_1}\sigma(g_2) = \overline{x}_0\sigma(g_1)\cdot {}^{g_1}\sigma(g_2),$$

where $*$ holds by the compatibility of the $G(k_s)$-action and the $\mathrm{Gal}(k_s|k)$-action on $X(k_s)$. We therefore obtain $\sigma(g_1g_2) = \sigma(g_1)\cdot {}^{g_1}\sigma(g_2)$, i.e. σ is a continuous 1-cocycle. Let $\overline{x}_i \in X(k_s)$ and $\sigma_i(g)$ be the unique element in $G(k_s)$ such that ${}^{g}\overline{x}_i = \overline{x}_i\sigma_i(g)$ for $i = 1, 2$. Suppose $\overline{x}_2 = {}^{h}\overline{x}_1$ for some $h \in \mathrm{Gal}(k_s|k)$. Then we conclude

$$\overline{x}_1\sigma_1(gh) = {}^{gh}\overline{x}_1 = {}^{g}\overline{x}_2 = \overline{x}_2\sigma_2(g) = \overline{x}_1\sigma_1(h)\sigma_2(g),$$

and it follows that $\sigma_1(gh) = \sigma_1(h)\sigma_2(g)$. More explicitly, we have

$$\sigma_2(g) = (\sigma_1(h))^{-1}\cdot\sigma_1(g)\cdot {}^{g}\sigma_1(h).$$

Therefore two k_s-points $\overline{x}_1$ and $\overline{x}_2$ lead to cohomologous cocycles.

Summing up, cohomologous 1-cocycles give rise to isomorphic k-torsors and conversely isomorphic k-torsors determine cohomologous 1-cocycles. These two constructions are being inverse to each other ($\overline{x}_0$ corresponds to the neutral element of $G(k_s)$), and we obtain a bijection between

$$k\text{-torsors under } G \text{ up to isomorphism}$$

and

$$\text{the pointed set } H^1(k, G) = H^1(\mathrm{Gal}(k_s|k), G(k_s)).$$

The distinguished point represents the class of the trivial torsor, i.e. G with its right action on itself.

Proposition 3.2.4. *Let G be an algebraic group over k and let X be a k-torsor under G. The following are equivalent:*

(1) X is isomorphic to the trivial k-torsor G,

(2) X has a k-point, i.e. $X(k) \neq \emptyset$,

Proof. Suppose X is isomorphic to the trivial k-torsor G. Note that $G(k)$ contains the neutral element, hence $X(k)$ is non-empty. Conversely, take $x \in X(k)$ and define a map $\varphi : G \to X$, $g \mapsto x.g$. This can be visualized by the following commutative diagram:

$$\begin{tikzcd} X \times_k G \arrow[r] \arrow[d, "pr_2"'] & X \times_k X \arrow[d, "pr_2"] \\ G \arrow[r, dashed] & X. \end{tikzcd}$$

Since the morphism $X \times_k G \to X \times_k X$ is an isomorphism, $X \times_k G \to X$, $(x, g) \mapsto x.g$ is a surjective morphism. It follows that φ is a homeomorphism. Finally by the commutativity of the diagram above, we obtain a morphism $\mathcal{O}_X \to \varphi_* \mathcal{O}_G$ of sheaves on X. Thus $\varphi : G \to X$ is a k-isomorphism. $\square$

3.3 Torsors over schemes

In this section, we study the constructions of X-torsors under an fppf X-group scheme G, the classification by Čech cohomology and end up with connections to rational points.

3.3.1 Torsors and Čech cohomology

Now we study the classification of X-torsors under an fppf X-group scheme G. The isomorphism classes of torsors are naturally described by the elements of the first non-abelian Čech cohomology **set**. We first recall the usual definition of the Čech cohomology with coefficients in a presheaf $\mathcal{P}$ of abelian groups.

Abelian Čech cohomology revisited

Construction. Suppose X is a scheme. Let $\mathfrak{U} = \{U_j \to X\}_{j \in J}$ be a covering in the étale topology over X. Let $\mathcal{P}$ be a presheaf of abelian groups on the étale (resp. fppf) topology over X. We write $U_{ij} = U_i \times_X U_j$ and $U_{ijk} = U_i \times_X U_j \times_X U_k$, and so on. If $I \subset J^{n+1}$ is a sequence $(j_0, \ldots, j_n)$ of indices of length $n+1$ then we write $I^{\hat{j}}$ for the sequence $(i_0, \ldots, \hat{i_j}, \ldots, i_n)$ of indices of length n. The canonical projections $p_{I^{\hat{j}}} : U_I \to U_{I^{\hat{j}}}$ induce the maps $p^*_{I^{\hat{j}}} : \mathcal{P}(U_{I^{\hat{j}}}) \to \mathcal{P}(U_I)$. The Čech complex consists of

$$\check{C}^n(\mathfrak{U}, \mathcal{P}) = \prod_{|I|=n+1} \mathcal{P}(U_I)$$

with differentials

$$(d^n x)_I = \sum_{j=0}^{n+1} (-1)^j p^*_{I^{\hat{j}}}(x_{I^{\hat{j}}})$$

defined for $|I| = n+2$ and $x \in \check{C}^n(\mathfrak{U}, \mathcal{P})$. The Čech cohomology groups $\check{H}^n(\mathfrak{U}|X, \mathcal{P})$ are the cohomology groups of the complex $\check{C}^\bullet(\mathfrak{U}, \mathcal{P})$, i.e.

$$\check{H}^n(\mathfrak{U}|X, \mathcal{P}) = H^n(\check{C}^\bullet(\mathfrak{U}, \mathcal{P})),$$

and $\check{H}^n(X, \mathcal{P})$ can be identified by passing to the inductive limit for all coverings (see III.2 in [37]).

Remark 3.3.1. We have a natural map $\pi : \mathcal{P}(X) \to \check{H}^0(\mathfrak{U}|X, \mathcal{P})$ constructed as follows. Let $\varphi_j : U_j \to X$ be the étale morphism for each $j \in J$. Then we obtain an induced morphism $\varphi_j^* : \mathcal{P}(X) \to \mathcal{P}(U_j)$. By construction, $\check{H}^0(\mathfrak{U}|X, \mathcal{P})$ consists of elements $s = (s_j)_{j \in J}$ such that $(d^0 s)_{ij} = p^*_{\hat{i}j}(s_j) - p^*_{i\hat{j}}(s_i) = 0$ for all $i \neq j$ in J. Here $p^*_{i\hat{j}} : \mathcal{P}(U_i) \to \mathcal{P}(U_{ij})$ is the morphism induced by the projection $U_{ij} \to U_i$ and $p^*_{\hat{i}j}$ is similarly defined. Since $U_{ij} = U_i \times_X U_j$, we have $p^*_{i\hat{j}} \circ \varphi_i^* = p^*_{\hat{i}j} \circ \varphi_j^*$ for all $i, j \in J$. Now we consider $x^* = (\varphi_i^*(x)) \in \prod \mathcal{P}(U_i)$, then we have

$(dx^*)_{ij} = p_{\hat{i}j}^*\varphi_j^*(x) - p_{i\hat{j}}^*\varphi_i^*(x) = 0$ by construction. This shows the image of $\mathcal{P}(X)$ lies in $\operatorname{Ker} d^0$ and hence we obtain a natural map $\mathcal{P}(X) \to \check{H}^0(\mathfrak{U}|X, \mathcal{P})$.

If $\mathcal{P}$ is a sheaf, then we have an exact sequence

$$\mathcal{P}(X) \to \prod_{i\in I} \mathcal{P}(U_i) \rightrightarrows \prod_{i,j\in I} \mathcal{P}(U_{ij}).$$

Therefore $\mathcal{P}(X)$ is identified with the kernel of the right arrow, which is $\check{H}^0(\mathfrak{U}|X, \mathcal{P})$.

By the spectral sequence for Čech cohomology (1.3.15), we have the spectral sequence

$$\check{H}^p(\mathfrak{U}|X, \mathcal{H}^q(\mathcal{P})) \Rightarrow H^{p+q}(X, \mathcal{P}),$$

where $\mathcal{H}^q(\mathcal{P})$ is the presheaf $U \mapsto H^q(U, \mathcal{P})$.

If a morphism $Y \to X$ is a covering, then we obtain a spectral sequence

$$\check{H}^p(Y|X, \mathcal{H}^q(\mathcal{P})) \Rightarrow H^{p+q}(X, \mathcal{P}).$$

The corresponding exact sequence of low degree terms begins as follows

$$0 \to \check{H}^1(Y|X, \mathcal{P}) \to H^1(X, \mathcal{P}) \to \check{H}^0(Y|X, \mathcal{H}^1(\mathcal{P})) \to \check{H}^2(Y|X, \mathcal{P}) \to H^2(X, \mathcal{P}).$$

We give examples of X-torsors when the above sequences have explicit descriptions.

Example 3.3.2 (Hochschild-Serre spectral sequence)**.** Let F be a finite group. A finite étale Galois covering $Y|X$ with Galois group F is an X-torsor under an X-group scheme F_X which as an X-scheme is the disjoint union of $|F|$ copies of X with the group structure inherited from that of F.

For any sheaf $\mathcal{P}$, we have

$$\mathcal{P}(Y \times_X F^n) = \operatorname{Hom}_{\mathfrak{Set}}(F^n, \mathcal{P}(Y)).$$

A direct verification then shows that the Čech complex $\check{C}^\bullet(Y|X, \mathcal{P})$ is isomorphic to the complex of non-homogeneous cochains of the group F with coefficients in $\mathcal{P}(Y)$. Thus the Čech cohomology groups of the canonical covering are computed in terms of group cohomology:

$$\check{H}^i(Y|X, \mathcal{P}) = H^i(F, \mathcal{P}(Y)).$$

Suppose now that our topology is flat or étale. Then Čech spectral sequence associated to the canonical covering is the Hochschild-Serre spectral sequence

$$H^p(F, H^q(Y, \mathcal{P})) \Rightarrow H^{p+q}(X, \mathcal{P}).$$

Passing to the limit, one extends this to profinite Galois coverings.

Sheaves of torsors over topologies

Now we define sheaves of torsors and classify them by non-abelian Čech cohomology set.

Definition 3.3.1. Let T be a topology. Let $\mathcal{G}$ be a sheaf of groups on T.

(1) A sheaf of **pseudo torsors** under $\mathcal{G}$ is a sheaf of sets $\mathcal{F}$ on T endowed with an action $\mathcal{G} \times \mathcal{F} \to \mathcal{F}$ such that the action $\mathcal{G}(U) \times \mathcal{F}(U) \to \mathcal{F}(U)$ is simply transitive when $\mathcal{F}(U)$ is non-empty.

A morphism $\mathcal{F} \to \mathcal{F}'$ of sheaves of pseudo torsors under $\mathcal{G}$ is a morphism of sheaves of sets compatible with the $\mathcal{G}$-actions.

(2) A sheaf of **torsors** under $\mathcal{G}$ is a sheaf $\mathcal{F}$ of pseudo torsors under $\mathcal{G}$ such that for each object U in T, there exists a covering $\{U_i \to U\}_{i\in I}$ of U such that $\mathcal{F}(U_i)$ is non-empty for all $i \in I$. In this case, we may say $\mathcal{F}$ is trivialized on the covering $\{U_i \to U\}_{i\in I}$.

A morphism of sheaves of torsors under $\mathcal{G}$ is a morphism of sheaves of pseudo torsors under $\mathcal{G}$. We may simply say a $\mathcal{G}$-torsor rather than a sheaf of torsors under $\mathcal{G}$.

(3) The **trivial** $\mathcal{G}$-torsor is the sheaf $\mathcal{G}$ endowed with the right $\mathcal{G}$-action.

Classification of torsors under $\mathcal{G}$

By construction of differentials in the Čech complex, a 1-cocycle $s \in \check{C}^1(\mathfrak{U}, \mathcal{G})$ with respect to the covering $\mathfrak{U} = \{U_i \to X\}_{i \in I}$ consists of a family $s_{ij} \in \mathcal{G}(U_{ij})$ for all $i, j \in I$ such that after restricting to U_{ijk} we have $s_{ij}s_{jk} = s_{ik}$. The cocycles s and s' are cohomologous if there exist elements $h_i \in \mathcal{G}(U_i)$ such that after restricting to U_{ij} we have $s'_{ij} = h_i s_{ij} h_j^{-1}$. The pointed set of cohomology classes is denoted by $\check{H}^1(\mathfrak{U}|X, \mathcal{G})$. Passing to the inductive limit for all coverings we obtain the set $\check{H}^1(X, \mathcal{G})$.

Let $\mathcal{Y}$ be a sheaf of torsors over X under $\mathcal{G}$ trivialized on a covering $\mathfrak{U} = \{U_i \to X\}_{i \in I}$. By assumption $\mathcal{Y}(U_i)$ is non-empty for each $i \in I$, hence we can choose local sections $y_i \in \mathcal{Y}(U_i)$. Then there exists a unique $s_{ij} \in \mathcal{G}(U_{ij})$ such that $y_i s_{ij} = y_j$ on $\mathcal{G}(U_{ij})$ by the simple transitivity. Hence we have $y_i s_{ik} = y_i s_{ij} s_{jk}$ for each i, j, k pairwise distinct, and again by the simple transitivity we conclude the family $\{s_{ij}\}$ is a 1-cocycle with coefficients in $\mathcal{G}$. This associates to a sheaf of torsors $\mathcal{Y}$ over X under $\mathcal{G}$ trivialized by $\mathfrak{U}$ a class in $\check{H}^1(\mathfrak{U}|X, \mathcal{G})$. The distinguished element of $\check{H}^1(\mathfrak{U}|X, \mathcal{G})$ corresponds to the sheaf of trivial torsors $\mathcal{G}$. This defines a bijection, more precisely, an isomorphism of pointed sets between

$$\text{sheaves of torsors over } X \text{ under } \mathcal{G} \text{ trivialized on } \mathfrak{U} \text{ up to isomorphism}$$

and

$$\text{the pointed set } \check{H}^1(\mathfrak{U}|X, \mathcal{G}).$$

Passing to the inductive limit, we obtain a bijection between

$$\text{sheaves of torsors over } X \text{ under } \mathcal{G} \text{ up to isomorphism}$$

and

$$\text{the pointed set } \check{H}^1(X, \mathcal{G}).$$

The cohomology class of a torsor $Y \to X$ in the relevant cohomology set (or group) is denoted by $[Y]$.

Remark 3.3.3. Let X be a scheme and let $\mathcal{G}$ be a sheaf of groups on the étale topology over X. Now we have a contravariant functor $\mathcal{G} : X_{\text{ét}} \to \mathfrak{Gr}$. When $\mathcal{G}$ is represented by an étale X-group scheme G, i.e. $\mathcal{G}(-) = \mathrm{Hom}_{\mathfrak{Sch}_X}(-, G)$, we shall write G instead of $\mathcal{G}$.

Example 3.3.4. Let X be a scheme and let $\mathcal{G}$ be a sheaf of groups on the flat topology over X. Suppose $\mathcal{G}$ is represented by G.

(1) If G is such that every sheaf of torsors over X under G is represented by an X-scheme, we have a bijection between

$$\{X\text{-torsors under } G \text{ up to isomorphism}\} \quad \text{and} \quad \{\text{the pointed set } \check{H}^1(X, G)\}.$$

(2) If G is commutative, we can replace the Čech cohomology group by the flat cohomology group and hence we obtain a bijection between X-torsors under G up to isomorphism and the group $H^1(X, G)$. Indeed, now $\mathcal{G}$ is a sheaf of abelian groups on the flat topology over X. It is known that $H^1(X, \mathcal{G})$ can always be computed as $\check{H}^1(X, \mathcal{G})$. More details are in [37], chapter III, corollary 2.10.

(3) If we assume further G is smooth over X, the flat topology can be replaced by the étale topology (Cf. [37], III.4). Thus when G is commutative, X-torsors under G are classified by the elements of the group $H^1_{\text{ét}}(X, G)$.

Let $\check{\mathcal{H}}^0(\mathcal{G})$ be the presheaf of groups defined by $U \mapsto \check{H}^0(U, \mathcal{G})$ and let $\check{\mathcal{H}}^1(\mathcal{G})$ be the presheaf of pointed sets defined by $U \mapsto \check{H}^1(U, \mathcal{G})$. For any sheaf of sets we have $\mathcal{G} = \check{\mathcal{H}}^0(\mathcal{G})$. Then there is an exact sequence of pointed sets

$$1 \to \check{H}^1(\mathfrak{U}|X, \mathcal{G}) \to \check{H}^1(X, \mathcal{G}) \to \check{H}^0(\mathfrak{U}|X, \check{\mathcal{H}}^1(\mathcal{G})).$$

The last arrow is given by the collection of restrictions from X to U_i, and $\check{H}^1(\mathfrak{U}|X, \check{\mathcal{H}}^0(\mathcal{G}))$ parameterizes the classes of cocycles trivialized on $\mathfrak{U}$.

Lemma 3.3.5. *Let G and G' be algebraic groups over k, and let X and Y be k-varieties such that $Y \to X$ is an X-torsor under G. There is an exact sequence of pointed sets*

$$1 \to \check{H}^1(Y|X, G') \to \check{H}^1(X, G') \to \check{H}^0(Y|X, \check{\mathcal{H}}^1(G')).$$

The pointed set $\check{H}^1(Y|X, G')$ can be interpreted as the set of equivalence classes of morphisms $f : Y \times_k G \to G'$ satisfying the cocycle condition $f(y,s)f(ys,s') = f(y,ss')$; f is equivalent to f' if

$$f'(y,s) = g(y)f(y,s)g(ys)^{-1}$$

for a morphism $g : Y \to G'$. If $G = G'$, then the class of the torsor $Y \to X$ in $\check{H}^1(Y|X, G)$ is given by the second projection $Y \times_k G \to G$.

Proof. All statements except the last one are straightforward. The last statement is verified directly from the definitions. Indeed, the torsor $Y \to X$ is trivialized by the covering $Y \to X$, and the map $Y \times_X Y \to Y$ has a section given by the diagonal morphism. Then the cocycle of $Y \to X$ in $H^0(Y \times_X Y, G)$ becomes the second projection after the isomorphism $H^0(Y \times_X Y, G) = H^0(Y \times_k G, G)$. □

3.3.2 Twisting by fppf descent

The construction of twisting by fppf descent is crucial for the application of torsors. Let G be an fppf X-group scheme. Let P be a right X-torsor under G and let Q be a scheme affine over X equipped with a left G-action which is compatible with the projection to X. We write $\rho_P : P \times_X G \to P$ and $\rho_Q : G \times_X Q \to Q$ for the G-actions. From the following diagram

$$\begin{tikzcd}
P \times_X G \times_X Q \arrow[rr, "pr"] \arrow[d, "pr"'] \arrow[dr, dashed] & & G \times_X Q \arrow[d, "\rho_Q"] \\
P \times_X G \arrow[d, "\mathrm{id} \times \mathrm{inv}"'] & P \times_X Q \arrow[r, "pr"] \arrow[d, "pr"'] & Q \arrow[d] \\
P \times_X G \arrow[r, "\rho_P"'] & P \arrow[r] & X
\end{tikzcd}$$

where each pr denotes the projection, we obtain a G-action

$$\rho : P \times_X G \times_X Q \to P \times_X Q$$

on $P \times_X Q$. After applying the functor of points, we may denote this action by $(p,q) \mapsto (pg^{-1}, gq)$ for $g \in G$.

Lemma 3.3.6. *The quotient of $P \times_X Q$ by the G-action ρ given by $(p,q) \mapsto (pg^{-1}, gq)$ exists as a scheme affine over X. In other words, there exists a morphism of X-schemes $\pi : P \times_X Q \to Y$ for some scheme Y endowed with an affine morphism $Y \to X$, such that fibres of π are orbits of G.*

Before we prove lemma (3.3.6), we give the following definition and we quote a result on descent theory of Grothendieck.

Definition 3.3.2. By lemma (3.3.6), the quotient of $P \times_X Q$ by the G-action exists. It is called the **contracted product** of P and Q with respect to G or the **twist** of Q by the X-torsor P. The quotient is denoted by $P \times_X^G Q$, $P \times^G Q$ or simply by ${}_PQ$. Note that P has the structure of a left X-torsor under ${}_PG$, so that ${}_PG$ acts on ${}_PQ$ on the left.

Theorem 3.3.7. *Let $f : P \to X$ be a faithfully flat and quasi-compact morphism of schemes. To give a scheme Y affine over X is the same as to give a scheme Y' affine over P together with an isomorphism $\varphi : p_1^*Y' \to p_2^*Y'$ satisfying the cocycle condition*

$$p_{31}^*(\varphi) = p_{32}^*(\varphi)p_{21}^*(\varphi),$$

where $p_1, p_2 : P \times_X P \to P$ and $p_{ij} : P \times_X P \times_X P \to P \times_X P$ for $i > j$ are the projections.

Proof. See [37], chapter I, theorem 2.23. □

Proof of (3.3.6). Let $p_1, p_2 : P \times_X P \to P$ and $p_{ij} : P \times_X P \times_X P \to P \times_X P$ for $i > j$ be the projections. Since P is a right X-torsor under G, we conclude

$$(P \times_X P) \times_P (P \times_X Q) \simeq P \times_X G \times_X Q.$$

Note that the G-action on $G \times_X Q$ is given by $(x, q) \mapsto (xg^{-1}, gq)$, therefore each orbit can be represented by (id_G, q) for a unique q. Thus to take the contracted product $G \times^G Q$ is the same as considering the morphism $\rho_Q : G \times_X Q \to Q$ given by the left G-action on Q. We conclude that $G \times^G Q$ exists and is canonically isomorphic to Q. Set $Y' = P \times_X Q$ and let

$$p_1^* Y' = P \times_X P \times_X Q \xrightarrow{\varphi} P \times_X P \times_X Q = p_2^* Y'$$

be the morphism given by $(x_1, x_2, q) \mapsto (x_1, x_2, s_{21}.q)$ where s_{21} is the unique element in G such that $x_2 = x_1.s_{21}$. From the following sequence

$$P \times_X P \times_X Q \to P \times_X G \times_X Q \to P \times_X G \times_X Q \to P \times_X P \times_X Q$$

given by

$$(x_1, x_2, q) \mapsto (x_1, s_{21}, q) \mapsto (x_1, s_{21}, s_{21}.q) \mapsto (x_1, x_2, s_{21}.q),$$

we obtain $(x_1, x_2, q) \mapsto (x_1, x_2, s_{21}.q)$ defines an isomorphism $\varphi : p_1^* Y' \to p_2^* Y'$. Then we need to check $p_{31}^*(\varphi) = p_{32}^*(\varphi) p_{21}^*(\varphi)$. Indeed, $p_{31}^*(\varphi)$ sends (x_1, x_2, x_3, q) to $(x_1, x_2, x_3, s_{31}.q)$ where $x_3 = x_1.s_{31}$. Similarly we obtain s_{21} and s_{32}. We have $s_{31} = s_{32} s_{21}$ since P is an X-torsor under G and thus the cocycle condition holds. This gives the existence of Y by descent theory. The map $P \times_X P \times_X Q \simeq P \times_X G \times_X Q \to P \times_X Q = Y'$ (quotient by G acting as in the statement of the lemma) descends to $P \times_X Q \to P \times^G Q = Y$. □

Example 3.3.8 (inner forms)**.** We take $Q = G$ and consider a left G-action $\rho_G : G \times_X G \to G$ given by conjugations $(g, x) \mapsto gxg^{-1}$. The contracted product is an X-group scheme ${}_PG = P \times^G G$, which locally in the fppf topology is isomorphic to G. If $X = \operatorname{Spec} k$, then ${}_PG$ is the inner form G^σ of G, where P is the k-torsor defined by $\sigma \in Z^1(\mathrm{Gal}(\bar{k}|k), G)$.

Example 3.3.9 (the inverse torsor)**.** Suppose Q is a left X-torsor under G with G-action $\rho : G \times_X Q \to Q$. We construct a right X-torsor Q' under G as follows. As an X-scheme, we put Q' to be isomorphic to Q via $\iota : Q' \to Q$. From the following diagram

$$\begin{tikzcd}
Q' \times_X G \arrow[dr, dashed] \arrow[drr, "\iota \circ pr_1"] \arrow[ddr, "\mathrm{inv} \circ pr_2"'] & & \\
& G \times_X Q \arrow[r] \arrow[d] & Q \arrow[d] \\
& G \arrow[r] & X
\end{tikzcd}$$

where $\mathrm{inv} : G \to G$ denotes the morphism $g \mapsto g^{-1}$, we obtain a morphism

$$Q' \times_X G \to G \times_X Q.$$

We obtain a morphism $\rho' : Q' \times_X G \to Q'$ by composition with $\iota^{-1} \circ \rho$. Let T be an X-scheme and let $(q', g) \in Q'(T) \times G(T)$. Then $\rho'(q', g) = \iota^{-1} \rho(g^{-1}, \iota(q'))$ by construction. It follows that $\rho'(q', \mathrm{id}_{G(T)}) = \iota^{-1} \iota(q') = q'$ and

$$\begin{aligned}
\rho'(q', g_1 g_2) &= \iota^{-1} \rho(g_2^{-1} g_1^{-1}, \iota(q')) = \iota^{-1} \rho(g_2^{-1}, \rho(g_1^{-1}, \iota(q'))) \\
&= \rho'(\iota^{-1} \rho(g_1^{-1}, \iota(q')), g_2) = \rho'(\rho'(g', g_1), g_2).
\end{aligned}$$

Therefore $\rho' : Q' \times_X G \to Q'$ is a right G-action. To simplify the notation, we may omit the isomorphism ι and simply denote this right G-action by

$$\rho' : Q' \times_X G \to Q',\ (q,g) \mapsto \rho(g^{-1}, q).$$

It is straightforward that Q' is a right X-torsor under G. Moreover, we can show that

$$Q' \times^G Q \simeq G.$$

In other terms, the diagonal image of Q in $Q' \times_X Q$ is an orbit of G, leading to a section of the quotient X-scheme. Therefore we call Q' the **inverse torsor** of Q under G.

Example 3.3.10 (twisting an X-torsor)**.** Let Q be a left X-torsor under G, let Q' be the inverse torsor of Q. Like any right torsor under G, Q' is also a left X-torsor under $G' := {}_{Q'}G$. Then Q is equipped with the structure of a right X-torsor under G' with respect to the action $x.g' := (g')^{-1}x$ for $g' \in G'$. Summing up, the contracted product $P \times^G Q$ is a right X-torsor under G', and a left X-torsor under ${}_PG$. The operation $P \mapsto P \times^G Q$ defines a bijection of sets

$$\check{H}^1(X, G) \to \check{H}^1(X, G'),$$

which sends the distinguished point to the class of Q. The inverse bijection is obtained by

$$\check{H}^1(X, G') \to \check{H}^1(X, G),\ P \mapsto P \times^{G'} Q',$$

i.e. taking the contracted product with Q' with respect to G'.

In the case when G is abelian, there is no difference between G and G', and the contracted product defines a group structure on $\check{H}^1(X, G)$, and the above bijection is just the translation by the class of Q.

Remark 3.3.11 (Twist right torsors by another right torsors)**.** When we have to twist a right X-torsor P under G with another right X-torsor E under G, we first consider the inverse E' which is a left torsor under G, and then form the contracted product $P \times^G E'$. In this case the twist $P \times^G E'$ is a right X-torsor under ${}_EG$, and is denoted by ${}_EP$. For example, ${}_PP$ is a trivial torsor under ${}_PG$. If G is abelian, the class of E' is the inverse of the class of E, hence in the group $H^1(X, G)$ we have a relation $[{}_EP] = [P] - [E]$.

We shall mostly deal with the case when X and P are varieties over k, G comes from an algebraic group over k and $E = X \times_k Z$, where Z is a right k-torsor under G. Then ${}_EP$, also denoted by ${}_ZP$, can be obtained by Galois descent: take a cocycle $\sigma \in Z^1(\mathrm{Gal}(\overline{k}|k), G)$ defining Z, then consider the quotient P^σ of $\overline{P}$ by the corresponding twisted action of $\mathrm{Gal}(\overline{k}|k)$, which is $(g, x) \mapsto {}^gx\sigma^{-1}(g)$. Note that to use Galois descent we need the assumption that P is a quasi-projective k-variety.

3.3.3 Partition of $X(k)$ defined by a torsor

Let k be a field. Let X be a variety over k and let G be an algebraic group over k. Let $f : Y \to X$ be an X-torsor under G. Suppose Z is a right k-torsor under G corresponding to the class $\sigma \in H^1(k, G)$. Let ${}_Zf : {}_ZY \to X$ be the corresponding twisted right X-torsor under ${}_ZG$. It exists provided Y is quasi-projective or G is affine.

Let $f : Y \to X$ be an X-torsor under G. For each rational point $P \in X(k)$, then the fibre Y_P is a $\kappa(P)$-torsor under G by verifying $Y_P \times_{\kappa(P)} G \to Y_P \times_{\kappa(P)} Y_P$ is an isomorphism. Note that P is a k-point on X, so $\kappa(P) \simeq k$ and we obtain the class $[Y_P]$ of Y_P in $H^1(k, G)$. Summing up, we obtain a well-defined map

$$\theta_Y : X(k) \to H^1(k, G),\ P \mapsto [Y_P].$$

This gives a partition of the set $X(k)$ into the subsets of points such that the corresponding fibres of f are isomorphic k-torsors under G,

$$X(k) = \bigsqcup_{\sigma \in H^1(k,G)} \theta_Y^{-1}(\sigma) = \bigsqcup_{\sigma \in H^1(k,G)} \{P \in X(k) \mid [Y_P] = \sigma\}.$$

Using the twisting operation, we can describe the partition of $X(k)$ defined by $f : Y \to X$ in a slightly different fashion. For $\sigma \in H^1(k, G)$, let $f^\sigma : Y^\sigma \to X$ be the twisted k-torsor under G^σ.

Lemma 3.3.12. *Suppose G is an fppf group scheme which is affine over X. We have*

$$\{P \in X(k) \mid [Y_P] = \sigma\} = f^\sigma(Y^\sigma(k)).$$

Proof. Let $P \in X(k)$ and let Z be a right k-torsor under G such that $[Z] = \sigma$ in $H^1(k, G)$.

Note that $P \in f^\sigma(Y^\sigma(k))$ holds if and only if $Y_P^\sigma(k) \neq \emptyset$, which is equivalent to say Y_P^σ is a trivial k-torsor under G^σ. Therefore $Y_P \times^G Z'$ is a trivial k-torsor under G. By taking the contracted product with Z on the right, we conclude $Y_P \simeq Z$ as k-torsors under G. This shows that $[Y_P] = \sigma$. Conversely, we have $Y_P \simeq Z$ as k-torsors under G. This implies Y_P^σ is a trivial k-torsor under G^σ. □

We summarize this by the formula

$$X(k) = \bigcup_{\sigma \in H^1(k,G)} f^\sigma(Y^\sigma(k)).$$

Here Z runs over the set of k-torsors under G containing one representative from every isomorphism class.

3.4 Descent obstructions

Let G be an affine algebraic group over k. Twisting a right X-torsor $f : Y \to X$ under G by a cocycle $\sigma \in Z^1(k, G)$ produces a right X-torsor $f^\sigma : Y^\sigma \to X$ under the twisted group G^σ. This operation commutes with base change. For example, twist operation commutes with taking the fibre Y_P at a k-point of X. In the abelian case, the inner form G^σ can be identified with G and the map $H^1(X, G) \to H^1(X, G^\sigma)$ is just the translation by $-[\sigma]$. Replacing σ by a cohomologous cocycle gives an isomorphic torsor. In particular, the subset $f^\sigma(Y^\sigma(k))$ of $X(k)$ depends only on the class $[\sigma] \in H^1(k, G)$. We shall use the notation $H^1(X, G)$ for the Čech cohomology set $\check{H}^1(X, G)$, this set classifies X-torsors under G up to isomorphism. We have the following partition of $X(k)$:

$$X(k) = \bigcup_{[\sigma] \in H^1(k,G)} f^\sigma(Y^\sigma(k)).$$

3.4.1 Descent obstruction to the Hasse principle

Suppose that $X(\mathbb{A}_k) \neq \emptyset$. Evaluating $f : Y \to X$ at an adelic point of X gives a map

$$\theta_f : X(\mathbb{A}_k) \to \prod_{v \in \Omega} H^1(k_v, G),\ (P_v) \mapsto ([Y_{P_v}]),$$

where $[Y_{P_v}]$ is the class of Y_{P_v} in $H^1(k_v, G)$. Note that since G is affine, then the set $H^1(k_v, G)$ is finite ([44] III.4). For each $\sigma \in Z^1(k, G)$, we let σ_v denote its image in $Z^1(k_v, G)$. This image is defined by first choosing a place w of $\overline{k}$ over v, and then restricting σ to the decomposition group D_w of w. The union of completions at w of finite subextensions $\overline{k}$ is an algebraic closure of k_v, and D_w is its Galois group over k_v ([44] p. 115). The corresponding map of cohomology sets $H^1(k, G) \to H^1(k_v, G)$ sends the class of a torsor T to the class of $T \times_k k_v$.

Definition 3.4.1. Let X be a smooth and geometrically integral variety over a number field k and let S be a finite set of places of k. Let $f : Y \to X$ be a torsor under a linear algebraic group G over k. Define $X(\mathbb{A}_k^S)^f$ as the subset of $X(\mathbb{A}_k^S)$ consisting of adelic points whose image under the evaluation map

$$X(\mathbb{A}_k^S) \to \prod_{v \in \Omega - S} H^1(k_v, G),\ (x_v) \mapsto ([Y_{x_v}])$$

comes from an element of $H^1(k,G)$. More explicitly,

$$X(\mathbb{A}_k^S)^f = \big\{(x_v) \in X(\mathbb{A}_k^S) \mid ([Y_{x_v}]) \in \operatorname{Im}(H^1(k,G) \to \prod_{v\in\Omega-S} H^1(k_v,G))\big\}.$$

Applying the twist operation, we obtain the following description:

$$X(\mathbb{A}_k^S)^f = \bigcup_{\sigma\in H^1(k,G)} f^\sigma(Y^\sigma(\mathbb{A}_k^S)).$$

We have $X(k) \subset X(\mathbb{A}_k^S)^f \subset X(\mathbb{A}_k^S)$.

When $S=\emptyset$, we shall write $X(\mathbb{A}_k)$ instead of $X(\mathbb{A}_k^\emptyset)$. The emptiness of $X(\mathbb{A}_k)^f$ is thus an obstruction to the existence of a k-point on X. In other words, when $X(\mathbb{A}_k)$ is non-empty the emptiness of $X(\mathbb{A}_k)^f$ is an obstruction to the Hasse principle. We call it **the descent obstruction to the Hasse principle associated to** $f : Y \to X$.

It is clear from this definition that $X(\mathbb{A}_k)^f$ depends only on the isomorphism class $[Y] \in H^1(X,G)$.

Note that if G is a k-group of multiplicative type, the diagonal image of $H^1(k,G)$ in the product $\prod_{v\in\Omega} H^1(k_v,G)$ is described by the Poitou-Tate exact sequence (cf. [38], I.4.20(b), I.4.13). There is a generalization of this sequence, due to R. Kottwitz, to the case when G is connected and reductive. A complete proof is also contained in [1], page 43, theorem 5.16.

Proposition 3.4.1. *Let $f : Y \to X$ be a torsor under a liner algebraic group G, and assume that X is a proper k-variety. Let $S \subset \Omega$ be a finite set of places. Then there are only finitely many classes $[\sigma] \in H^1(k,G)$ such that $Y^\sigma(k^S) \neq \emptyset$.*

Proof. For a finite set of places $S' \supset S$ containing all the archimedean places of k, let $\mathcal{O}_{k,S'} \subset k$ be the ring of S'-integers of k. Let us fix S' sufficiently large such that G extends to a smooth group scheme $\mathcal{G}$ over $\operatorname{Spec}\mathcal{O}_{k,S'}$, X extends to a proper scheme $\mathcal{X}$ over $\operatorname{Spec}\mathcal{O}_{k,S'}$, and Y extends to an $\mathcal{X}$-torsor $\mathcal{Y}$ under $\mathcal{G}$. These are visualized as the following fibred product squares:

$$\begin{array}{ccc} G & \longrightarrow & \mathcal{G} \\ \downarrow & & \downarrow \\ \operatorname{Spec} k & \longrightarrow & \operatorname{Spec}\mathcal{O}_{k,S'} \end{array} \qquad \begin{array}{ccc} X & \longrightarrow & \mathcal{X} \\ \downarrow & & \downarrow \\ \operatorname{Spec} k & \longrightarrow & \operatorname{Spec}\mathcal{O}_{k,S'} \end{array} \qquad \begin{array}{ccc} Y & \longrightarrow & \mathcal{Y} \\ \downarrow & & \downarrow \\ X & \longrightarrow & \mathcal{X}. \end{array}$$

Let G^0 be the connected component of G. Then $F = G/G^0$ is a finite k-group. We denote by $\mathcal{G}^0$ and $\mathcal{F}$ some group schemes over $\operatorname{Spec}\mathcal{O}_{k,S'}$ extending G^0 and F, respectively. By enlarging S', we can assume that there is an exact sequence

$$1 \to \mathcal{G}^0 \to \mathcal{G} \to \mathcal{F} \to 1.$$

Then we have a commutative diagram

$$\begin{array}{ccccc} H^1(\mathcal{O}_v,\mathcal{G}) & \longrightarrow & H^1(k_v,G) & \longleftarrow & H^1(k,G) \\ \downarrow{\scriptstyle p_v} & & \downarrow{\scriptstyle \pi_v} & & \downarrow{\scriptstyle \pi} \\ H^1(\mathcal{O}_v,\mathcal{F}) & \longrightarrow & H^1(k_v,F) & \longleftarrow & H^1(k,F) \end{array}$$

for each place $v \notin S'$.

Let $\sigma \in H^1(k,G)$ be such that $Y^\sigma(k^S) \neq \emptyset$. We denote by σ_v the image of σ in $H^1(k_v,G)$ under the above homomorphism. By construction, the condition $Y^\sigma(k_v) \neq \emptyset$ means that there exists a k_v-point $x_v \in X(k_v)$ such that $[Y_{x_v}] = \sigma_v$. Since $\mathcal{X}$ is proper over $\mathcal{O}_{k,S'}$, we have $X(k_v) = \mathcal{X}(\mathcal{O}_v)$ for each $v \notin S'$. Therefore the class σ_v coincides with the image of $[\mathcal{Y}_{x_v}]$ under the natural map $H^1(\mathcal{O}_v,\mathcal{G}) \to H^1(k_v,G)$ for each $v \notin S'$ by our choice of S'. Thus the image of σ_v in $H^1(k_v, F)$ comes from $H^1(\mathcal{O}_v, \mathcal{F})$ for each $v \notin S'$. Suppose the image of $\sigma \in H^1(k, G)$ in $H^1(k, F)$ is represented by a k-torsor Z under F.

Note that F is a finite k-group and hence Z is a 0-dimensional k-scheme. Moreover, we conclude $Z = \operatorname{Spec}\Gamma(Z, \mathcal{O}_Z)$ where the étale k-algebra $\Gamma(Z, \mathcal{O}_Z)$ is a product of separable extensions of k. The fact that the image of σ_v in $H^1(k_v, F)$ comes from $H^1(\mathcal{O}_v, \mathcal{F})$ implies that each of these fields are not ramified at each $v \notin S'$. The degrees of these extensions of k are bounded by $|F(\bar{k})|$. There are only finitely many extensions of k of bounded degree which are unramified away from S' (see [33], V.4, theorem 5). In particular, there exists a finite Galois field extension $k'|k$ which contains all these extensions. Thus the image of $\sigma \in H^1(k, G)$ in $H^1(k, F)$ is contained in a finite subset (the image of $H^1(\operatorname{Gal}(k'|k), F)$ in $H^1(k, F)$), which we an take to be the image of a finite subset $\Phi \subset H^1(k, G)$ consisting of elements coming from $H^1(\mathcal{O}_v, \mathcal{G})$ for each $v \notin S'$.

Now we conclude. Suppose that the set

$$\Lambda = \{\sigma \in H^1(k, G) \mid \pi(\sigma) = 1, \text{ and } \sigma_v \in \operatorname{Im}\left(H^1(\mathcal{O}_v, \mathcal{G}) \to H^1(k_v, G)\right) \text{ for each } v \notin S'\}$$

is finite. Then we are done by replacing G with its twist by a cocyle representing a class in Φ. So it is enough to show Λ is a finite set. Let $\rho_v \in H^1(\mathcal{O}_v, \mathcal{G})$ be a class mapping to $\sigma_v \in H^1(k_v, G)$. We claim that $p_v(\rho_v) = 1$ in $H^1(\mathcal{O}_v, \mathcal{F})$. Since $\pi(\sigma) = 1$, $\pi_v(\sigma_v) = 1$ by the commutativity of the right square. Hence it will be sufficient to show that the canonical map $H^1(\mathcal{O}_v, \mathcal{F}) \to H^1(k_v, F)$ between pointed sets has trivial kernel. Suppose that $\mathcal{U}$ is a $\operatorname{Spec}\mathcal{O}_v$-torsor under $\mathcal{F}$ such that the image of $[\mathcal{U}]$ in $H^1(k_v, F)$ is trivial. Since $\mathcal{F}$ is finite (hence proper) over $\mathcal{O}_v$, it follows $\mathcal{U}$ is also proper over $\mathcal{O}_v$. By the valuative criterion of the proper morphism $\mathcal{U} \to \operatorname{Spec}\mathcal{O}_v$, a section $\operatorname{Spec} k_v \to \mathcal{U}$ extends uniquely to a section $\operatorname{Spec}\mathcal{O}_v \to \mathcal{U}$. This means that $\mathcal{U}$ is a trivial $\operatorname{Spec}\mathcal{O}_v$-torsor and therefore $p_v(\rho_v) = 1$ in $H^1(\mathcal{O}_v, \mathcal{F})$. By construction of $\mathcal{F}$, we conclude that ρ_v comes from $H^1(\mathcal{O}_v, \mathcal{G}^0)$. However, every $\operatorname{Spec}\mathcal{O}_v$-torsor under the smooth and connected group $\mathcal{G}^0$ is trivial by Lang's theorem (which allows us to find a rational point in the closed fibre, see [32]) and Hensel's lemma (which allows us to lift it to a section over $\operatorname{Spec}\mathcal{O}_v$). It follows that $H^1(\mathcal{O}_v, \mathcal{G}^0)$ is trivial, hence $\rho_v = 1$ and this implies that its image $\sigma_v = 1$ in $H^1(k_v, G)$ for each $v \notin S'$. Since every set $H^1(k_v, G)$ is finite, the family

$$(\sigma_v) \in \prod_{v \in \Omega - S} H^1(k_v, G)$$

belongs to the finite subset of $\prod_{v \in \Omega - S} H^1(k_v, G)$ consisting of (α_v) such that α_v is arbitrary for $v \in S' - S$ and $\alpha_v = 1$ otherwise. Finally, by a theorem of Borel and Serre (see [44], III, 4.6) the natural diagonal map

$$H^1(k, G) \to \prod_{v \in \Omega - S} H^1(k_v, G)$$

has finite fibres, hence the inverse image of our finite subset is also finite. Thus the set of classes $\sigma \in H^1(k, G)$ such that $Y^\sigma(k_v) \neq \emptyset$ for any $v \notin S$ is finite. □

3.4.2 Descent obstruction to weak approximation

Let X be a proper, smooth and geometrically integral variety. We claim that the set $X(\mathbb{A}_k^S)^f$ also provides an obstruction to weak approximation away from S. The key fact is that the map

$$X(k_v) \to H^1(k_v, G), \ x_v \mapsto [f^{-1}(x_v)]$$

is locally constant when $X(k_v)$ is endowed with the v-adic topology. To see this, we can assume that $[f^{-1}(x_v)] = 0$ is the trivial torsor by applying the twist operation if necessary. Recall that the k_v-torsor $f^{-1}(x_v)$ is trivial iff it contains a k_v-point, so $x_v = f(y_v)$ for some $y_v \in Y(k_v)$. By the v-adic inverse function theorem over a small v-adic neighbourhood of x_v, we can find a section of f passing through y_v. Thus the class of the fibre is also 0 for all k_v-points in this neighbourhood.

Proposition 3.4.2. *Let X be a proper, smooth and geometrically integral variety such that $X(k) \neq \emptyset$. Let $\overline{X(k)}^S$ be the closure of the image of $X(k)$ in $X(\mathbb{A}_k^S)$. Then*

$$\overline{X(k)}^S \subset X(\mathbb{A}_k^S)^f.$$

Proof. By proposition (3.4.1), we can find a finite set $\Sigma \subset H^1(k, G)$ such that $Y^\sigma(\mathbb{A}_k^S) = \emptyset$ for $[\sigma] \notin \Sigma$. Therefore

$$X(\mathbb{A}_k^S)^f = \bigcup_{\sigma \in H^1(k,G)} f^\sigma(Y^\sigma(\mathbb{A}_k^S)) = \bigcup_{\sigma \in \Sigma} f^\sigma(Y^\sigma(\mathbb{A}_k^S))$$

is actually a finite union. Now it is enough to show that $f(Y(\mathbb{A}_k^S))$ is closed in $X(\mathbb{A}_k^S)$.

Let $(x_v) \in X(\mathbb{A}_k^S)$ be a point lies in the closure of $f(Y(\mathbb{A}_k^S))$. For any $v \notin S$, let $U_v \subset X(k_v)$ be a small neighbourhood of $x_v \in X(k_v)$ in the corresponding v-adic topology such that $[f^{-1}(x'_v)] = [f^{-1}(x_v)] \in H^1(k_v, G)$ for any $x'_v \in U_v$. The open set U_v contains the image $f(y_v)$ for some $y_v \in Y(k_v)$. Therefore $[f^{-1}(x_v)] = [f^{-1}(f(y_v))] = 0$, which means that the fibre above x_v is a trivial k_v-torsor and hence $x_v = f(z_v)$ for some $z_v \in Y(k_v)$. Hence $(x_v) \in f(Y(\mathbb{A}_k^S))$ which proves that $f(Y(\mathbb{A}_k^S))$ is closed. ☐

By (3.4.2), the condition $X(\mathbb{A}_k)^f \neq X(\mathbb{A}_k)$ is an obstruction to weak approximation on X, and $X(\mathbb{A}_k^S)^f \neq X(\mathbb{A}_k^S)$ is an obstruction to weak approximation outside S on X. Note that unlike the Brauer-Manin obstruction, the descent obstruction to weak approximation is only defined for **proper** varieties X (this comes from the fact that there is no convenient analogue of the unramified Brauer group).

Definition 3.4.2. Let X be a proper, smooth and geometrically integral variety such that $X(k) \neq \emptyset$.

(1) We say that X has the **descent obstruction to weak approximation associated to** $f : Y \to X$ if $X(\mathbb{A}_k)^f \neq X(\mathbb{A}_k)$.

(2) We say that X has the **descent obstruction to weak approximation outside** S **associated to** $f : Y \to X$ if $X(\mathbb{A}_k^S)^f \neq X(\mathbb{A}_k^S)$.

(3) We say that the descent obstruction to the Hasse principle and weak approximation associated to the torsor $f : Y \to X$ is **the only one** if

$$\overline{X(k)} = X(\mathbb{A}_k)^f.$$

3.4.3 The Manin obstruction as a particular case

Let k be a field and let X be a smooth k-variety. We denote by $\mathrm{Br}_{\mathrm{Az}}(X)$ the Brauer group of X. This is the group of similarity classes of Azumaya algebras over X. We have seen that there is a canonical injective map $\mathrm{Br}_{\mathrm{Az}}(X) \to \mathrm{Br}(X)$ holds for any scheme X. More precisely, the exact sequence of étale sheaves

$$1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1$$

gives rise to the exact sequence of pointed sets

$$H^1(X, \mathbb{G}_m) \to H^1(X, \mathrm{GL}_n) \to H^1(X, \mathrm{PGL}_n) \xrightarrow{d_n} \mathrm{Br}(X).$$

The group $\mathrm{Br}_{\mathrm{Az}}(X) \subset \mathrm{Br}(X)$ is the union of images of $d_n(H^1(X, \mathrm{PGL}_n))$ for all n. It is known that $d_n(H^1(X, \mathrm{PGL}_n)) \subset \mathrm{Br}_{\mathrm{Az}}(X)[n]$. If k is a number field or a local field, it is known that

$$d_n : H^1(\operatorname{Spec} k, \mathrm{PGL}_n) \to \mathrm{Br}(k)[n]$$

is bijective.

Proposition 3.4.3. *Let X be a proper, smooth and geometrically integral variety. Let $\mathbb{PGL}$ be the disjoint union of sets $H^1(X,\mathrm{PGL}_n)$ for all $n \geq 2$. We have*

$$X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{Az}}(X)} = \bigcap_{f\in\mathbb{PGL}} X(\mathbb{A}_k)^f.$$

Proof. For $n \geq 1$, let $d_n : H^1(X,\mathrm{PGL}_n) \to \mathrm{Br}(X)$ be the natural morphism obtained from the short exact sequence $1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1$ of étale sheaves on X. Take $\mathcal{A} \in \mathrm{Br}_{\mathrm{Az}}(X)$. Then $\mathcal{A} = d_n([Y])$ for some integer n and some X-torsor $f : Y \to X$ under PGL_n. Therefore $n\mathcal{A} = 0$ since the image of d_n is contained in the n-torsion part of $\mathrm{Br}_{\mathrm{Az}}(X)$.

Let $(x_v) \in X(\mathbb{A}_k)$. Then we have the following commutative diagram

$$\begin{tikzcd}
H^1(X,\mathrm{PGL}_n) \arrow[r, "d_n"] \arrow[d] & \mathrm{Br}(X)[n] \arrow[d] \\
\prod_{v\in\Omega} H^1(k_v,\mathrm{PGL}_n) \arrow[r, "d_n"] & \prod_{v\in\Omega} \mathrm{Br}(k_v)[n] \\
H^1(k,\mathrm{PGL}_n) \arrow[r, "d_n"] \arrow[u] & \mathrm{Br}(k)[n] \arrow[u]
\end{tikzcd}$$

where the upper vertical maps are induced by $x_v \in X(k_v)$, and the lower ones are the natural diagonal maps. The image of $[Y]$ in $\prod_{v\in\Omega} H^1(k_v,\mathrm{PGL}_n)$ is just $([Y_{x_v}])$ and the image of $[Y]$ in $\prod_{v\in\Omega} \mathrm{Br}(k_v)[n]$ via $\mathrm{Br}(X)[n]$ is $(\mathcal{A}(x_v))$. By the commutativity of the diagram, the image of $([Y_{x_v}])$ in $\prod_{v\in\Omega} \mathrm{Br}(k_v)[n]$ coincides with $(\mathcal{A}(x_v))$. Since the middle and the bottom horizontal maps are bijective, we conclude

$$([Y_{x_v}]) \in \mathrm{Im}\left(H^1(k,\mathrm{PGL}_n) \to \prod_{v\in\Omega} H^1(k_v,\mathrm{PGL}_n)\right)$$

if and only if

$$(\mathcal{A}(x_v)) \in \mathrm{Im}\left(\mathrm{Br}(k) \to \prod_{v\in\Omega} \mathrm{Br}(k_v)\right).$$

Finally by the global reciprocity law, we obtain $(x_v) \in X(\mathbb{A}_k)^{\mathcal{A}}$ if and only if $(\mathcal{A}(x_v))$ lies in $\mathrm{Im}\left(\mathrm{Br}(k) \to \prod_{v\in\Omega} \mathrm{Br}(k_v)\right)$. It follows that $X(\mathbb{A}_k)^f = X(\mathbb{A}_k)^{\mathcal{A}}$. Since $\mathrm{Br}_{\mathrm{Az}}(X)$ is the union of the images of $H^1(X,\mathrm{PGL}_n)$ in $\mathrm{Br}(X)$ for $n \geq 1$, we conclude

$$X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{Az}}(X)} = \bigcap_{\mathcal{A}\in\mathrm{Br}_{\mathrm{Az}}(X)} X(\mathbb{A}_k)^{\mathcal{A}} = \bigcap_{f\in\mathbb{PGL}} (X(\mathbb{A}_k))^f$$

as required. ☐

Part II

Recent Results on Rational Points

Introduction

In 1982, Colliot-Thélène, Sansuc and Swinnerton-Dyer took up the fibration method which Hasse used to establish the Hasse principle for quadratic forms in four variables. The fibration method is to use analogue of the following theorem to study whether X satisfies weak approximation and the Hasse principle.

Theorem. Let $\pi : X \to B$ be a projective flat surjective morphism of k-varieties with X smooth over k. Suppose
(1) B is projective and satisfies weak approximation,
(2) all but finitely many k-fibres of π satisfies the weak approximation, and
(3) all fibres of π are geometrically integral.
Then X satisfies weak approximation.

In the first chapter of this part, we are interested in conic bundle surfaces over number fields. Here a conic bundle surface over a number field k is a projective non-singular surface X which is endowed with a dominant k-morphism $\pi : X \to \mathbb{P}^1_k$ such that all fibres of π are conics. The work before this paper has been restricted to the case in which the number r of degenerated geometric fibres is small. In our situation each fibre is given by a conic, so a degenerate fibre is just a union of two conjugated lines. For example, for $0 \leq r \leq 3$, the Hasse principle holds and furthermore, X is k-rational as soon as $X(k) \neq \emptyset$. For $r = 4$, we know that X is either a Châtelet surface or a quadric del Pezzo surface with a conic bundle surface structure. For $r = 5$, X is k-isomorphic to a smooth cubic surface containing a line defined over k. In particular $X(k)$ is non-empty. We introduce the work of T.D. Browning, L. Matthiesen and A.N. Skorobogatov which deals unconditionally with conic bundle surfaces over $\mathbb{Q}$ with all the degenerate fibres are all defined over $\mathbb{Q}$. The main result is the following

Theorem. Let $X|\mathbb{P}^1_{\mathbb{Q}}$ be a conic bundle surface over $\mathbb{Q}$ in which degenerate fibres exist and are all defined over $\mathbb{Q}$. Then the set $X(\mathbb{Q})$ is Zariski dense in X. Furthermore, the Brauer-Manin obstruction is the only obstruction to weak approximation for X.

In our situation, the intersection of the two components of a degenerate fibre is a $\mathbb{Q}$-point, therefore our conic bundle surface will always has a $\mathbb{Q}$-point. This is why we assume the degenerate fibre exists.

An important feature of the previous theorem is that it holds without requiring the number of the degenerate fibres. For example, it can be applied to the surfaces given by the equation

$$f(t)x^2 + g(t)y^2 + h(t)z^2 = 0,$$

where t is a coordinate function on $\mathbb{A}^1_{\mathbb{Q}}$, $[x : y : z]$ are homogeneous coordinates in $\mathbb{P}^2_{\mathbb{Q}}$ and f, g, h are products of linear polynomials with rational coefficients. We will also use the previous theorem to construct families of minimal del Pezzo surfaces X of degree 1 and 2 over $\mathbb{Q}$ for which the set $X(\mathbb{Q})$ is non-empty and dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$.

In section 1 we establish a technical result based only on recent work by L. Matthiesen and then we use it to prove the main result in section 2. We prove the Brauer-Manin obstruction is the only one to the Hasse principle and weak approximation for products of conic bundle surfaces under certain conditions in section 3. Section 4 gives analogues to higher-dimensional quadrics and section 5 is about higher dimensional varieties. In section 6 we apply these results to study del Pezzo surfaces in degree 1 and 2.

For the second chapter of this part, we are interested in norm forms $N_{K|k}(\boldsymbol{x}) = P(t)$ where $K|k$ is a finite field extension and $P(t)$ is a polynomial in one variable. Suppose X is a smooth projective k-variety which is k-birational to the affine variety $N_{K|k}(\boldsymbol{x}) = P(t)$. Then we can ask typical questions like whether $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ implies $X(k) \neq \emptyset$. We can successfully answer these questions due to the results in [26] by Y. Harpaz, A.N. Skorobogatov and O. Wittenberg. Historically, Shinzel's hypothesis is used to prove that the Brauer-Manin obstruction controls the Hasse principle and weak approximation on pencils of conics and similar varieties. We are lucky that the finite complexity case of the generalised Hardy-Littlewood conjecture was proved by Green and Tao ([20], [21]) and Green-Tao-Ziegler ([22]). We can use their results to establish Schinzel's Hypothesis over $\mathbb{Q}$ and then prove the following

Theorem. Let X be a geometrically integral variety over $\mathbb{Q}$ with a smooth and surjective morphism $\pi : X \to \mathbb{P}^1$ such that

(1) each fibre of π contains a geometrically integral irreducible component except finitely many $\mathbb{Q}$-fibres $X_1, \ldots, X_r$,

(2) for all i, the fibre X_i contains an irreducible component such that the algebraic closure of $\mathbb{Q}$ in its function field is an abelian extension of $\mathbb{Q}$.

Then $\mathbb{P}^1(\mathbb{Q}) \cap \pi(X(\mathbb{A}_{\mathbb{Q}}))$ is dense in $\pi(X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}) \subset \mathbb{P}^1(\mathbb{A}_{\mathbb{Q}}) = \prod_v \mathbb{P}^1(\mathbb{Q}_v)$.

In fact, a more powerful theorem which allows us to get rid of the assumption on being abelian field extensions was established by Y. Harpaz and O. Wittenberg in 2016 (see [27]). We make the assumption (2) here because we would like to write each abelian extension as a composite of cyclic extensions and then compute explicitly with the corresponding cyclic algebras.

We will illustrate how this theorem helps to study Severi-Brauer varieties and norm forms. In section 1 we introduce how recent results help to establish Shinzel's hypothesis. We prove the main results in section 2. We apply these results to norm form and products of norm forms in section 3.

Chapter 4

Pencils of conics and quadrics with degenerate fibres

In this chapter, we study the paper [3] by T.D. Browning, L. Matthiesen and A.N. Skorobogatov. Sometimes a fibration in algebraic curves is a smooth surface X and a proper surjective morphism $X \to C$ to a smooth curve C with connected fibres. In this case X is sometimes said to be a pencil of curves. We study similar situations in this chapter.

4.1 Rational points on a certain class of varieties

We establish the following result in this section.

Theorem 4.1.1. *Let $a_1, \ldots, a_r \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$ and let $f_1, \ldots, f_r \in \mathbb{Q}[u_1, \ldots, u_s]$ be a system of pairwise non-proportional homogeneous linear polynomials with $s \geq 2$. We consider the smooth variety $\mathscr{V} \subset \mathbb{A}^{2r+s}_{\mathbb{Q}}$ over $\mathbb{Q}$ defined by*

$$0 \neq x_i^2 - a_i y_i^2 = f_i(u_1, \ldots, u_s)$$

for $i = 1, \ldots, r$. Then $\mathscr{V}(\mathbb{Q})$ is Zariski dense in $\mathscr{V}$ as soon as $\mathscr{V}(\mathbb{Q})$ is non-empty. Furthermore, $\mathscr{V}$ satisfies the Hasse principle and weak approximation.

Proof. Before proving the theorem, we briefly introduce the idea as follows. Suppose we have shown $\mathscr{V}$ satisfies the Hasse principle and weak approximation. Then the Zariski density of $\mathscr{V}(\mathbb{Q})$ follows from weak approximation by (2.3.6) when $\mathscr{V}(\mathbb{Q}) \neq \emptyset$. So all we need to do is to show the second assertion. More precisely, we assume that the variety $\mathscr{V}$ defined by the equations

$$0 \neq x_i^2 - a_i y_i^2 = f_i(u_1, \ldots, u_s)$$

is everywhere locally soluble, i.e. $\mathscr{V}(\mathbb{Q}_v) \neq \emptyset$ for all $v \in \Omega$. Here Ω denotes the set of all places of $\mathbb{Q}$. Then we show that $\mathscr{V}(\mathbb{Q})$ is non-empty and that $\mathscr{V}$ satisfies weak approximation under this hypothesis. Since conics defined by a single equation with $\mathbb{Q}$-points satisfy weak approximation, it will be sufficient to place weak approximation conditions on the variables $\boldsymbol{u} = (u_1, \ldots, u_s)$ in $\mathscr{V}$ alone.

Step 1. Reduce to counting integral points under certain conditions.

We can find a suitable positive integer d such that $d^2 a_i \in \mathbb{Z}$ and $d^2 f_i \in \mathbb{Z}[u_1, \ldots, u_s]$ for each $i = 1, \ldots, r$. Since the variety defined by

$$0 \neq (dx_i)^2 - (d^2 a_i) y_i^2 = d^2 f_i(u_1, \ldots, u_s)$$

in $\mathbb{A}^{2r+s}_{\mathbb{Q}}$ is just our variety $\mathscr{V}$, we can assume without loss of generality that

$$a_1, \ldots, a_r \in \mathbb{Z} \text{ and } f_1, \ldots, f_r \in \mathbb{Z}[u_1, \ldots, u_s].$$

Let $|-|_p$ denote the p-adic norm for each finite place $p \in \Omega$, and let $|-|$ denote the norm for the real place. Let $S \subset \Omega$ be any finite set which we need to approximate. Let $\varepsilon > 0$ be a sufficiently small positive constant. Let $(\mathbf{x}^{(v)}, \mathbf{y}^{(v)}, \mathbf{u}^{(v)}) \in \mathscr{V}(\mathbb{Q}_v)$ for each $v \in \Omega$ be the given point we need to approximate. Our task is to find a rational point $(\mathbf{x}, \mathbf{y}, \mathbf{u}) \in \mathscr{V}(\mathbb{Q})$ such that

$$|\mathbf{u} - \mathbf{u}^{(v)}|_v < \varepsilon$$

for each $v \in S$.

We can enlarge S such that S contains the real place and all finite places p bounded by L for some parameter L to be determined later. Since scaling by an integer $a \in \mathbb{Z}_{>0}$ on the ring homomorphism $\mathbb{Q}_p[\mathbf{X}, \mathbf{Y}, \mathbf{U}] \to \mathbb{Q}_p$ does not change the associated morphism of schemes $\operatorname{Spec} \mathbb{Q}_p \to \operatorname{Spec} \mathbb{Q}_p[\mathbf{X}, \mathbf{Y}, \mathbf{U}]$, we can assume $(\mathbf{x}^{(p)}, \mathbf{y}^{(p)}, \mathbf{u}^{(p)}) \in \mathbb{Z}_p^{2r+s}$ for each finite place $p \in S$. Applying the Chinese remainder theorem for $\mathbb{Z}^{2r+s}$, then we can find $(\mathbf{x}^{(M)}, \mathbf{y}^{(M)}, \mathbf{u}^{(M)}) \in \mathbb{Z}^{2r+s}$ such that

$$|\mathbf{x}^{(M)} - \mathbf{x}^{(p)}|_p < \varepsilon, \quad |\mathbf{y}^{(M)} - \mathbf{y}^{(p)}|_p < \varepsilon, \quad |\mathbf{u}^{(M)} - \mathbf{u}^{(p)}|_p < \varepsilon$$

for each finite place $p \in S$. We replace $|\mathbf{u} - \mathbf{u}^{(p)}|_p < \varepsilon$ by the sufficient condition that $\mathbf{u} \in \mathbb{Z}^s$ and

$$u_j \equiv u_j^{(M)} \pmod{M} \tag{4.1}$$

for $j = 1, \ldots, s$ and for an appropriate modulus $M \in \mathbb{Z}_{>0}$. For technical reasons we require that M has the following property. If $\ell | M$ is a prime divisor and if we write $m = \operatorname{val}_\ell(M)$, then

$$m \geq \max_{1 \leq i \leq r} \left\{ \operatorname{val}_\ell(4a_i) \right\}$$

and

$$f_i(\mathbf{u}^{(p)}) \not\equiv 0 \pmod{\ell^m}$$

for $i = 1, \ldots, r$ and all finite places $p \in S$. By assumption $f_i(\mathbf{u}^{(p)}) \neq 0$ in $\mathbb{Q}_p$, hence we can arrange for this property to hold by possibly decreasing the value of ε in $|\mathbf{u} - \mathbf{u}^{(p)}|_p < \varepsilon$.

For the real place, we will seek points in $\mathscr{V}(\mathbb{Z})$ satisfying

$$|\mathbf{u} - B\mathbf{u}^{(\infty)}| < \varepsilon B, \tag{4.2}$$

where $B = C^2$ and C is a sufficiently large positive integer verifying $C \equiv 1 \pmod{M}$. It is clear that any solution $(\mathbf{x}, \mathbf{y}, \mathbf{u}) \in \mathscr{V}(\mathbb{Z})$ satisfying (4.1) and (4.2) will give rise to a solution $(C^{-1}\mathbf{x}, C^{-1}\mathbf{y}, C^{-2}\mathbf{u}) \in \mathscr{V}(\mathbb{Q})$ satisfying $|C^{-2}\mathbf{u} - \mathbf{u}^{(p)}|_p < \varepsilon$ for each finite place $p \in S$ and $|C^{-2}\mathbf{u} - \mathbf{u}^{(\infty)}| < \varepsilon$.

Let us decompose the set of indices $\{1, \ldots, r\}$ as $I_- \bigsqcup I_+$, where $i \in I_\pm$ iff $\operatorname{sign}(a_i) = \pm$. Let $(\mathbf{x}^{(\infty)}, \mathbf{y}^{(\infty)}, \mathbf{u}^{(\infty)}) \in \mathscr{V}(\mathbb{R})$ be a solution. Then $f_i(\mathbf{u}^{(\infty)}) = (x_i^{(\infty)})^2 - a_i (y_i^{(\infty)})^2 > 0$ for $i \in I_-$. It follows that after decreasing ε if necessary, any $\mathbf{u} \in \mathbb{R}^s$ satisfying $|\mathbf{u} - C^2\mathbf{u}^{(\infty)}| < \varepsilon C^2$ will produce positive values of $f_i(\mathbf{u})$ for $i \in I_-$.

Let $q_i(x, y) = x^2 - a_i y^2$ for $i = 1, \ldots, r$. Then $q_i(x, y)$ is a primitive binary quadratic form of discriminant $4a_i$. Moreover, $q_i(x, y)$ is positive definite for $i \in I_-$ and indefinite for $i \in I_+$. For $d \leq -4$, let

$$w(d) = \begin{cases} 4 & \text{if } d = -4, \\ 2 & \text{if } d < -4, \end{cases}$$

and for $d > 0$, let $\eta(d)$ denote the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Let us call a solution $(\mathbf{x}, \mathbf{y}, \mathbf{u}) \in \mathbb{Z}^{2r+s}$ of

$$0 \neq x_i^2 - a_i y_i^2 = f_i(u_1, \ldots, u_s)$$

primary if the pair (x_i, y_i) lies in a fixed fundamental domain for the action of the group of automorphisms $\mathscr{E}_i$ of q_i for $i = 1, \ldots, r$. Our strategy will be to estimate asymptotically, when $B \to \infty$, the total number $N(B)$ of primary solutions $(\mathbf{x}, \mathbf{y}, \mathbf{u}) \in \mathbb{Z}^{2r+s}$ which satisfies (4.1) and (4.2) and to show that this quantity is positive for sufficiently large B.

We will henceforth view ε, M together with the coefficients of $\mathscr{V}$ and $\mathbf{u}^{(M)}, \mathbf{u}^{(\infty)}$ as being fixed once and for all. Given $n \in \mathbb{Z}$, we define the representation functions

$$R_i(n) = \mathrm{Card}\{(x,y) \in \mathbb{Z}^2/\mathscr{E}_i \mid q_i(x,y) = n\}$$

for $i = 1, \ldots, r$. We put $R_i(n) = 0$ if $n \leq 0$ and $i \in I_-$. Then we obtain

$$N(B) = \sum_{\substack{\mathbf{u} \in \mathbb{Z}^s \\ (4.1),(4.2) \text{ hold}}} \prod_{i=1}^{r} R_i(f_i(\mathbf{u})).$$

Step 2. The computation of $N(B)$.

We eliminate the constraint (4.1) in $N(B)$ by writing $u_j = u_j^{(M)} + Mt_j$ for $j = 1, \ldots, s$. This leads to the expression

$$N(B) = \sum_{\mathbf{t} \in \mathbb{Z}^s \cap K} \prod_{i=1}^{r} R_i(g_i(\mathbf{t})),$$

where

$$K = \{\mathbf{t} \in \mathbb{R}^s \mid |M\mathbf{t} + \mathbf{u}^{(M)} - B\mathbf{u}^{(\infty)}| < \varepsilon B\}$$

and

$$g_i(\mathbf{t}) = f_i(\mathbf{u}^{(M)} + M\mathbf{t}),$$

for $i = 1, \ldots, r$. The region K is convex and contained in $[-uB, uB]^s$ for an appropriate absolute positive constant u. K has measure $m(K) = (2\varepsilon M^{-1}B)^s \gtrsim B^s$, where $x \gtrsim y$ means that there exists a positive constant a such that $x > ay$. Our choice of ε ensures that $g_i(K)$ is positive for every $i \in I_-$. Moreover, $(g_1, \ldots, g_r) : \mathbb{Z}^s \to \mathbb{Z}^r$ defines a system of linear polynomials of finite complexity in the language of Green and Tao. Indeed, the linear parts of any two g_i, g_j with $i \neq j$, are non-proportional. Given $A \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$, let

$$\rho_i(q, A) = \mathrm{Card}\{(x,y) \in (\mathbb{Z}/q\mathbb{Z})^2 \mid x^2 - a_i y^2 \equiv A \pmod{q}\}.$$

It then follows from theorem 1.1 in [36] that

$$N(B) = \beta_\infty \prod_p \beta_p + o(B^s)$$

as $B \to \infty$. Here the main term is a product of local densities, given by

$$\beta_\infty = m(K) \prod_{i \in I_-} \frac{\pi}{\omega(4a_i)\sqrt{|a_i|}} \prod_{j \in I_+} \frac{\log \eta(a_j)}{\sqrt{a_j}}$$

and

$$\beta_p = \lim_{k \to \infty} p^{-(s+r)k} \sum_{\mathbf{t} \in (\mathbb{Z}/p^k\mathbb{Z})^s} \prod_{i=1}^{r} \rho_i(p^k, g_i(\mathbf{t}))$$

for each prime p. Since $\beta_\infty \gtrsim m(K) \gtrsim B^s$, we see that in order to complete the proof, it remains to show that $\prod_p \beta_p \gtrsim 1$.

For each prime p, let

$$\beta_p' = \lim_{k \to \infty} p^{-(s+r)k} \sum_{\mathbf{u} \in (\mathbb{Z}/p^s\mathbb{Z})^s} \prod_{i=1}^{r} \rho_i(p^k, f_i(\mathbf{u}))$$

be the local factor associated to the original system of equations. By lemma 8.3 in [35], these factors satisfy $\beta_p' = 1 + O(p^{-2})$. Since the change of variables from $f_i(\mathbf{t})$ to $g_i(\mathbf{t}) = f_i(\mathbf{u}^{(M)} + M\mathbf{t})$ is non-singular modulo p when $p \nmid M$, we conclude that $\beta_p = \beta_p'$ for $p \nmid M$. Recall that primes

$p \nmid M$ satisfy $p > L$. We may now specify the parameter $L = O(1)$ to be such that $\beta'_p > 0$ for all $p > L$. Hence for this choice of L, we have

$$\prod_{p \nmid M} \beta_p = \prod_{p \nmid M} \beta'_p \gtrsim 1.$$

Our final task is to show that $\beta_p > 0$ for primes $p|M$. It will be convenient to write

$$\begin{aligned} G(p^k) &= \sum_{\mathbf{t} \in (\mathbb{Z}/p^k\mathbb{Z})^s} \prod_{i=1}^{r} \rho_i(p^k, g_i(\mathbf{t})) \\ &= \mathrm{Card}\{(\mathbf{x}, \mathbf{y}, \mathbf{u}) \in (\mathbb{Z}/p^k\mathbb{Z})^{2r+s} \mid x_i^2 - a_i y^2 \equiv g_i(\mathbf{t}) \pmod{p^k},\ i = 1, \dots, r\}, \end{aligned}$$

so that

$$\beta_p = \lim_{k \to \infty} p^{-(s+r)k} G(p^k).$$

Suppose $\mathrm{val}_p(M) = m > 0$. To start with, observe that the integer vector $(\mathbf{x}^{(M)}, \mathbf{y}^{(M)}, \mathbf{z}^{(M)})$ satisfies

$$0 \neq x_i^2 - a_i y_i^2 = f_i(u_1, \dots, u_s)$$

modulo M. This implies $G(p^m) \geq p^{sm}$ since $g_i(\mathbf{t}) = f_i(\mathbf{u} + M\mathbf{t})$. To analyse $G(p^k)$ for $k > m$, we shall employ corollary 6.4 in [35]. This yields

$$\rho_i(p^k, A) = \frac{1}{p} \rho_i(p^{k+1}, A + \ell p^k)$$

for any $\ell \in \mathbb{Z}/p\mathbb{Z}$, providing that $k \geq \mathrm{val}_p(4a_i)$ and $A \not\equiv 0 \pmod{p^k}$. We have arranged things so that M satisfies

$$m \geq \max_{1 \leq i \leq r} \left\{ \mathrm{val}_p(4a_i) \right\} \quad \text{and} \quad f_i(\mathbf{u}^{(v)}) \not\equiv 0 \pmod{p^m}.$$

Thus the conditions hold for $k > m$ when $A = g_i(\mathbf{t})$ and $\mathbf{t} \in \mathbb{Z}^s$, and we deduce that $G(p^{k+1}) = p^{s+r} G(p^k)$. Hence

$$\beta_p = p^{-(s+r)m} G(p^m) \geq p^{-rm} > 0$$

for $p|M$. Finally, $N(B) = \beta_\infty \prod_p \beta_p + o(B^s) \gtrsim m(K) \gtrsim B^s$ implies that $N(B) > 1$ when B is sufficiently large. This completes the proof. □

4.2 Rational points on conic bundle surfaces

Definition 4.2.1. Let k be a number field. Let X be a projective non-singular surface over k. X is called a **conic bundle surface** if there is a dominant k-morphism $X \to \mathbb{P}^1_k$ such that all fibres are conics.

Colliot-Thélène and Sansuc conjectured in 1979 that the Brauer-Manin obstruction is the only obstruction to the Hasse principle and weak approximation for conic bundle surfaces. It is worth noting that the analogue for 0-cycles of degree 1 is known due to Colliot-Thélène and Swinnerton-Dyer (see [14]). We want to study unconditional resolutions of the conjecture.

Remark 4.2.1. It is convenient to assume without loss of generality that the conic bundle $\pi : X \to \mathbb{P}^1_k$ is **relatively minimal**, which means that no irreducible component of a degenerate fibre is defined over the field of definition of that fibre. More explicitly, suppose the fibre X_P above $P \in \mathbb{P}^1_k$ is degenerate and is defined over k. Hence topologically, X_P is a union of two conjugated lines, say U_P and V_P. Then the relative minimality says that U_P and V_P are defined over $k(\sqrt{a_P})$ for some $a_P \in k^\times - (k^\times)^2$.

We establish the following result by applying (4.1.1) in this section.

Theorem 4.2.2. *Let $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a conic bundle surface over $\mathbb{Q}$. Suppose the degenerate fibres of π exist and all these degenerate fibres are defined over $\mathbb{Q}$. Then the set of $\mathbb{Q}$-points $X(\mathbb{Q})$ is Zariski dense in X. Furthermore, the Brauer-Manin obstruction is the only obstruction to weak approximation for X.*

Proof. We assume without loss of generality that $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ is relatively minimal and by a change of variables in $\mathbb{P}^1_{\mathbb{Q}}$, we may assume that the fibre of π at infinity is smooth. Let $P(t) \in \mathbb{Q}[t]$ be the separable monic polynomial of degree r that vanishes at the points of $\mathbb{A}^1_{\mathbb{Q}} = \mathbb{P}^1_{\mathbb{Q}} - \{\infty\}$ that produce degenerate fibres. Our hypotheses are therefore equivalent to a factorisation $P(t) = (t - e_1) \dots (t - e_r)$ with $e_1, \dots, e_r \in \mathbb{Q} = \mathbb{A}^1_{\mathbb{Q}}(\mathbb{Q})$ pairwise distinct, and $a_1, \dots, a_r \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$ such that each irreducible component of the fibre X_{e_i} is defined over $\mathbb{Q}(\sqrt{a_i})$ for $i = 1, \dots, r$.

The elements of the cohomological Brauer group $\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m)$ have the following explicit description. Since $X(\mathbb{Q}) \neq \emptyset$, we obtain a section of the structural morphism $X \to \operatorname{Spec} \mathbb{Q}$ and hence the natural map $\mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(X)$ is injective. We put

$$\delta : (\mathbb{Z}/2\mathbb{Z})^r \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

to be the map that sends $(n_1, \dots, n_r) \in (\mathbb{Z}/2\mathbb{Z})^r$ to the class of $a_1^{n_1} \cdots a_r^{n_r}$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. By the Faddeev reciprocity law we have $a_1 \cdots a_r \in (\mathbb{Q}^\times)^2$, hence $(1, \dots, 1) \in \mathrm{Ker}(\delta)$ by construction of δ. For $i = 1, \dots, r$, the quaternion algebras $(a_i, t - e_i)$ form classes in $\mathrm{Br}(\mathbb{Q}(t))$. An integral linear combination $\sum_{i=1}^r n_i(a_i, t - e_i)$ gives rise to an element of $\mathrm{Br}(X)$ iff $(n_1, \dots, n_r) \in \mathrm{Ker}(\delta)$. Therefore we obtain a well-defined homomorphism

$$\eta : \mathrm{Ker}(\delta) \to \mathrm{Br}(X)/\,\mathrm{Br}(\mathbb{Q})$$

which sends $(n_1, \dots, n_r)$ to the class of $\sum_{i=1}^r n_i(a_i, t - e_i)$ in $\mathrm{Br}(X)/\,\mathrm{Br}(\mathbb{Q})$. By proposition 7.1.2 in [47], η is surjective with the kernel generated by $(1, \dots, 1)$. Hence we have

$$\mathrm{Br}(X)/\,\mathrm{Br}(\mathbb{Q}) \simeq \mathrm{Ker}(\delta)/\,\mathrm{Ker}(\eta),$$

and $\mathrm{Ker}(\delta)$ is generated by $(1, \dots, 1)$ iff $\mathrm{Br}(X) = \mathrm{Br}(\mathbb{Q})$.

To show the Brauer-Manin obstruction is the only one to weak approximation for X, we have to show that $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(X)}$ under the product topology. Here $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(X)}$ denotes the right kernel in the Brauer-Manin pairing $\mathrm{Br}(X) \times X(\mathbb{A}_{\mathbb{Q}}) \to \mathbb{Z}/2\mathbb{Z}$. Recall that the pairing is additive in the first variable, it follows that the image of paring lies in $\mathbb{Z}/2\mathbb{Z}$ by $\mathrm{Br}(X)/\,\mathrm{Br}(\mathbb{Q}) \simeq \mathrm{Ker}(\delta)/\,\mathrm{Ker}(\eta)$.

According to work of Colliot-Thélène and Sansuc (theorem 2.6.4(iii) in [9]), any universal torsor $\mathscr{T}$ over X is $\mathbb{Q}$-birationally equivalent to $W_{\boldsymbol{\lambda}} \times C \times \mathbb{A}^1_{\mathbb{Q}}$, where C is a conic over $\mathbb{Q}$ and $W_{\boldsymbol{\lambda}} \subset \mathbb{A}^{2r+2}_{\mathbb{Q}}$ is the variety defined by

$$u - e_i v = \lambda_i(x_i^2 - a_i y_i^2)$$

with $i = 1, \dots, r$ for suitable $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_r) \in (\mathbb{Q}^\times)^r$. An application of (4.1.1) in the special case $s = 2$ shows that all universal torsors $\mathscr{T}$ over X satisfy the Hasse principle and weak approximation. Since $X(\mathbb{Q}) \neq \emptyset$, it follows from the descent theory of Colliot-Thélène and Sancuc (see [9], theorem 3.5.1 and proposition 3.8.7) that $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(X)}$ under the product topology, as required for the second part of the assertion.

This implies that there is a finite set S of places of $\mathbb{Q}$ such that weak approximation holds away from S. In particular, for almost all primes p, the set $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$ under the p-adic topology. This shows that the first part of the assertion follows from the second part. □

Remark 4.2.3. If π does not have degenerate fibres, then we can use the fibration method mentioned in the introduction to conclude. So we assume the degenerate fibres exist and are all defined over $\mathbb{Q}$. In this case, the intersection of the two components of a degenerate fibre is therefore a $\mathbb{Q}$-point.

4.3 Smooth proper models of product of conic bundle surfaces

Let Y be a variety over a number field k, and let $f : Z \to Y$ be a torsor under a k-torus T. We write $\mathbb{A}_k$ for the ring of adèles of k. Specialising the torsor at an adelic point defines the evaluation map

$$Y(\mathbb{A}_k) \to \prod_v H^1(k_v, T)$$

where the product is taken over all completions k_v of k. Let $Y(\mathbb{A}_k)^f$ be the set of adelic points for which the image of the evaluation map is contained in the image of the natural map $H^1(k, T) \to \prod_v H^1(k_v, T)$. It is clear that the diagonal image of $Y(k)$ in $Y(\mathbb{A}_k)$ is in $Y(\mathbb{A}_k)^f$.

There is an equivalent way to define $Y(\mathbb{A}_k)^f$. Up to isomorphism, the k-torsors R of T are classified by their classes $[R] \in H^1(k, T)$. The twist of $f : Z \to Y$ by R is defined as the quotient of $Z \times R$ by the diagonal action of T, with the morphism to Y induced by the first projection. We denote the twisted torsor by $f^R : Z^R \to Y$. Then $Y(\mathbb{A}_k)^f$ is the union of the images of projections $f^R : Z^R(\mathbb{A}_k) \to Y(\mathbb{A}_k)$ for all $[R] \in H^1(k, T)$.

Proposition 4.3.1. *Let X be a smooth geometrically integral variety over a number field k. Let $Y \subset X$ be a dense open set, and let $f : Z \to Y$ be a torsor of a k-torus T. Then $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ implies $Y(\mathbb{A}_k)^f \neq \emptyset$.*

If X is proper, then $X(\mathbb{A}_k)^{\mathrm{Br}}$ is contained in the closure of $Y(\mathbb{A}_k)^f$ in $X(\mathbb{A}_k) = \prod_v X(k_v)$. In this case, if all the twists of Z by k-torsors of T satisfy the Hasse principle and weak approximation, then $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$.

Proof. Let $\hat{T}$ be the group of homomorphisms $T \times_k \overline{k} \to \mathbb{G}_{m,\overline{k}}$ of algebraic groups. Equipped with the discrete topology, $\hat{T}$ is a continuous $\mathrm{Gal}(\overline{k}|k)$-module. The natural pairing of discrete $\mathrm{Gal}(\overline{k}|k)$-modules $T(\overline{k}) \times \hat{T} \to \overline{k}^\times$ gives rise to the cup product pairing

$$\cup : H^1_{\text{ét}}(Y, T) \times H^1(k, \hat{T}) \to H^1_{\text{ét}}(Y, T) \times H^1_{\text{ét}}(Y, \hat{T}) \to H^2_{\text{ét}}(Y, \mathbb{G}_m) = \mathrm{Br}(Y).$$

([47], page 63-64) Let $[Z] \in H^1_{\text{ét}}(Y, T)$ be the class of the torsor Z/Y, and let $B \subset \mathrm{Br}(Y)$ be the subgroup $[Z] \cup H^1(k, \hat{T})$. Since $H^1(k, \hat{T})$ is finite, B is also finite. Let $Y(\mathbb{A}_k)^B$ be the set of adelic points of Y that are orthogonal to B with respect to the Brauer-Manin paring. By (2.4.12) we have $X(\mathbb{A}_k)^{B\cap \mathrm{Br}(X)} \neq \emptyset$ iff $Y(\mathbb{A}_k)^B \neq \emptyset$, and the latter set is dense in the former when X is proper. Since $X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)^{B\cap \mathrm{Br}(X)}$, it remains to prove that $Y(\mathbb{A}_k)^B = Y(\mathbb{A}_k)^f$. This is a well-known consequence of the Poitou-Tate duality for tori; see the proof of statement (2) in [47], page 115, 119-121. $\square$

We can use the above proposition to prove the following:

Theorem 4.3.2. *Let $\pi_j : X_j \to \mathbb{P}^1_{\mathbb{Q}}$ be conic bundle surfaces over $\mathbb{Q}$ for $j = 1, \dots, n$. Suppose the degenerate fibres of these π_j are all defined over $\mathbb{Q}$. Let*

$$X = X_1 \times_{\mathbb{P}^1} X_2 \times_{\mathbb{P}^1} \times \cdots \times_{\mathbb{P}^1} X_n$$

be the fibred product. Assume that whenever two or more of these conic bundles have degenerate fibers over the same point of $\mathbb{P}^1_{\mathbb{Q}}$, the irreducible components of their fibres at this point are defined over the same quadratic field. Then the Brauer-Manin obstruction is the only obstruction to the Hasse principle and weak approximation on any smooth and proper $\mathbb{Q}$-varieties that are birational to X.

Proof. Step 1. We construct a dense open subset $Y \subset X$.

Without loss of generality, we assume that $X_j \to \mathbb{P}^1$ is relatively minimal and the fibre at infinity of $X_j \to \mathbb{P}^1$ is smooth for each $j = 1, \dots, n$. Then there are $e_1, \dots, e_r$ in $\mathbb{Q} = \mathbb{A}^1(\mathbb{Q})$ such that the restriction of $X_j \to \mathbb{P}^1$ to $\mathbb{P}^1 - \{e_1, \dots, e_r\}$ is a smooth morphism for each j. By assumption, for $i = 1, \dots, r$ there exists $a_i \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$ defined up to a square, such that the fibre of each $X_j \to \mathbb{P}^1$ at e_i is either a smooth conic or a union of two conjugate lines defined over $\mathbb{Q}(\sqrt{a_i})$.

Let $U = \mathbb{A}^1 - \{e_1, \dots, e_r\}$. For $j = 1, \dots, n$, we take $Y_j = \pi_j^{-1}(U) \subset X_j$ as the inverse image of $U \subset \mathbb{P}^1$. Let Y be the fibred product $Y_1 \times_U \cdots \times_U Y_n$ over U. Then Y is a dense open subset of X.

Step 2. We construct a Y-torsor under a $\mathbb{Q}$-torus T.

Let $\mathscr{W}_{\boldsymbol{\lambda}} \subset \mathbb{A}_{\mathbb{Q}}^{2r+2}$ for $\boldsymbol{\lambda} \in (\mathbb{Q}^\times)^r$, be the variety given by

$$v\prod_{i=1}^{r}(u - e_i v) \neq 0 \quad \text{and} \quad u - e_i v = \lambda_i(x_i^2 - a_i y_i^2),\ i = 1, \dots, r. \tag{4.3}$$

The morphism $\mathscr{W}_{\boldsymbol{\lambda}} \to U$ that sends the point (u, v, x_i, y_i) to the point with the coordinate $t = u/v$ is a torsor of the following $\mathbb{Q}$-torus T:

$$v = x_1^2 - a_1 y_1^2 = \cdots = x_r^2 - a_r y_r^2 \neq 0.$$

The fibred product $Y \times_U \mathscr{W}_{\boldsymbol{\lambda}}$ is a Y-torsor of T for any $\boldsymbol{\lambda}$.

Step 3. We classify the $\mathbb{Q}$-torsors under T and compute the twists of the above Y-torsor by these $\mathbb{Q}$-torsors.

The $\mathbb{Q}$-torsors of T are the affine varieties $R_{\mathbf{c}}$ given by

$$v = c_1(x_1^2 - a_1 y_1^2) = \cdots = c_r(x_r^2 - a_r y_r^2) \neq 0,$$

where $\mathbf{c} = (c_1, \dots, c_r) \in (\mathbb{Q}^\times)^r$. The isomorphism classes of $\mathbb{Q}$-torsors of T bijectively correspond to $\mathbf{c} \in (\mathbb{Q}^\times)^r$ up to a common non-zero rational multiple and multiplication of each c_i by the norm of a non-zero element of $\mathbb{Q}(\sqrt{a_i})$. The twist $\mathscr{W}_{\boldsymbol{\lambda}}^{R_{\mathbf{c}}}$ is the torsor $\mathscr{W}_{\mathbf{c}\boldsymbol{\lambda}}$, where $\boldsymbol{c\lambda} = (c_1\lambda_1, \dots, c_r\lambda_r)$. Thus the set of torsors $Y \times_U \mathscr{W}_{\boldsymbol{\lambda}} \to Y$ for all $\boldsymbol{\lambda} \in (\mathbb{Q}^\times)^r$ is closed under all twists by $\mathbb{Q}$-torsors of T.

Step 4. We check the Hasse principle and weak approximation hold for these twisted varieties and then we conclude the assertion.

For $j = 1, \dots, n$, we denote by

$$I_j = \big\{1 \le i \le n \bigm| \text{the fibre of } \pi_j : X_j \to \mathbb{P}^1 \text{ at } e_i \text{ is singular}\big\},$$

and let $r_j = |I_j|$ be the cardinality of I_j. We define $\mathscr{W}_{\boldsymbol{\lambda}}^{(j)} \subset \mathbb{A}_{\mathbb{Q}}^{2r_j+2}$ to be the variety given by

$$v\prod_{i=1}^{r}(u - e_i v) \neq 0 \quad \text{and} \quad u - e_i v = \lambda_i(x_i^2 - a_i y_i^2),\ i \in I_j$$

for $\boldsymbol{\lambda} \in (\mathbb{Q}^\times)^{r_j}$. As proved in [9] (theorem 2.6.4(ii)(a) and remark 2.6.8), there exist a conic C_j over $\mathbb{Q}$ such that $Y_j \times_U \mathscr{W}_{\boldsymbol{\lambda}}^{(j)}$ is birationally equivalent to $C_j \times \mathscr{W}_{\boldsymbol{\lambda}}^{(j)}$ for each j. There is a natural morphism $\mathscr{W}_{\boldsymbol{\lambda}} \to \mathscr{W}_{\boldsymbol{\lambda}}^{(j)}$ that forgets the coordinates x_i, y_i for $i \notin I_j$. This morphism is obviously compatible with the projection to U, hence $Y_j \times_U \mathscr{W}_{\boldsymbol{\lambda}}$ is birationally equivalent to $C_j \times \mathscr{W}_{\boldsymbol{\lambda}}$. Therefore $Y \times_U \mathscr{W}_{\boldsymbol{\lambda}}$ is birationally equivalent to $C_1 \times \cdots \times C_n \times \mathscr{W}_{\boldsymbol{\lambda}}$. By (4.1.1) and the Hasse-Minkowski theorem (4.3.5) this variety satisfies the Hasse principle and weak approximation. It now follows from (4.3.1) that $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$. $\square$

Remark 4.3.3. A quadratic form $Q = Q(x_1, \dots, x_n)$ over k is a homogeneous polynomial of degree 2 with coefficients in k. Therefore we can write $Q = \sum_{i=1}^{n} a_{ij} x_i x_j$ with $a_{ij} = a_{ji} \in k$.

Theorem 4.3.4 (Hasse-Minkowski). *A quadratic form Q with rational coefficients has a zero in $\mathbb{Q}$ if and only if Q has a zero in $\mathbb{Q}_v$ for each $v \in \Omega$, where Ω is the set of all places of $\mathbb{Q}$.*

The following theorem is a variant in the language of algebraic geometry.

Theorem 4.3.5 (Hasse-Minkowski). *Let X be a smooth projective quadric of dimension at least 1 over a number field k. Then X satisfies the Hasse principle.*

4.4 Generalisation to higher-dimensional quadrics

Now we turn to the arithmetic of pencils of 2-dimensional quadratics. We start with the relevant definition from [45]. Let k be a field of characteristic different from 2.

Definition 4.4.1. A quadric over k is a hypersurface of degree 2 in $\mathbb{P}^n_k$ for some $n \geq 2$.

(1) A geometrically integral variety X over k endowed with a morphism $\pi : X \to \mathbb{P}^1_k$ is a **quadric bundle** if every closed point $P \in \mathbb{P}^1_k$ has a Zariski open neighbourhood $U_P \subset \mathbb{P}^1_k$ such that $\pi^{-1}(U_P)$ is the closed subset of $U_P \times \mathbb{P}^3_k$ defined by the vanishing of a quadratic form $Q_P(x_1, x_2, x_3, x_4) = 0$ with coefficients in the k-algebra of regular functions on U_P such that $\det(Q_P)$ is not identically zero.

(2) A quadric bundle X over $\mathbb{P}^1_k$ is **admissible** if for every closed point $P \in \mathbb{P}^1_k$ for which the fibre X_P is singular, U_P and $Q_P(x_1, x_2, x_3, x_4)$ in (1) can be chosen so that

$$Q_P(x_1, x_2, x_3, x_4) = \sum_{i=1}^{4} f_i x_i^2$$

where each f_i is invertible outside P with at most a simple zero at P and $f_1(P)f_2(P) \neq 0$.

(3) An admissible quadric bundle is **relatively minimal** if in the notation of (2), for each closed point $P \in \mathbb{P}^1_k$ such that $f_3(P) = f_4(P) = 0$, the (well-defined) values of the functions $-f_1/f_2$ and $-f_3/f_4$ at P are both non-squares in the residue field $k(P)$.

If $\pi : X \to \mathbb{P}^1_k$ is a relatively minimal admissible quadric bundle, then the closed fibre X_P is not geometrically integral iff X_P is the zero set of a quadric form of rank 2. In our notation, X_P is given by $f_1(P)x_1^2 + f_2(P)x_2^2 = 0$. Thus X_P is the union of two conjugate projective planes defined over the quadratic extension $k(P)(\sqrt{a_P})$ of the residue field $k(P)$, where $a_P = -f_1(P)/f_2(P)$. In particular, the (non-trivial) class of a_P in $k(P)^\times/(k(P)^\times)^2$ is uniquely determined by the morphism $\pi : X \to \mathbb{P}^1_k$.

The singular locus $(X_P)_{\mathrm{Sing}}$ of X_P is the projective line given by $x_1 = x_2 = 0$. An easy calculation (see [45], corollary 2.1) shows that the singular locus X_{Sing} is contained in the union of singular loci of the closed fibres of $X \to \mathbb{P}^1_k$ that are not geometrically integral. Let $b_P \in k(P)^\times$ be the value of $-f_3/f_4$ at P. By proposition 2.2 in [45], we conclude $X_{\mathrm{Sing}} \cap X_P$ is the subscheme of $(X_P)_{\mathrm{Sing}}$ given by $x_4^2 = b_P x_3^2$. In particular, the non-trivial class of b_P in $k(P)^\times/(k(P)^\times)^2$ is uniquely determined by the morphism $\pi : X \to \mathbb{P}^1_k$.

Recall that a scheme over k is called **split** if it contains a non-empty geometrically integral open subscheme ([46], definition 0.1, page 906). Let us denote by $\tilde{X}$ the blow-up of X_{Sing} in X. By proposition 2.4 in [45], $\tilde{X}$ is a smooth projective threefold. Since $X \to \mathbb{P}^1_k$ is relatively minimal, each fibre of $\tilde{X} \to \mathbb{P}^1_k$ that is not geometrically integral consists of two irreducible components, none of them is geometrically integral since a_P and b_P are both non-square in $k(P)^\times$ (see remark 2.2 in [45]). Hence a fibre of $\tilde{X} \to \mathbb{P}^1_k$ is split iff it is geometrically integral.

Let $a_i \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$ and $c_i \in \mathbb{Q}^\times$ for $i = 1, \ldots, n$. Given pairwise distinct rational numbers $e_1, \ldots, e_{2n}$, (4.3.2) can be applied to the intersection of quadrics

$$(u - e_{2i-1}v)(u - e_{2i}v) = c_i(x_i^2 - a_i y_i^2)$$

for $i = 1, \ldots, n$ in $\mathbb{P}^{2n+1}_{\mathbb{Q}}$. Indeed, no two of the conic bundles in the fibred product have degenerate fibres over the same point of $\mathbb{P}^1_{\mathbb{Q}}$. The funny fact is that for such varieties counter-examples to the Hasse principle and weak approximation are known (see §7 in [6]). Theorem (4.3.2) tells us that all such counter-examples are explained by the Brauer-Manin obstruction. This was previously known only when $n = 2$, by using a descent argument to reduce the problem to an intersection of two quadrics in $\mathbb{P}^6_{\mathbb{Q}}$ covered by theorem 6.7 in [11].

Now we generalise theorem (4.2.2) to families of higher-dimensional (at least 3) quadrics. Before we start, we recall the following result.

Proposition 4.4.1. *Let Y be a smooth and geometrically integral variety over a number field k. Suppose $Y(k) \neq \emptyset$ and Y satisfies weak approximation. Let Z be a smooth scheme over Y with surjective structural morphism such that each fibre is a quadric of dimension at least 3. Let X over k be any smooth and geometrically integral variety which is k-birational to Z. Then the Hasse principle and weak approximation hold for Z and X.*

Proof. See proposition 3.9 in [11]. □

Remark 4.4.2. Let k be a number field and let Y be a non-empty open subset of an affine space $\mathbb{A}^n_k$ over k. Then $Y(k) \neq \emptyset$ and Y satisfies weak approximation because Y is k-birational to $\mathbb{A}^n_k$. Let Z be any variety with a surjective morphism to Y such that the fibres are smooth projective quadrics of dimension at least 3. Then by (4.4.1), Z satisfies the Hasse principle and weak approximation.

Thus we focus on the case of a variety with a surjective morphism to $\mathbb{P}^1_{\mathbb{Q}}$ such that the fibres are 2-dimensional quadrics. Progress so far has been restricted to the case in which there are at most three geometric fibres that are quadrics of rank 2 or less, as in [12] and [45].

Theorem 4.4.3. *Let X be a smooth, proper and geometrically integral variety of dimension 3 over $\mathbb{Q}$ equipped with a surjective morphism $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ such that the generic fibre is a 2-dimensional quadric. If all the fibres that are not geometrically integral are defined over $\mathbb{Q}$, then the set $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(X)}$.*

Proof. Step 1. Reduce to a $\mathbb{Q}$-birationally equivalent variety X' which is relatively minimal admissible quadric bundle and reformulate the assumptions explicitly.

By proposition 2.1 with its proof and proposition 2.3 in [45], it follows that there exists a relatively minimal admissible quadric bundle $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$ such that the generic fibres of $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ and $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$ are isomorphic. This shows that in particular, X and X' are birationally equivalent. If a fibre X_P is geometrically integral, hence split, then $\widetilde{X}'_P$ is split too (see corollary 2.2 in [46]). By the previous paragraph $\widetilde{X}'_P$ is then a geometrically integral quadric, hence so is X'_P. It follows that X'_P is geometrically integral when X_P is geometrically integral.

If all the fibres of $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$ are geometrically integral, the variety X satisfies the Hasse principle and weak approximation (see theorem 3.10 in [11] or theorem 2.1 in [46]). Thus we may assume that at least one $\mathbb{Q}$-fibre X'_P of $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$ is given by a quadratic form of rank 2. Then almost all $\mathbb{Q}$-points on the common line of the two planes of X'_P are smooth in X', hence $X(\mathbb{Q}) \neq \emptyset$.

By a change of variables we may assume the fibre of $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$ at infinity is smooth. Let $\mathbb{A}^1_{\mathbb{Q}} \subset \mathbb{P}^1_{\mathbb{Q}}$ be the complement to the point at infinity, and let t be a coordinate function on $\mathbb{A}^1_{\mathbb{Q}}$. By assumption we know that there are $e_1, \dots, e_r \in \mathbb{Q}$ such that the fibres $X'_{e_1}, \dots, X'_{e_r}$ can be given by quadratic forms of rank 2, and all the other fibres of $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$ are geometrically integral. Let $a_1, \dots, a_r \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$, defined up to squares, be such that $\mathbb{Q}(\sqrt{a_i})$ is the quadratic field over which the components of X'_{e_i} are defined.

Let $U = \mathbb{A}^1_{\mathbb{Q}} - \{e_1, \dots, e_r\}$ and let U_i be a Zariski open neighbourhood of e_i as in (4.4.1). Then by definition, the restriction of $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$ to U_i is given by the vanishing of the equation

$$x_1^2 - \alpha_i x_2^2 + \gamma_i (t - e_i)(x_3^2 - \beta_i x_4^2) = 0,$$

where $\alpha_i, \beta_i, \gamma_i$ are invertible regular functions on U_i (by the relative minimality of $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$). Then at e_i we have $x_1^2 - \alpha_i(e_i)x_2^2 = 0$ which is decomposed to two conjugate planes over $\mathbb{Q}(\sqrt{a_i})$, hence we have $a_i = \alpha_i(e_i)$.

Step 2. Reduce to the case which we can apply (4.3.1).

Let Ω be the set of all places of $\mathbb{Q}$. For any finite set $S \subset \Omega$, we write $\mathbb{Z}_S$ for the subring of $\mathbb{Q}$ consisting of the fractions with denominators divisible only by primes in S. Now we choose

$S \subset \Omega$ to be a finite subset containing 2 and the real place. Then we enlarge the set S such that for all $i = 1, \dots, r$, we have

$$e_i \in \mathbb{Z}_S, \quad a_i \in \mathbb{Z}_S^\times, \quad e_i - e_j \in \mathbb{Z}_S^\times \ \text{ for } \ i \neq j.$$

Moreover, by further increasing S, we can assume that X' has an integral model $\mathcal{X}' \to \mathbb{P}^1_{\mathbb{Z}_S}$ such that for any $p \notin S$, its reduction modulo p, i.e. the morphism $\mathcal{X}'_{\mathbb{F}_p} \to \mathbb{P}^1_{\mathbb{F}_p}$ obtained from

$$\begin{tikzcd} \mathcal{X}'_{\mathbb{F}_p} \arrow[r] \arrow[d] & \mathcal{X}' \arrow[d] \\ \mathbb{P}^1_{\mathbb{F}_p} \arrow[r] & \mathbb{P}^1_{\mathbb{Z}_S} \end{tikzcd}$$

is an admissible quadric bundle with exactly r fibres that are quadrics of rank 2 at the reductions of $e_1, \dots, e_r$ modulo p. For $i = 1, \dots, r$, we define $\mathcal{U}_i \subset \mathbb{P}^1_{\mathbb{Z}_S}$ as the complement to the Zariski closure of $\mathbb{P}^1_{\mathbb{Q}} - U_i$ in $\mathbb{P}^1_{\mathbb{Z}_S}$ and hence we have $U_i = \mathcal{U}_i \times_{\mathbb{Z}_S} \mathbb{Q}$. By enlarging S, we ensure that $\alpha_i, \beta_i, \gamma_i$ are invertible regular functions on $\mathcal{U}_i$, and

$$x_1^2 - \alpha_i x_2^2 + \gamma_i (t - e_i)(x_3^2 - \beta_i x_4^2) = 0,$$

is an equation for $\mathcal{X}'$ over $\mathcal{U}_i$.

Let $a_0 = a_1 \dots a_r$. For $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_r) \in (\mathbb{Q}^\times)^r$, we define the variety $\mathscr{W}_{\boldsymbol{\lambda}}$ as follows:

$$u - e_i v = \lambda_i (x_i^2 - a_i y_i^2) \neq 0, \quad v = x_0^2 - a_0 y_0^2 \neq 0. \tag{4.4}$$

The morphism $\mathscr{W}_{\boldsymbol{\lambda}} \to U$ that sends the point (u, v, x_i, y_i) to the point with the coordinate $t = u/v$ is a torsor of the following $\mathbb{Q}$-torus T:

$$v = x_0^2 - a_0 y_0^2 = x_1^2 - a_1 y_1^2 = \cdots = x_r^2 - a_r y_r^2 \neq 0.$$

Let $Y \subset X'$ be the inverse image of U under $\pi' : X' \to \mathbb{P}^1_{\mathbb{Q}}$. The fibred product $Y \times_U \mathscr{W}_{\boldsymbol{\lambda}}$ is a Y-torsor of T for any $\boldsymbol{\lambda}$. As in the proof of (4.3.2), we see that the family of torsors $Y \times_U \mathscr{W}_{\boldsymbol{\lambda}} \to Y$ is closed under all twists by $\mathbb{Q}$-torsors of T. By (4.3.1), it will be sufficient to prove that the varieties $Y \times_U \mathscr{W}_{\boldsymbol{\lambda}}$ satisfy the Hasse principle and weak approximation.

Write $\mathscr{W} = \mathscr{W}_{\boldsymbol{\lambda}}$. Let us enlarge the set S such that it contains all the primes where we need to approximate, and contains all primes such that $\lambda_i \in \mathbb{Z}_S^\times$ for $i = 1, \dots, r$. We are given a family of $\mathbb{Q}_p$-points N_p for all primes p and a real point N_∞ on $Y \times_U \mathscr{W}$. Let M_p, M_∞ be the images of these points under the natural projection in $\mathscr{W}$. By (4.1.1) the variety $\mathscr{W}$ satisfies the Hasse principle and weak approximation. Indeed, if $a_0 \notin (\mathbb{Q}^\times)^2$, then (4.1.1) can be directly applied to $\mathscr{W}$. If $a_0 \in (\mathbb{Q}^\times)^2$, a change of variables in the last equation of

$$u - e_i v = \lambda_i (x_i^2 - a_i y_i^2) \neq 0, \quad v = x_0^2 - a_0 y_0^2 \neq 0$$

gives $v = x_0' y_0'$, so that $\mathscr{W}$ is birationally equivalent to the product of $\mathbb{A}^1_{\mathbb{Q}}$ and the variety

$$u - e_i v = \lambda_i (x_i^2 - a_i y_i^2), \ i = 1, \dots, r \quad \text{and} \quad v \prod_{i=1}^r (u - e_i v) \neq 0$$

to which (4.1.1) can be applied.

Thus in all cases we can find a point $M \in \mathscr{W}(\mathbb{Q})$ arbitrarily close to the points M_∞ and M_p for $p \in S$, in their real topology and p-adic topology respectively. Let $P \in U(\mathbb{Q})$ be the image of M under the map $\mathscr{W}(\mathbb{Q}) \to U(\mathbb{Q})$ induced by $\mathscr{W} \to U$. We can choose M so that P is contained in a given non-empty open subset of $\mathbb{P}^1_{\mathbb{Q}}$, for example in the open set $U_0 \subset U \cap U_1 \cap \cdots \cap U_r$ defined by the property that $Y_P = X'_P$ is a smooth quadric for any P in U_0. Then Y_P can be given by

$$x_1^2 - \alpha_i x_2^2 + \gamma_i (t - e_i)(x_3^2 - \beta_i x_4^2) = 0$$

for any $i = 1, \dots, r$. By the implicit function theorem, Y_P has $\mathbb{Q}_p$-points close to N_p for $p \in S$ and a real point close to N_∞. We claim that

$$Y(\mathbb{Q}_p) \neq \emptyset \quad \text{for all } p \notin S. \tag{4.5}$$

Once achieved this will show that Y_P is everywhere locally soluble over $\mathbb{Q}$ and hence has a $\mathbb{Q}$-point and satisfies weak approximation (by the theorem of Hasse and the rationality of a smooth quadric with a $\mathbb{Q}$-point). This, in turn, implies that $Y \times_U \mathscr{W}$ also has a $\mathbb{Q}$-point and satisfies weak approximation, as required to complete the proof of (4.4.3).

Step 3. Conclude the assertion by verifying (4.5).

Let $\mathscr{W}_0$ be the inverse image of U_0 in $\mathscr{W}$. To establish (4.5), it will be sufficient to show that the natural projection

$$(Y \times_U \mathscr{W}_0)(\mathbb{Q}_p) \to \mathscr{W}_0(\mathbb{Q}_p)$$

is surjective for all $p \notin S$. We can assume that there exists a point in $\mathscr{W}_0(\mathbb{Q}_p)$ with coordinates $(x_0, y_0, \dots, x_r, y_r) \in \mathbb{Z}_p^{2r+2}$, not all divisible by p. It maps to the point $P = [u : v] \in U_0(\mathbb{Q}_p)$, where $u, v \in \mathbb{Z}_p$, and $t = u/v \in \mathbb{Q}_p$ is such that $t \neq \emptyset$, for any $i = 1, \dots, r$. Let us denote by $x \mapsto \overline{x}$ the map $\mathbb{Q}_p \to \mathbb{F}_p \cup \{\infty\}$ such that $\overline{x} \equiv x \pmod p$ if $x \in \mathbb{Z}_p$ and $\overline{x} = \infty$ if $x \in \mathbb{Q}_p - \mathbb{Z}_p$. We have three possible cases:

(a) $\bar{t}$ is not equal to any of the points $\overline{e}_i$ for $i = 1, \dots, r$;

(b) $\bar{t} = \overline{e}_i$ for some $i \in \{1, \dots, r\}$ and $\mathrm{val}_p(v)$ is even;

(c) $\bar{t} = \overline{e}_i$ for some $i \in \{1, \dots, r\}$ and $\mathrm{val}_p(v)$ is odd.

In case (a), the quadric Y_P reduces to a geometrically integral quadric over $\mathbb{F}_p$. Such a quadric has smooth $\mathbb{F}_p$-points, and any smooth $\mathbb{F}_p$-point lifts to a $\mathbb{Q}_p$-point on Y_P by Hensel's lemma. Thus (4.5) holds in this case.

Now suppose that we are in case (b) or case (c). Then the reduction of Y_P modulo p is the same as that of Y_{e_i}. If a_i is a square modulo p, the reduction of Y_P modulo p is a union of two projective planes defined over $\mathbb{F}_p$. Any $\mathbb{F}_p$-point not on the common line of the two planes is smooth and hence lifts to a $\mathbb{Q}_p$-point in Y_P by Hensel's lemma. Now assume that a_i is not a square modulo p. Since $P = (t : 1) \in U_i(\mathbb{Q})$, we can evaluate

$$x_1^2 - \alpha_i x_2^2 + \gamma_i (t - e_i)(x_3^2 - \beta x_4^2) = 0,$$

at P and obtain an equation for $Y_P = X'_P$. From (4.4) we see that $\mathrm{val}_p(u - e_i v)$ must be even.

In case (b), we deduce that $\mathrm{val}_p(t - e_i)$ is also even. But then Y_P can be given by a quadratic form over $\mathbb{Z}_p$ that reduces to a rank 4 quadratic form over $\mathbb{F}_p$. This implies that Y_P has a $\mathbb{Q}_p$-point, as required for (4.5).

Finally, the case (c) is not compatible with the condition that a_i is not a square modulo p. Indeed, if $\mathrm{val}_p(v)$ is odd, then $\mathrm{val}_p(t - e_i) > 0$ is also odd. Take any $j \in \{1, \dots, r\}$ with $j \neq i$. Since $e_i - e_j \in \mathbb{Z}_S^\times$, we see that $t - e_j \in \mathbb{Z}_S^\times$, so that $u - e_j v$ has odd valuation. Now (**??**) implies that a_j is a square modulo p. Since $v = x_0^2 - a_0 y_0^2$ has odd valuation, a_0 must also be a square modulo p. This is a contradiction to the fact that $a_0 \dots a_r$ is a square. This finishes the proof of (4.5) and so completes the proof of the theorem. □

4.5 Analogous for higher-dimensional varieties

We can also deduce analogous statements for suitable higher-dimensional varieties. Let $m \geq 1$ and $n \geq 3$. The equation

$$\sum_{i=1}^{n} f_i(\mathbf{t}) X_i^2 = 0$$

defines a variety in $\mathbb{P}_{\mathbb{Q}}^{n-1} \times_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}}^m$, where $\mathbf{t} = (t_1, \dots, t_m) \in \mathbb{Q}^m$ and $f_1, \dots, f_n \in \mathbb{Q}[\mathbf{t}]$. We have the following result.

Theorem 4.5.1. *The Brauer-Manin obstruction is the only obstruction to weak approximation on smooth and proper varieties which are $\mathbb{Q}$-birational to the variety*

$$\sum_{i=1}^{n} f_i(\mathbf{t})X_i^2 = 0$$

provided that $f_1, \ldots, f_n$ are products of non-zero linear polynomials defined over $\mathbb{Q}$.

Proof. Let us denote by V the variety defined by $\sum_{i=1}^{n} f_i(\mathbf{t})X_i^2 = 0$. If $n \geq 5$, then each fibre of $V \to \mathbb{A}^m_{\mathbb{Q}}$ is a quadric of dimension at least 3. Hence by (4.4.1), it will be sufficient to assume $n = 3$ or $n = 4$.

On multiplying $\sum_{i=1}^{n} f_i(\mathbf{t})X_i^2 = 0$ and each of the variables X_i by an appropriate non-zero rational function in $\boldsymbol{t} = (t_1, \ldots, t_m)$, it suffices to replace $\sum_{i=1}^{n} f_i(\mathbf{t})X_i^2 = 0$ by a $\mathbb{Q}$-birationally equivalent variety that is given by an equation of the same form satisfying the following additional conditions. There exist pairwise non-proportional, non-constant polynomials $l_1, \ldots, l_r \in \mathbb{Q}[\boldsymbol{t}]$ of degree 1, which are not necessarily homogeneous, such that for $j = 1, \ldots, n$ we can write $f_j = c_j \prod_{i \in I_j} l_i$ where $c_j \in \mathbb{Q}^\times$ and $I_j \subset \{1, \ldots, r\}$. Moreover, for $n = 3$, (resp. $n = 4$), each l_i divides exactly one of f_1, f_2, f_3 (resp. one or two of f_1, f_2, f_3, f_4). Finally, we may assume that

$$l_i(\boldsymbol{t}) = t_1 + d_{i,2}t_2 + \cdots + d_{i,m}t_m + d_{i,0}$$

for $i = 1, \ldots, r$ and appropriate constants $d_{i,0}, d_{i,2}, \ldots, d_{i,m} \in \mathbb{Q}$. Indeed, for $i = 1, \ldots, r$, we can write $l_i(\boldsymbol{t}) = L_i(\boldsymbol{t}) + l_i(0)$, where $L_i(\boldsymbol{t})$ is homogeneous of degree 1. There is a non-zero vector $\boldsymbol{a} \in \mathbb{Q}^m$ such that $L_i(\boldsymbol{a}) \neq 0$ for $i = 1, \ldots, r$. Assuming without loss of generality that $a_1 \neq 0$, one achieves the claim by making the change of variables $t_1 = a_1 t_1'$ and $t_i = t_i' + a_i t_1'$ for $2 \leq i \leq m$ and then replacing c_j by $c_j \prod_{i \in I_j} L_i(\boldsymbol{a})$. The case when $\sum_{i=1}^{n} f_i(\mathbf{t})X_i^2 = 0$ is a quadric over $\mathbb{Q}$ being a subject of Hasse-Minkowski theorem, we can assume without loss of generality that f_1 is not constant and is divisible by $l_1(\boldsymbol{t})$.

When $m = 1$, the statement of the theorem follows from (4.2.2) and (4.4.3). We assume for the remainder of the proof that $m \geq 2$. The map $p : V \to \mathbb{A}^{m-1}_{\mathbb{Q}}$ sending $(X_1, \ldots, X_n, \boldsymbol{t})$ to $(t_2, \ldots, t_m)$ is a surjective morphism. The fibre $V_{\boldsymbol{b}} = p^{-1}(\boldsymbol{b})$ above a point $\boldsymbol{b} = (b_2, \ldots, b_m)$ of $\mathbb{A}^{m-1}_{\mathbb{Q}}$ is given by the following equation with coefficients in the residue field $\mathbb{Q}(\boldsymbol{b})$:

$$\sum_{j=1}^{n} \tilde{f}_j(t)X_j^2 = 0,$$

where $\tilde{f}_j(t) = f_j(t, \boldsymbol{b})$. We note that the morphism p has a section s that sends $(t_2, \ldots, t_m)$ to the point of V with coordinates $X_1 = 1, X_2 = \cdots = X_n = 0,\ t_1 = -l_1(0, t_2, \ldots, t_m)$.

The proof will follow from a variant of the fibration method with a section, which is a result of Harari (theorem 4.3.1 in [24]), once we check that

(1) the generic fibre V_η of p is geometrically integral and geometrically rational, and the section s defines a smooth point of V_η;

(2) there is a non-empty open subset $U \subset \mathbb{A}^{m-1}_{\mathbb{Q}}$ such that for any point $\boldsymbol{b} \in U(\mathbb{Q})$, the Brauer-Manin obstruction is the only obstruction to weak approximation on smooth and proper models of $V_{\boldsymbol{b}}$.

Let $U \subset \mathbb{A}^{m-1}_{\mathbb{Q}}$ be the open subset given by $l_{i_1}(0, \boldsymbol{b}) \neq l_{i_2}(0, \boldsymbol{b})$ for all $i_1 \neq i_2$. This set is not empty since no two polynomials l_{i_1} and l_{i_2} are equal for $i_1 \neq i_2$. The restriction of p to U has geometrically integral fibres, as follows from our assumption that if $n = 3$ (resp. $n = 4$), then each l_i divides exactly one of f_1, f_2, f_3 (resp. one or two of f_1, f_2, f_3, f_4). In the case $n = 3$, the fibre $V_{\boldsymbol{b}}$ is a smooth conic bundle over $\mathbb{A}^1_{\mathbb{Q}(\boldsymbol{b})}$ for any $\boldsymbol{b}$ in U. In particular, V_η is smooth, so the point of V_η defined by s is certainly smooth. In the case $n = 4$ the fibre $V_{\boldsymbol{b}}$ is an admissible quadric bundle over $\mathbb{A}^1_{\mathbb{Q}(\boldsymbol{b})}$. A direct verification shows that at every point of the singular locus $(V_\eta)_{\mathrm{Sing}}$ exactly two of the coordinates X_1, X_2, X_3, X_4 must vanish. Hence the point of V_η defined by s is also smooth in this case. Thus condition (1) is satisfied. Condition (2) follows from (4.2.2) and (4.4.3), so the proof is completed. $\square$

4.6 Rational points on some del Pezzo surfaces of degree 1 and 2

In this section we construct families of del Pezzo surfaces of degree 1 and 2 for which the failure of weak approximation is controlled by the Brauer-Manin obstruction. Recall that a smooth projective surface V is called **minimal** if any birational morphism $V \to V'$, where V' is smooth and projective, is an isomorphism.

We start with describing del Pezzo surfaces in terms of the Galois group action on the set of exceptional curves. Let X be a del Pezzo surface of degree d defined over an algebraically closed field k. Let Γ_d be the graph whose vertices are the exceptional curves on X. Two vertices C_1 and C_2 are connected by n edges if the intersection number $\langle C_1, C_2\rangle_X$ of the corresponding curves is n.

Now let X be a del Pezzo surface of degree d defined over $\mathbb{Q}$. We simply write G for the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$. Let Γ_d be the graph of exceptional curves on $\overline{X} = X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$. Then we obtain an action of the Galois group G on Γ_d.

Let $\Gamma(1)$ be the graph with two vertices joined by a single edge. For a positive integer r, we denote by $\Gamma(r)$ the disconnected union of r copies of $\Gamma(1)$. Recall that a subgraph Γ' of a graph Γ is induced if the vertices of Γ' are connected by exactly the same edges as in Γ.

Proposition 4.6.1. *Consider the family of del Pezzo surfaces of degree $d \leq 7$ over $\mathbb{Q}$ for which Γ_d has an induced subgraph $\Gamma(8-d)$ such that all the connected components of $\Gamma(8-d)$ are G-invariant. All surfaces in this family have the property that the Brauer-Manin obstruction is the only obstruction to weak approximation. Moreover, if $d \in \{1, 2, 4\}$, then the surfaces for which no vertex of $\Gamma(8-d)$ is fixed by G are minimal over $\mathbb{Q}$.*

Proof. See [3], proposition 5.1. □

Let $f, g, h \in \mathbb{Q}[t]$ be polynomials such that $f(t)g(t)h(t) = c\prod_{i=1}^{r}(t - e_i)$ for $c \in \mathbb{Q}^\times$ and pairwise different $e_1, \ldots, e_r \in \mathbb{Q}$. Assume that $l = \deg f$, $m = \deg g$ and $n = \deg h$ are integers of the same parity such that $l \leq m \leq n$. Consider the smooth surface in $\mathbb{P}^2_{\mathbb{Q}} \times \mathbb{A}^1_{\mathbb{Q}}$ defined by

$$f(t)x^2 + g(t)y^2 + h(t)z^2 = 0,$$

where t is a coordinate function on $\mathbb{A}^1_{\mathbb{Q}}$. We embed $\mathbb{A}^1_{\mathbb{Q}}$ into $\mathbb{P}^1_{\mathbb{Q}}$ as the complement to the point ∞. We may also take $\mathbb{A}^1_{\mathbb{Q}} \subset \mathbb{P}^1_{\mathbb{Q}}$ to be the complement to the point $t = 0$ with the coordinate function $T = 1/t$. Let $F(T) = T^l f(1/T)$, $G(T) = T^m g(1/T)$ and $H(T) = T^n h(1/T)$. Consider the smooth surface in $\mathbb{P}^2_{\mathbb{Q}} \times \mathbb{A}^1_{\mathbb{Q}}$ given by

$$F(T)X^2 + G(T)Y^2 + H(T)Z^2 = 0.$$

Let $\pi : V \to \mathbb{P}^1_{\mathbb{Q}}$ be the conic bundle obtained by gluing the above two surfaces. For this we identify the restrictions of the two fibrations to $\mathbb{P}^1_{\mathbb{Q}} - \{0, \infty\}$ by means of the isomorphism $t = T^{-1}$, $x = T^{l_1}X$, $y = T^{m_1}Y$, $z = T^{n_1}Z$, where $(l, m, n) = 2(l_1, m_1, n_1)$ or $(l, m, n) + (1, 1, 1) = 2(l_1, m_1, n_1)$. Since $F(0)G(0)H(0) \neq 0$, the fibre of π at $t = \infty$ is smooth, so π has precisely $r = l + m + n$ degenerate fibres.

The case $r = 5$

Suppose $r = 5$ with $(l, m, n) = (1, 1, 3)$. Setting $z = 1$ in $f(t)x^2 + g(t)y^2 + h(t)z^2 = 0$ and passing to homogeneous coordinates we obtain a smooth cubic surface in $\mathbb{P}^3_{\mathbb{Q}}$ with the equation

$$c_1(u - e_1v)x^2 + c_2(u - e_2v)y^2 + c_3(u - e_3v)(u - e_4v)(u - e_5v) = 0.$$

It contains the line $u = v = 0$. If the conic bundle is relatively minimal, then, contracting this line, we obtain a minimal del Pezzo surface of degree 4 with a $\mathbb{Q}$-point by [29], proposition 2.1.

The case $r = 6$

Suppose that $r = 6$ with $(l, m, n) = (2, 2, 2)$.

Proposition 4.6.2. *Let $f(t) = a(t-e_1)(t-e_2)$, $g(t) = b(t-e_3)(t-e_4)$, $h(t) = c(t-e_5)(t-e_6)$, where $e_1, \ldots, e_6 \in \mathbb{Q}$ are pairwise distinct and $a, b, c \in \mathbb{Q}^\times$. If $f(t), g(t)$ and $h(t)$ are linearly independent over $\mathbb{Q}$, then V is a del Pezzo surface of degree 2 for which the Brauer-Manin obstruction is the only obstruction to weak approximation. If moreover, the classes*

$$-1,\ a,\ b,\ c,\ e_i - e_j \text{ for } 1 \leq i < j \leq 6$$

are linearly independent in the $\mathbb{F}_2$-vector space $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, then V is minimal.

Proof. See [3] proposition 5.2. □

The case $r = 7$

The case $r = 7$ translates as $K_V^2 = 1$. Note that $r = 7$ iff $(l, m, n) = (1, 1, 5)$ or $(l, m, n) = (1, 3, 3)$. We claim that neither of these surfaces can be isomorphic to a del Pezzo surface of degree 1. Recall that del Pezzo surfaces are defined by the property that their anticanonical divisor is ample. It will be sufficient to find a geometrically integral curve C on V for which $\langle C, -K_V \rangle \leq 0$. We adapt an argument of Iskovskikh [29], proposition 1.3 and corollary 1.4.

In the case $(l, m, n) = (1, 1, 5)$ consider the curve C that is the Zariski closure in V of the closed subset of $f(t)x^2 + g(t)y^2 + h(t)z^2 = 0$ given by $z = 0$. We claim that this is a smooth curve of genus 0 such that $\langle C, -K_V \rangle = -1$. To see this we note that C is a smooth curve of genus 0 such that $\langle C, F \rangle = 2$, where $F \in \mathrm{Pic}(V)$ is the class of a fibre. The divisor of the rational function z/x on V is $C + 2F_\infty - C'$, where F_∞ is the fibre at infinity and C' is the Zariski closure in V of the closed subset of $f(t)x^2 + g(t)y^2 + h(t)z^2 = 0$ given by $x = 0$. Since $\langle C, C' \rangle = 1$, we see that $\langle C, C \rangle = -3$ and then from the adjunction formula we find that $\langle C, -K_V \rangle = -1$ as claimed.

In the case $(l, m, n) = (1, 3, 3)$ we consider the pencil of genus 1 curves $E = E_{(\lambda:\mu)}$ cut out by $\lambda y + \mu z = 0$ on V. It is easy to see that $\langle E, E \rangle = 1$ and hence adjunction formula gives $\langle E, -K_V \rangle = 1$. It follows that $E = -K_V$. This pencil contains two reducible members, each consisting of the union of one component of the degenerate fibre at $f(t) = 0$ and a residual rational curve C. It follows that $\langle C, -K_V \rangle = 0$.

The case $r = 8$

We can use some special conic bundles with 8 degenerate fibres to construct del Pezzo surfaces of degree 1 to which (4.2.2) can be applied. Note that $r = 8$ gives $K_V^2 = 0$. Let $e_1, \ldots, e_8 \in \mathbb{Q}$ be pairwise distinct. Let $\pi : V \to \mathbb{P}^1_\mathbb{Q}$ be the conic bundle constructed as above from the surface given by the equation

$$x^2 = \prod_{i=1}^{4} \frac{t - e_i}{e_8 - e_i} y^2 + \prod_{j=5}^{8} (t - e_j) z^2$$

in $\mathbb{P}^2_\mathbb{Q} \times \mathbb{A}^1_\mathbb{Q}$. This conic bundle is not relatively minimal because the fibre at $t = e_8$ is a union of components defined over $\mathbb{Q}$. Either of them can be smoothly contracted, thus producing a conic bundle surface $W \to \mathbb{P}^1_\mathbb{Q}$ with seven degenerate fibres.

Recall that the discriminant of the quartic polynomial $p(t) = \sum_{i=0}^{4} p_i t^i$ is a homogeneous form $D_4(p_0, \ldots, p_4)$ of degree 6. Thus $D_4 = 0$ defines a hypersurface $Z =\subset \mathbb{P}^4_\mathbb{Q}$ of degree 6. The space of projective lines in $\mathbb{P}^4_\mathbb{Q}$ is naturally identified with the Grassmannian $\mathrm{Gr}(2, 5)$. The open subset of $\mathrm{Gr}(2, 5)$ parameterizing those lines that meet Z in six distinct complex points is non-empty. Joining two points by a line gives a dominant rational map from $\mathbb{A}^5_\mathbb{Q} \times \mathbb{A}^5_\mathbb{Q}$ to $\mathrm{Gr}(2, 5)$. It follows that the open subset of $\mathbb{A}^5_\mathbb{Q} \times \mathbb{A}^5_\mathbb{Q}$ consisting of pairs of polynomials $(p(t), q(t))$ such that the discriminant of $rp(t) + aq(t)$ vanishes for exactly six points $(r : s) \in \mathbb{P}^1_\mathbb{C}(\mathbb{C})$ is non-empty. These six points of Z are necessarily smooth in Z, and hence for each of them $rp(t) + sq(t)$ has exactly one double root. We conclude that there is a non-zero polynomial $f(p_0, \ldots, p_4, q_0, \ldots, q_4)$ with coefficients in $\mathbb{Q}$ such that if $f(p_0, \ldots, p_4, q_0, \ldots, q_4) \neq 0$, then $rp(t) + sq(t)$ has multiple roots for exactly six values of $(r : s) \in \mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$, and for each of these values, $rp(t) + sq(t)$ has exactly one double root. Writing the coefficients as symmetric functions of the roots and applying this to the polynomials

$$p(t) = \prod_{i=1}^{4}(t - e_i) \quad \text{and} \quad q(t) = \prod_{j=5}^{8}(t - e_j).$$

We obtain a non-zero polynomial $F(e_1, \ldots, e_8)$ with coefficients in $\mathbb{Q}$.

Proposition 4.6.3. *If $e_1, \ldots, e_8 \in \mathbb{Q}$ satisfy $F(e_1, \ldots, e_8) \neq 0$, then W is a del Pezzo surface of degree 1 over $\mathbb{Q}$ for which the Brauer-Manin obstruction is the only obstruction to weak approximation. If moreover, the classes of $e_i - e_j$ where $1 \leq i \leq 4$ and $5 \leq j \leq 8$ are linearly independent in the $\mathbb{F}_2$-vector space $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, then W is minimal.*

Proof. See [3] proposition 5.3. □

Chapter 5

The Hardy-Littlewood conjecture and rational points

In this chapter, we introduce the results of Y. Harpaz, A.N. Skorobogatov and O. Wittenberg. The main reference is their paper [26].

5.1 Schinzel's hypothesis (H)

In this section we will show how recent results in additive combinatorics help to study the Hasse principle and weak approximation.

A corollary of the Hardy-Littlewood conjecture in the finite complexity case

In a series of papers, Green and Tao ([20], [21]) and Green-Tao-Ziegler ([22]) proved the generalised Hardy-Littlewood conjecture in the finite complexity case. The following statement is corollary 1.9 in [20].

Theorem 5.1.1 (Green, Tao, Ziegler)**.** *Let $L_1(x,y),\dots,L_r(x,y) \in \mathbb{Z}[x,y]$ be pairwise non-proportional linear forms and let $c_1,\dots,c_r \in \mathbb{Z}$. Assume that for each prime number p, there exists $(m,n) \in \mathbb{Z}^2$ such that p does not divide $L_i(m,n)+c_i$ for $i=1,\dots,r$. Let $K \subset \mathbb{R}^2$ be an open convex cone containing a point $(m,n) \in \mathbb{Z}^2$ such that $L_i(m,n) > 0$ for $i=1,\dots,r$. Then there exist infinitely many pairs $(m,n) \in K \cap \mathbb{Z}^2$ such that $L_i(m,n)+c_i$ are all prime numbers.*

Let $S \subset \mathbb{Z}$ be a finite subset of prime numbers. We write $\mathbb{Z}_S = \mathbb{Z}[S^{-1}]$ for the localization of $\mathbb{Z}$ at the multiplicatively closed subset generated by the prime numbers in S.

Proposition 5.1.2. *Let $S \subset \mathbb{Z}$ be a finite subset of prime numbers. Suppose we are given $(\lambda_p,\mu_p) \in \mathbb{Q}_p^2$ for $p \in S$ and a positive real constant C. Let $e_1,\dots,e_r \in \mathbb{Z}_S$. Then there exist pairs $(\lambda,\mu) \in \mathbb{Z}_S^2$ such that*

(1) $\lambda > C\mu > 0$,

(2) (λ,μ) is arbitrarily close to (λ_p,μ_p) in the p-adic topology for $p \in S$,

(3) $\lambda - e_i\mu = u_ip_i$ with $u_i \in \mathbb{Z}_S^\times$ for $i=1,\dots,r$, where $p_1,\dots,p_r$ are prime numbers not in S such that $p_i = p_j$ iff $e_i = e_j$.

Proof. By eliminating repetitions we can assume $e_1,\dots,e_r$ are pairwise distinct. We can multiply λ_p,μ_p by a product of powers of primes in S, so we may assume $(\lambda_p,\mu_p) \in \mathbb{Z}_p^2$ for $p \in S$. We can assume $C > e_i$ for $i=1,\dots,r$ by increasing C. Now we consider the equations $x \equiv \lambda_p \pmod{p^{n_p}}$ where $n_p \gg 0$. By Chinese remainder theorem, we can find a solution $\lambda_0 \in \mathbb{Z}$. Similarly we obtain $\mu_0 \in \mathbb{Z}$ such that $\mu_0 \equiv \mu_p \pmod{p^{n_p}}$. Note that $\lambda_0 + ap^{n_p}$ and $\mu_0 + bp^{n_p}$ are also solutions to $x \equiv \lambda_p \pmod{p^{n_p}}$ and $x \equiv \mu_p \pmod{p^{n_p}}$ respectively. We can therefore assume $\lambda_0 > C\mu_0 > 0$ by choosing a, b sufficiently large. In particular, $\lambda_0 - e_i\mu_0 > \lambda_0 - C\mu_0 > 0$ for all i.

Let d be a product of powers of primes in S such that $de_i \in \mathbb{Z}$ for all i. Let us write

$$d(\lambda_0 - e_i\mu_0) = M_i c_i$$

where M_i is a product of powers of primes in S and $c_i \in \mathbb{Z}$ is coprime to the primes in S. Let N be a product of primes in S such that $N > c_i - c_j$ for any i, j. Take

$$m_p \geq \max_{1\leq i\leq r} \{n_p, \mathrm{val}_p(N) + \mathrm{val}_p(M_i)\},$$

and $M = \prod_{p\in S} p^{m_p}$. Then $m_p \geq \mathrm{val}_p(N) + \mathrm{val}_p(M_i)$ implies N divides M/M_i for all i. Now we look for λ and μ of the form

$$\lambda = \lambda_0 + Mm, \quad \mu = \mu_0 + Mn, \quad (m, n) \in \mathbb{Z}^2.$$

We put $L_i(x, y) = M_i^{-1} Md(x - e_i y)$, then

$$\begin{aligned} \lambda - e_i\mu &= (\lambda_0 - e_i\mu_0) + M(m - e_i n) \\ &= d^{-1}M_i c_i + d^{-1}M_i(M_i^{-1}Md(m - e_i n)) \\ &= d^{-1}M_i(L_i(m, n) + c_i). \end{aligned}$$

Let us check the linear functions $L_i(x, y) + c_i$ satisfy the condition of (5.1.1) and choose an open convex cone K. For $p \in S$, $L_i(0, 0) + c_i = c_i$ is coprime to the primes in S by construction. For $p \notin S$, take $m = \prod_i(\lambda_0 - e_i\mu_0)p$, then $L_i(m, 0) + c_i = c_i(M\prod_{j\neq i}(\lambda_0 - e_j\mu_0)p + 1)$ which is clearly coprime to p. For K, we choose $(m_0, n_0) \in \mathbb{Z}^2$ such that $m_0 > Cn_0 > 0$ and $L_i(m_0, n_0)$ are pairwise distinct. After reordering the subscripts, we obtain the inequalities

$$m_0 > Cn_0 > 0 \quad \text{and} \quad L_1(m_0, n_0) > \cdots > L_r(m_0, n_0) > 0.$$

Define $K \subset \mathbb{R}^2$ by these inequalities.

Then we apply (5.1.1) to these $L_i(x, y)+c_i$ and the cone K. Thus there exist infinitely many pairs $(m, n) \in K \cap \mathbb{Z}^2$ such that $L_i(m, n) + c_i = p_i$, where p_i is a prime not in S for all i. Since N divides $M_i^{-1}Md$ and $L_i(m, n) - L_{i+1}(m, n) > 0$,

$$L_i(m, n) - L_{i+1}(m, n) \geq N > c_{i+1} - c_i$$

holds. Thus $p_i > p_{i+1}$ for $i = 1, \ldots, r-1$. In particular, these p_i are pairwise distinct. $(m, n) \in K$ implies $n > 0$ and $m > Cn$, and it follows that $\mu = \mu_0 + Mn > 0$ and $\lambda = \lambda_0 + Mm > C\mu$. Finally, $\lambda - e_i\mu = d^{-1}M_i(L_i(m, n) + c_i) = d^{-1}M_i p_i$ tells us $u_i = d^{-1}M_i \in \mathbb{Z}_S^\times$. □

An application

We can use the previous proposition to study Hasse principle and weak approximation for certain varieties. For a field extension $K|\mathbb{Q}$ of degree n, we denote by $N_{K|\mathbb{Q}}(\mathbf{x})$ the corresponding norm with $\mathbf{x} = (x_1, \ldots, x_n)$ defined by choosing a basis of K over $\mathbb{Q}$.

Theorem 5.1.3. *Let K_i be a cyclic extension of $\mathbb{Q}$ of degree d_i and let $b_i \in \mathbb{Q}^\times$, $e_i \in \mathbb{Q}$ for $i = 1, \ldots, r$. Then the affine variety $V \subset \mathbb{A}^2 \times \mathbb{A}^{d_1} \times \cdots \times \mathbb{A}^{d_r}$ over $\mathbb{Q}$ defined by*

$$b_i(u - e_i v) = N_{K_i|\mathbb{Q}}(\mathbf{x}_i) \neq 0$$

for $i = 1, \ldots, r$ satisfies the Hasse principle and weak approximation.

Proof. Let Ω be the set of all places of $\mathbb{Q}$. Then Ω_f is identified with the set of all positive prime numbers in $\mathbb{Z}$ and Ω_∞ consists of the only real place. We will denote finite places v of $\mathbb{Q}$ be the corresponding prime numbers p. Let $(M_v) \in \prod_{v\in\Omega} V(\mathbb{Q}_v)$ be the point we need to approximate.

We write $M_p \in V(\mathbb{Q}_p)$ for each prime number p and write $M_0 \in V(\mathbb{R})$ for the real place. Let S be a finite set of places of $\mathbb{Q}$ which we need to approximate. We first find a rational point and then show that the diagonal image $V(\mathbb{Q}) \hookrightarrow \prod_{v\in\Omega} V(\mathbb{Q}_v)$ is dense.

Step 1. Note that the set of real points $(u, v, \mathbf{x}_1, \ldots, \mathbf{x}_r) \in V(\mathbb{R})$ with $(u, v) \in \mathbb{Q}^2$ is dense in $V(\mathbb{R})$, and so it will be sufficient to prove the claim when the coordinates u and v of M_0 are in $\mathbb{Q}$. By a $\mathbb{Q}$-linear change of variables we can assume without loss of generality that M_0 has coordinates $(u, v) = (1, 0)$.

We enlarge S such that the following properties hold. We can assume $b_i \in \mathbb{Z}_S^\times$, $e_i \in \mathbb{Z}_S$ by adding prime factors of the denominators of b_i and e_i for each i. And we can assume the field K_i is unramified outside S for all i. Note that each K_i is unramified at all but finitely many places, hence the enlarged S is still a finite set. We write $(\lambda_p, \mu_p, \mathbf{x}_{1,p}, \ldots, \mathbf{x}_{r,p})$ for the $\mathbb{Q}_p$-point M_p on V. Thus for each $p \in S$ we now have a pair $(\lambda_p, \mu_p) \in \mathbb{Q}_p^2$ such that

$$b_i(\lambda_p - e_i\mu_p) = N_{K_i|\mathbb{Q}}(\mathbf{x}_{i,p}) \neq 0$$

for $i = 1, \ldots, r$, and for some $\mathbf{x}_{i,p} \in K_i \otimes_\mathbb{Q} \mathbb{Q}_p \simeq (\mathbb{Q}_p)^{d_i}$. Let $C > e_i$ for each i be a positive constant determined later. Then by (5.1.2), we can find $(\lambda, \mu) \in \mathbb{Z}_S^2$, $\lambda > C\mu > 0$ such that for each i, the number $b_i(\lambda - e_i\mu)$ is a local norm for $K_i|\mathbb{Q}$ at each finite place of S. It remains to show this is also true for the real place of $\mathbb{Q}$. M_0 has coordinates $(u, v) = (1, 0)$ and $K_i|\mathbb{Q}$ is cyclic, so we conclude $b_i = N_{K_i|\mathbb{Q}}(\mathbf{x}_i) > 0$. By construction $\lambda - e_i\mu > 0$ for all i, it follows $b_i(\lambda - e_i\mu) > 0$ and hence it is a local norm. Moreover, for each i we have $b_i(\lambda - e_i\mu) = p_i u_i$, where $p_i \notin S$, $u_i \in \mathbb{Z}_S^\times$. Recall that $p_i = p_j$ iff $e_i = e_j$.

Step 2. We prove the Hasse principle now. Let $(K_i|\mathbb{Q}, b_i(\lambda - e_i\mu)) \in \mathrm{Br}(\mathbb{Q})$ be the class of the corresponding cyclic algebra. Since $b_i(\lambda_p - e_i\mu_p)$ is a local norm for $p \in S$, we conclude $\mathrm{inv}_p(K_i|\mathbb{Q}, b_i(\lambda_p - e_i\mu_p)) = 0$. By construction, (λ, μ) is close to (λ_p, μ_p) in the p-adic topology for $p \in S$, hence $\mathrm{inv}_p(K_i|\mathbb{Q}, b_i(\lambda - e_i\mu)) = 0$ for $p \in S$, and $\mathrm{inv}_\mathbb{R}(K_i|\mathbb{Q}, b_i(\lambda - e_i\mu)) = 0$ by continuity. Next, $b_i(\lambda - e_i\mu) = u_i p_i$ is a unit at every prime $p \notin S \cup \{p_i\}$ and $K_i|\mathbb{Q}$ is unramified outside S, hence we obtain

$$\mathrm{inv}_p(K_i|\mathbb{Q}, b_i(\lambda - e_i\mu)) = 0$$

for any prime $p \neq p_i$ and for real place. By Hasse's reciprocity law, we have an exact sequence

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{v\in\Omega} \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

We therefore know the case at p_i:

$$0 = \sum_{v\in\Omega} \mathrm{inv}_v(K_i|\mathbb{Q}, b_i(\lambda - e_i\mu)) = \mathrm{inv}_{p_i}(K_i|\mathbb{Q}, b_i(\lambda - e_i\mu)) = \mathrm{inv}_{p_i}(K_i|\mathbb{Q}, p_i).$$

Since $K_i|\mathbb{Q}$ is unramified outside S, the prime p_i splits completely in K_i. In particular, $b_i(\lambda - e_i\mu)$ is a local norm at every place of $\mathbb{Q}$. By Hasse's norm theorem it is a global norm, so that

$$b_i(\lambda - e_i\mu) = N_{K_i|\mathbb{Q}}(\mathbf{x}_i) \neq 0$$

for some $\mathbf{x}_i \in \mathbb{Q}^{d_i}$, i.e. $(\lambda, \mu, \mathbf{x}_1, \ldots, \mathbf{x}_r)$ is a rational point of V. This proves the Hasse principle for V.

Step 3. Now we prove weak approximation for V. Write $d = d_1 \ldots d_r$. Using weak approximation in $\mathbb{Q}$, we find a positive rational number ρ that is arbitrarily close to 1 in the p-adic topology for each prime $p \in S$ and ρ^d is arbitrarily close to $\lambda > 0$ in the real topology. We now make the change of variables

$$\lambda = \rho^d\lambda', \ \mu = \rho^d\mu', \ \mathbf{x}_i = \rho^{d/d_i}\mathbf{x}_i'$$

for all i. Then (λ', μ') is still arbitrarily close to (λ_p, μ_p) in the p-adic topology for each $p \in S$. In the real topology (λ', μ') is arbitrarily close to $(1, \mu/\lambda)$. Since $0 < \mu/\lambda < C^{-1}$, by choosing a sufficiently large C, we ensure that (λ', μ') is close to $(1, 0)$. We can conclude by using weak approximation in the norm tori $N_{K_i|\mathbb{Q}}(\mathbf{z}) = 1$. □

Shinzel's hypothesis

Hypothesis (H_1)**.** Let $e_1, \dots, e_r \in \mathbb{Q}$ be pairwise distinct. Let S be a finite set of primes containing the prime factors of the denominators of $e_1, \dots, e_r$ and the primes $p \leq r$. Suppose we are given $\tau_p \in \mathbb{Q}_p$ for $p \in S$ and a positive real number C. Then there exist $\tau \in \mathbb{Q}$ and primes $p_1, \dots, p_r$ not in S such that

(1) τ is arbitrarily close to τ_p in the p-adic topology for $p \in S$,
(2) $\tau > C$,
(3) $\mathrm{val}_p(\tau - e_i) = 0$ for any $p \notin S \cup \{p_i\}$, $i = 1, \dots, r$,
(4) $\mathrm{val}_{p_i}(\tau - e_i) = 1$ for any $i = 1, \dots, r$.

Hypothesis (H_1) is usually supplemented with the following statement. Let $K|\mathbb{Q}$ be a cyclic extension unramified outside S. Assuming the conclusion of (H_1), we have the following implication: if $\sum_{p\in S} \mathrm{inv}_p(K|\mathbb{Q}, \tau_p - e_i) = 0$ for some i, then p_i splits completely in $K|\mathbb{Q}$. Hypothesis (H_1) and its supplement can be compared to the following consequence of (5.1.2).

Proposition 5.1.4. *Let $e_1, \dots, e_r \in \mathbb{Q}$ and let S be a finite set of primes containing the prime factors of the denominators of $e_1, \dots, e_r$. Suppose that we are given $\tau_p \in \mathbb{Q}_p$ for $p \in S$ and a positive real constant C. Then there exist $\tau \in \mathbb{Q}$ and primes $p_1, \dots, p_r$ not in S with $p_i = p_j$ iff $e_i = e_j$, such that*

(1) τ is arbitrarily close to τ_p in the p-adic topology for $p \in S$,
(2) $\tau > C$,
(3) for each $i = 1, \dots, r$, we have $\mathrm{val}_p(\tau - e_i) \leq 0$ for any $p \notin S \cup \{p_i\}$,
(4) for each $i = 1, \dots, r$, we have $\mathrm{val}_{p_i}(\tau - e_i) = 1$,
(5) for any cyclic extension $K|\mathbb{Q}$ unramified outside S and such that

$$\sum_{p\in S} \mathrm{inv}_p(K|\mathbb{Q}, \tau_p - e_i) = c \in \mathbb{Q}/\mathbb{Z}$$

for some i, we have $\mathrm{inv}_{p_i}(K|\mathbb{Q}, \tau - e_i) = -c$. In particular, if $c = 0$, then p_i splits completely in $K|\mathbb{Q}$.

Proof. By increasing the set $\{e_1, \dots, e_r\}$, we may assume $r \geq 2$ and $e_i \neq e_j$ for some $i \neq j$. We also assume $C > e_i$ for all i. Then we apply (5.1.1) to $(\lambda_p, \mu_p) = (\tau_p, 1)$ for $p \in S$. This provides $(\lambda, \mu) \in \mathbb{Z}_S^2$ such that

(a) $\lambda > C\mu > 0$, (λ, μ) is close to $(\lambda_p, \mu_p) = (\tau_p, 1)$ in the p-adic topology for $p \in S$, and
(b) $\lambda - e_i\mu = u_i p_i$ with $u_i \in \mathbb{Z}_S^\times$ for $i = 1, \dots, r$, where $p_1, \dots, p_r$ are prime numbers not in S such that $p_i = p_j$ iff $e_i = e_j$.

We take $\tau = \lambda/\mu$. Then we prove the above five properties as follows.

(1) Now we have

$$\tau - \tau_p = \lambda/\mu - \tau_p = \mu^{-1}(\lambda - \mu\tau_p) = \mu^{-1}(\lambda - \tau_p + \tau_p(1 - \mu)).$$

Hence τ is arbitrarily close to τ_p.

(2) This holds by $\tau = \lambda/\mu > C$.

(3) By construction μ is an element in $\mathbb{Z}_S$, hence the denominator of μ is a product of primes in S. Thus for $p \notin S$, we have $\mathrm{val}_p(\mu) \geq 0$. Now we take any $p \notin S \cup \{p_i\}$, then we have $\mathrm{val}_p(\lambda - e_i\mu) = \mathrm{val}_p(u_i p_i) = 0$, and it follows that

$$\mathrm{val}_p(\tau - e_i) = \mathrm{val}_p(\lambda - e_i\mu) - \mathrm{val}_p(\mu) \leq 0.$$

(4) We claim $\mathrm{val}_{p_i}(\mu) = 0$ for each $i = 1, \dots, r$. If not, then $\mathrm{val}_{p_i}(\mu) > 0$ for some i. We conclude $\mathrm{val}_{p_i}(\lambda) = \mathrm{val}_{p_i}(u_i p_i + e_i\mu) \geq \min(\mathrm{val}_{p_i}(u_i p_i), \mathrm{val}_{p_i}(e_i\mu)) > 0$. Here we use the fact $\mathrm{val}_{p_i}(e_i\mu) = \mathrm{val}_{p_i}(e_i) + \mathrm{val}_{p_i}(\mu) > 0$ since $e_i \in \mathbb{Z}_S$ and $\mathrm{val}_{p_i}(\mu) > 0$. By assumption we can take j such that $e_i \neq e_j$. It follows that

$$\mathrm{val}_{p_i}(\lambda - e_j\mu) \geq \min(\mathrm{val}_{p_i}(\lambda), \mathrm{val}_{p_i}(e_j\mu)) > 0,$$

which contradicts to (3). Therefore $\mathrm{val}_{p_i}(\mu) = 0$ for all i and

$$\mathrm{val}_{p_i}(\tau - e_i) = \mathrm{val}_{p_i}(\lambda - e_i\mu) = \mathrm{val}_{p_i}(u_ip_i) = 1.$$

(5) Since (λ, μ) is close to $(\tau_p, 1)$ in the p-adic topology for $p \in S$, by continuity we have

$$\sum_{p\in S} \mathrm{inv}_p(K|\mathbb{Q}, \lambda - e_i\mu) = c.$$

We also have $\lambda - e_i\mu > 0$, hence it is a norm and it follows that $\mathrm{inv}_{\mathbb{R}}(K|\mathbb{Q}, \lambda - e_i\mu) = 0$. By the global reciprocity law of class field theory, i.e. the short exact sequence

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{v\in\Omega} \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

we conclude that

$$\sum_{p\notin S} \mathrm{inv}_p(K|\mathbb{Q}, \lambda - e_i\mu) = -c.$$

Since $\mathrm{val}_p(\lambda - e_i\mu) = \mathrm{val}_p(u_ip_i) = 0$ for any prime $p \notin S \cup \{p_i\}$ and $K|\mathbb{Q}$ is unramified outside S, we have $\mathrm{inv}_p(K|\mathbb{Q}, \lambda - e_i\mu) = 0$ for any prime $p \notin S \cup \{p_i\}$. Thus

$$\mathrm{inv}_{p_i}(K|\mathbb{Q}, \lambda - e_i\mu) = -c.$$

When $c = 0$, then $\mathrm{inv}_{p_i}(K|\mathbb{Q}, p_i) = \mathrm{inv}_{p_i}(K|\mathbb{Q}, u_ip_i) = \mathrm{inv}_{p_i}(K|\mathbb{Q}, \lambda - e_i\mu) = 0$. Therefore p_i splits completely in K. □

5.2 Varieties fibred over the projective line

Main theorem I

Let X be an integral variety over $\mathbb{Q}$ and let $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a dominant $\mathbb{Q}$-morphism. Then we obtain an induced homomorphism $\mathbb{Q}(\mathbb{P}^1_{\mathbb{Q}}) \to \mathbb{Q}(X)$ between the corresponding function fields. Applying the functor $\mathrm{Br}(-)$, we obtain a homomorphism $\pi^* : \mathrm{Br}(\mathbb{Q}(\mathbb{P}^1_{\mathbb{Q}})) \to \mathrm{Br}(\mathbb{Q}(X))$ by sending any center simple algebra A over $\mathbb{Q}(\mathbb{P}^1_{\mathbb{Q}})$ to $A \otimes_{\mathbb{Q}(\mathbb{P}^1_{\mathbb{Q}})} \mathbb{Q}(X)$. Recall for integral varieties we have a canonical injection $\mathrm{Br}(X) \to \mathrm{Br}(\mathbb{Q}(X))$. These lead us to the:

Definition 5.2.1. Let $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a dominant morphism of integral varieties over $\mathbb{Q}$. We define the corresponding **vertical Brauer group** of X as

$$\mathrm{Br}_{\mathrm{vert}}(X) := \mathrm{Br}(X) \cap \pi^* \mathrm{Br}(\mathbb{Q}(\mathbb{P}^1_{\mathbb{Q}})) \subset \mathrm{Br}(\mathbb{Q}(X)).$$

By a **$\mathbb{Q}$-fibre** of $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ we mean a fibre above a $\mathbb{Q}$-point of $\mathbb{P}^1_{\mathbb{Q}}$.

We will need the Lang-Weil estimate and we briefly recall it here.

Theorem 5.2.1 (Lang-Weil)**.** *Let $\mathbb{F}_q$ be the finite field with q elements. There exists a constant $C(n, r, d)$ such that for all finite field $\mathbb{F}_q$ and all geometrically integral closed subvariety X of degree d and dimension r of $\mathbb{P}^n_{\mathbb{F}_q}$, we have*

$$|\operatorname{Card}(X(\mathbb{F}_q)) - q^r| < C(n, r, d)q^{r-1/2}.$$

By Lang-Weil estimate, we have $q^r - Cq^{r-1/2} < \operatorname{Card}(X(\mathbb{F}_q))$ where C does not depend on q. Hence we may enlarge q such that X can be defined over $\mathbb{F}_q$ and $q^r - Cq^{r-1/2} > 0$, this means that X has $\mathbb{F}_q$-points. The following result is lemma 1.3 in [13] which is a consequence of Lang-Weil estimate and Hensel's lemma. Although it is proved for number fields, we simply deal with the case of rational numbers.

Lemma 5.2.2. *Let* $\operatorname{Spec} R$ *be a non-empty open subset of* $\operatorname{Spec}\mathbb{Z}$*. Let* $\mathcal{X} \to \operatorname{Spec} R$ *be a flat quasi-projective morphism and let* X *be its generic fibre. Then there exists a finite set* $S \subset \operatorname{Spec} R$ *such that for any non-zero prime number* $p \in \operatorname{Spec} R$ *and* $p \notin S$*, if the fibre* $\mathcal{X}_{\mathbb{F}_p}$ *over* $\mathbb{F}_p$ *splits, then* $\mathcal{X}_{\mathbb{F}_p}$ *contains a smooth* $\mathbb{F}_p$*-point and* X *contains a smooth* $\mathbb{Q}_p$*-point.*

We denote by $\mathbb{Q}_v$ the completions of $\mathbb{Q}$ with respect to the place $v \in \Omega$ and by $\mathbb{A}_{\mathbb{Q}}$ the associated ring of adeles. When v is a finite place, $\mathbb{Q}_v = \mathbb{Q}_p$ for some prime number p and $\mathbb{Q}_v = \mathbb{R}$ for the real place of $\mathbb{Q}$. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$.

Theorem 5.2.3. *Let* X *be a geometrically integral variety over* $\mathbb{Q}$ *with a smooth and surjective morphism* $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ *such that*

(1) each fibre of π *contains a geometrically integral irreducible component except finitely many* $\mathbb{Q}$*-fibres* $X_1, \ldots, X_r$*,*

(2) for each $i = 1, \ldots, r$*, the fibre* X_i *contains an irreducible component* U_i *such that the algebraic closure of* $\mathbb{Q}$ *in its function field* $\mathbb{Q}(U_i)$ *is an abelian extension of* $\mathbb{Q}$*.*

Then $\mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q}) \cap \pi(X(\mathbb{A}_{\mathbb{Q}}))$ *is dense in* $\pi(X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}) \subset \mathbb{P}^1_{\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}}) = \prod_v \mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q}_v)$*.*

Proof. Let $\mathbb{A}^1_{\mathbb{Q}}$ be the affine line over $\mathbb{Q}$. By a change of variables if necessary, we may assume that X_i is the fibre above a $\mathbb{Q}$-point e_i on $\mathbb{A}^1_{\mathbb{Q}} \subset \mathbb{P}^1_{\mathbb{Q}}$ for $i = 1, \ldots, r$. Note that $\mathbb{A}^1_{\mathbb{Q}}(\mathbb{Q}) = \mathbb{Q}$, so we may identify the point e_i on $\mathbb{A}^1_{\mathbb{Q}}$ with a rational number which we will also write e_i by abuse of language. Let K_i be the algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}(U_i)$ and $K_i|\mathbb{Q}$ is an abelian extension as in the assumption (2).

Step 1. Let us recall a description of $\mathrm{Br}_{\mathrm{vert}}(X)$. Since $K_i|\mathbb{Q}$ is an abelian extension, we can write K_i as a composite of cyclic extensions $K_{ij}|\mathbb{Q}$. Let $\chi_{ij} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$ be a character such that K_{ij} is isomorphic to the invariant subfield of $\mathrm{Ker}(\chi_{ij})$, i.e. $K_{ij} \simeq \{x \in \overline{\mathbb{Q}} \mid \sigma(x) = x,\ \forall \sigma \in \operatorname{Ker}\chi_{ij}\}$. Let t be a coordinate on $\mathbb{A}^1_{\mathbb{Q}} \subset \mathbb{P}^1_{\mathbb{Q}}$ such that $\mathbb{Q}(\mathbb{P}^1_{\mathbb{Q}}) = \mathbb{Q}(t)$. Let

$$A_{ij} = (K_{ij}|\mathbb{Q}, t - e_i) \in \mathrm{Br}(\mathbb{Q}(t))$$

be the class of the corresponding cyclic algebra. Here we simply write $(K_{ij}|\mathbb{Q}, t - e_i)$ instead of $(K_{ij}(t)|\mathbb{Q}(t), t - e_i)$ to simplify notations. By (2.2.22), the residue of A_{ij} is non-zero only at e_i and $\infty \in \mathbb{P}^1_{\mathbb{Q}}$ with residues χ_{ij} and $-\chi_{ij}$, respectively. Let $A \in \mathrm{Br}(\mathbb{Q}(t))$ be such that $\pi^*A \in \mathrm{Br}(X)$, i.e. $\pi^*A \in \mathrm{Br}_{\mathrm{vert}}(X)$. Assumptions (1) and (2) together with (2.2.20) imply that A on $\mathbb{P}^1_{\mathbb{Q}}$ is unramified away from $e_1, \ldots e_r$, and that the residue of A at e_i belongs to

$$\operatorname{Ker}\big(\mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}|K_i), \mathbb{Q}/\mathbb{Z})\big).$$

This group is generated by the characters χ_{ij}. Hence there exist $n_{ij} \in \mathbb{Z}$ such that $A - \sum n_{ij}A_{ij}$ is unramified on $\mathbb{A}^1$. Since $\mathrm{Br}(\mathbb{A}^1_{\mathbb{Q}}) = \mathrm{Br}(\mathbb{Q})$ we conclude that $A = \sum n_{ij}A_{ij} + A_0$ for some $A_0 \in \mathrm{Br}(\mathbb{Q})$. A is unramified at $\infty \in \mathbb{P}^1_{\mathbb{Q}}$ and $A_0 \in \mathrm{Br}(\mathbb{Q})$ imply, by considering residues at ∞, that

$$\sum n_{ij}\chi_{ij} = 0 \in \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}), \mathbb{Q}/\mathbb{Z}).$$

Therefore, every element of $\mathrm{Br}_{\mathrm{vert}}(X)$ is of the form $\sum n_{ij}\pi^*A_{ij} + A_0$ for some n_{ij} such that $\sum n_{ij}\chi_{ij} = 0$ and some $A_0 \in \mathrm{Br}(\mathbb{Q})$.

Step 2. Now we slightly modify the point we need to approximate by a point arbitrarily close to it and we enlarge the set of places we need to approximate. We can assume $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}} \neq \emptyset$, otherwise there is nothing to prove. Take $(M_v) \in X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}$ to be the point we need to approximate. As usual, we write M_p for points in $X(\mathbb{Q}_p)$ for each prime p and M_0 for points in $X(\mathbb{R})$. By replacing (M_v) by a point arbitrarily close to it, we can assume that M_p does not belong to any of the fibres $X_1, \ldots, X_r$.

We include the real place in the finite set of places S where we need to approximate. The set of real points $M_0 \in X(\mathbb{R})$ for which $\pi(M_0) \in \mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q})$ is dense in $X(\mathbb{R})$, and so it is sufficient to approximate adelic points (M_p) such that $\pi(M_0) \in \mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q})$. By a change of variables we then assume that $\pi(M_0) = \infty$. By replacing (M_p) by a point arbitrarily close to it for each prime p, we can further assume that $\pi(M_p) \neq \infty$ when $p \neq 0$.

Then we enlarge S such that the following properties hold. First, for any $p \notin S$, X has a good reduction at p, i.e. X admits a smooth model over $\mathbb{Z}_{(p)}$. Second, by adding prime factors appeared in the denominators, we can assume $e_i \in \mathbb{Z}_S$ for all i, and $e_i - e_j \in \mathbb{Z}_S^\times$ for all $i \neq j$. Third, for any $p \notin S$, p is unramified in any of the fields K_i. Furthermore, by (5.2.2) we increase S so that if K_i has a place of degree 1 over $p \notin S$, then the corresponding $\mathbb{F}_p$-component of the degenerate fibre of π over the reduction of e_i has an $\mathbb{F}_p$-point. By a similar argument we assume that on the reduction of X modulo $p \notin S$ any geometrically integral component of a fibre over an $\mathbb{F}_p$-point contains an $\mathbb{F}_p$-point. All these $\mathbb{F}_p$-points are smooth, because π is a smooth morphism.

Since $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\mathrm{vert}}} \neq \emptyset$, by the result of Step 1 we can use Harari's formal lemma (2.4.12) to increase $S \subset S_1$ and choose $M_p \in X(\mathbb{Q}_p)$ for $p \in S_1 - S$ away from the fibres $X_1, \dots, X_r$ so that for all i, j we have

$$\sum_{p \in S_1} \mathrm{inv}_p \left(A_{ij}(\pi(M_p))\right) = 0.$$

Step 3. Let τ_p be the coordinate of $\pi(M_p) \in \mathbb{A}^1_\mathbb{Q}$, where p is a prime number in S_1 and let $\tau_0 \in \mathbb{P}^1_\mathbb{Q}(\mathbb{R})$ be the image of M_0. Note that $M_p \in \mathbb{P}^1_\mathbb{Q}(\mathbb{Q}_p)$ implies that $\tau_p \in \mathbb{A}^1_\mathbb{Q}(\mathbb{Q}_p) = \mathbb{Q}_p$ for each prime number $p \in S_1$. An application of (5.1.4) produces an arbitrarily large positive rational number $\tau \in \mathbb{Q}$ such that τ is arbitrarily close to τ_p in the p-adic topology for each prime number $p \in S_1$. Let $M \in \mathbb{A}^1_\mathbb{Q}(\mathbb{Q}) \subset \mathbb{P}^1_\mathbb{Q}(\mathbb{Q})$ be the point with coordinate τ. We claim $X_M(\mathbb{A}_\mathbb{Q}) \neq \emptyset$.

By construction we obtain $X_{\tau_p}(\mathbb{Q}_p) \neq \emptyset$ and $X_{\tau_0}(\mathbb{R}) \neq \emptyset$. The fibre X_M is smooth, hence by the inverse function theorem we have $X_M(\mathbb{R}) \neq \emptyset$ and $X_M(\mathbb{Q}_p) \neq \emptyset$ for $p \in S_1$. Thus it remains to consider the following two cases.

(I) $\mathbb{Q}_v = \mathbb{Q}_p$ where $p = p_i$, $i = 1, \dots, r$. Since $\mathrm{val}_{p_i}(\tau - e_i) = 1$, the reduction of τ modulo p_i equals the reduction of e_i. We conclude

$$\sum_{p \in S_1} \mathrm{inv}_p(K_{ij}|\mathbb{Q}, \tau - e_i) = \sum_{p \in S_1} \mathrm{inv}_p(A_{ij}(\tau)) = \sum_{p \in S_1} \mathrm{inv}_p(A_{ij}(\tau_p)) = 0,$$

since τ is close to τ_p in the p-adic topology and inv_p is locally constant. Now property (5) of (5.1.4) implies that for each $i = 1, \dots, r$, all the cyclic fields K_{ij} are split at p_i, and thus K_i is also split. Hence there is a geometrically integral irreducible component of the $\mathbb{F}_{p_i}$-fibre over the reduction of e_i modulo p_i. We arranged that it has an $\mathbb{F}_{p_i}$-point in step 2. By Hensel's lemma, it gives rise to a $\mathbb{Z}_{p_i}$-point in X_M.

(II) $\mathbb{Q}_v = \mathbb{Q}_p$ where $p \notin S_1 \cup \{p_1, \dots, p_r\}$. We have $\mathrm{val}_p(\tau - e_i) \leq 0$ for all i, and hence the reduction of τ modulo p is a point of $\mathbb{P}^1(\mathbb{F}_p)$ other than the reduction of any of $e_1, \dots, e_r$. Thus any $\mathbb{F}_p$-point on a geometrically integral irreducible component of the fibre at $\tau \pmod p$ gives rise to a $\mathbb{Z}_p$-point on X_M by Hensel's lemma.

In both cases we constructed a $\mathbb{Q}_p$-point that comes from a $\mathbb{Z}_p$-point on an integral model of X_M, therefore $X_M(\mathbb{A}_\mathbb{Q}) \neq \emptyset$. ☐

Corollary 5.2.4. *In the situation of (5.2.3), let us assume further that all but finitely many $\mathbb{Q}$-fibres of $\pi : X \to \mathbb{P}^1_\mathbb{Q}$ satisfy the Hasse principle. Then $\pi(X(\mathbb{Q}))$ is dense in $\pi(X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\mathrm{vert}}})$. If these $\mathbb{Q}$-fibres X_τ are such that $X_\tau(\mathbb{Q})$ is dense in $X_\tau(\mathbb{A}_\mathbb{Q})$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\mathrm{vert}}}$.*

Proof. We can assume $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\mathrm{vert}}} \neq \emptyset$, otherwise there is nothing to prove. Then we can take an adelic point $(M_v) \in X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\mathrm{vert}}}$. Let's say $\pi((M_v)) = (\tau_v) \in \mathbb{P}^1_\mathbb{Q}(\mathbb{A}_\mathbb{Q})$. By (5.2.3), we can find $\lambda \in \mathbb{P}^1_\mathbb{Q}(\mathbb{Q}) \cap \pi(X(\mathbb{A}_\mathbb{Q}))$ which is arbitrarily close to (τ_v). Since all but finitely many $\mathbb{Q}$-fibres of π satisfies the Hasse principle, we may assume the fibre X_λ satisfies the Hasse principle. Note that $\lambda \in \pi(X(\mathbb{A}_\mathbb{Q}))$, $X_\lambda(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ holds and it follows that $X_\lambda(\mathbb{Q}) \neq \emptyset$ by the Hasse principle. Therefore $\pi(X(\mathbb{Q}))$ is dense in $\pi(X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\mathrm{vert}}})$.

For the second assertion, let $(M_v) \in X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\mathrm{vert}}}$ be the point we need to approximate. We can find $\tau = \pi(N) \in \mathbb{P}^1_\mathbb{Q}(\mathbb{Q})$ for some $N \in X(\mathbb{Q})$ that is arbitrarily close to $\pi((M_v))$ by the first assertion and such that $X_\tau(\mathbb{Q})$ is dense in $X_\tau(\mathbb{A}_\mathbb{Q})$ by assumption. Then $N \in X(\mathbb{Q})$ is arbitrarily close to (M_v) and we are done. ☐

Remark 5.2.5. If the generic fibre of $\pi : X \to \mathbb{P}^1$ is proper, then all but finitely many fibres of π are proper. For proper $\mathbb{Q}$-fibres X_τ, the approximation assumptions in (5.2.4) is that of weak approximation, since in this case $X_\tau(\mathbb{A}_\mathbb{Q}) = \prod_{v\in\Omega} X_\tau(\mathbb{Q}_v)$. By Hironaka's theorem, we can always replace $\pi : X \to \mathbb{P}^1$ by a partial compactification $\pi' : X' \to \mathbb{P}^1$ such that X is a dense open subset of X' and the morphism π' is smooth with proper generic fibre.

Application: a new proof of Theorem (5.1.3)

We can prove (5.1.3) in a different manner. Let W be the quasi-affine subvariety of $\mathbb{A}^2 \times \mathbb{A}^{d_1} \times \cdots \times \mathbb{A}^{d_r}$ given by

$$b_i(u - e_i v) = N_{K_i|\mathbb{Q}}(\mathbf{x}_i)$$

for $i = 1, \ldots, r$ and $(u, v) \neq (0, 0)$. Then the variety

$$b_i(u - e_i v) = N_{K_i|\mathbb{Q}}(\mathbf{x}_i) \neq 0$$

for $i = 1, \ldots, r$ is a dense open subset of W. The projection to the coordinates (u, v) defines a morphism $W \to \mathbb{A}^2_\mathbb{Q} - (0, 0)$. Then we obtain a morphism $\pi : W \to \mathbb{P}^1_\mathbb{Q}$ by composing the projection $\left(\mathbb{A}^2_\mathbb{Q} - (0, 0)\right) \to \mathbb{P}^1_\mathbb{Q}$. Let X be the smooth locus of π. Since each fibre of π contains a smooth point, we see that $\pi(X) = \mathbb{P}^1_\mathbb{Q}$. Let $\pi' : Y \to \mathbb{P}^1_\mathbb{Q}$ be a partial compactification of $\pi : X \to \mathbb{P}^1_\mathbb{Q}$. Then π' is smooth with proper generic fibre.

Let $t = u/v$ be a coordinate on $\mathbb{P}^1_\mathbb{Q}$. We can conclude (5.1.3) by verifying (1) assumptions of theorem (5.2.3) holds, (2) geometrically integral, proper $\mathbb{Q}$-fibres of π' satisfy the Hasse principle and weak approximation, and (3) $\mathrm{Br}_{\mathrm{vert}}(Y) = \mathrm{Br}_0(Y)$. These indeed hold by §3.3 in [26].

Main theorem II

Next we give a statement for a smooth and proper variety X, to be compared with theorem 1.1 in [13]. We need several results in [12].

Let $f : X \to Z$ be a surjective k-morphism between integral k-varieties over a field k of characteristic 0. Then we define $\mathrm{Br}_{\mathrm{vert}}(X) = \mathrm{Br}(X) \cap f^* \mathrm{Br}(k(Z)) \subset \mathrm{Br}(k(X))$. Here $k(X)$ and $k(Z)$ are the function fields of X and Z, respectively. Since Z is integral, we conclude that $\mathrm{Br}(Z) \subset \mathrm{Br}(k(Z))$ and hence $f^* \mathrm{Br}(Z) \subset \mathrm{Br}_{\mathrm{vert}}(X)$.

Lemma 5.2.6. *Let k be a field of characteristic 0. Let X, Z be regular geometrically integral k-varieties. Let $f : X \to Z$ be a flat surjective morphism with geometrically split fibres at points of Z of codimension one and with geometrically integral generic fibre. Then $\mathrm{Br}_{\mathrm{vert}}(X)/f^* \mathrm{Br}(Z)$ is finite.*

Proof. For an arbitrary scheme S, we write $S^{(1)}$ for the set of points of codimension one on S. For any $z \in Z^{(1)}$, the fibre X_z is non-empty and all the components of X_z have codimension 1 in X since f is flat and surjective. We consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Br}(Z) \arrow[r] \arrow[d, "f^*"] & \mathrm{Br}(k(Z)) \arrow[r] \arrow[d, "f^*"] & \bigoplus_{z\in Z^{(1)}} H^1(\kappa(z), \mathbb{Q}/\mathbb{Z}) \arrow[d, "e_{x|z}\cdot f^*"] \\
0 \arrow[r] & \mathrm{Br}(X) \arrow[r] & \mathrm{Br}(k(X)) \arrow[r] & \bigoplus_{x\in X^{(1)}} H^1(\kappa(x), \mathbb{Q}/\mathbb{Z}),
\end{tikzcd}$$

where $z = f(x)$, and $e_{x|z}$ is the multiplicity in the fibre X_z of the irreducible component whose generic point is x.

Since the fibres X_z are geometrically split, for each $z \in Z^{(1)}$, we can choose $x' \in X^{(1)}$ such that $f(x') = z$ and $e_{x'|z} = 1$. Let $\kappa_{x'}$ be the integral closure of $\kappa(z)$ in $\kappa(x')$. Then $\kappa_{x'}$ is a finite and separable extension of $\kappa(z)$. Then the map $e_{x'|z} \cdot f^*$ on $H^1(\kappa(z), \mathbb{Q}/\mathbb{Z})$ decomposes as

$$H^1(\kappa(z), \mathbb{Q}/\mathbb{Z}) \stackrel{r_{z,x'}}{\to} H^1(\kappa_{x'}, \mathbb{Q}/\mathbb{Z}) \hookrightarrow H^1(\kappa(x'), \mathbb{Q}/\mathbb{Z}),$$

where $r_{z,x'}$ is the restriction map and the last map is injective since $\kappa_{x'}$ is integrally closed in $\kappa(x')$. By the commutativity of the diagram, we get the inclusion

$$\mathrm{Br}_{\mathrm{vert}}(X)/f^*(\mathrm{Br}(Z)) \hookrightarrow \bigoplus_x \mathrm{Ker}\, r_{z,x'}.$$

If X_z is geometrically integral, then $\mathrm{Ker}\, r_{z,x'} = 0$. Since the generic fibre of f is geometrically integral, this is the case for all but a finite number of $z \in Z^{(1)}$. In general, $\mathrm{Ker}\, r_{z,x'}$ is a finite group. □

Corollary 5.2.7. *With the same assumptions as in (5.2.6), let $Y \subset X$ be an open subset such that the composite map $Y \to X \to Z$ is surjective and has geometrically split fibres at points of codimension one of Z. Then $\mathrm{Br}_{\mathrm{vert}}(X)$ is a subgroup of $\mathrm{Br}_{\mathrm{vert}}(Y)$ of finite index. If moreover Z is proper and k-birational to a projective space, then the group $\mathrm{Br}_{\mathrm{vert}}(Y)/\mathrm{Br}_0(Y)$ is finite.*

Proof. Let $j : Y \to X$ be the open immersion. Then $f \circ j : Y \to Z$ is a flat and surjective morphism. Hence $\mathrm{Br}_{\mathrm{vert}}(Y)/(f \circ j)^* \mathrm{Br}(Z)$ is finite by (5.2.6). Then $\mathrm{Br}_{\mathrm{vert}}(X)$ is a subgroup of finite index by (5.2.6).

If Z is proper and k-birational to a projective space, then $\mathrm{Br}(Z) = \mathrm{Br}(k)$. We conclude by definition $\mathrm{Br}_0(Y) = \mathrm{Im}(f \circ j)^* \mathrm{Br}(k)$. □

Proposition 5.2.8. *Let X be a smooth and geometrically integral variety over a number field k. Let $Y \subset X$ be a dense open subset. Let $B \subset \mathrm{Br}(Y)$ be a subgroup such that $[B : B \cap \mathrm{Br}_0(Y)]$ is finite. Then $X(\mathbb{A}_k)^{B \cap \mathrm{Br}(X)} \neq \emptyset$ iff $Y(\mathbb{A}_k)^B \neq \emptyset$. If X is a proper k-variety, then $Y(\mathbb{A}_k)^B$ is dense in the closed subset $X(\mathbb{A}_k)^{B \cap \mathrm{Br}(X)}$ of $X(\mathbb{A}_k) = \prod_{v \in \Omega} X(k_v)$.*

Proof. Let X_c be the smooth compactification of X, then X is an open subset of X_c and X_c is smooth and geometrically integral. We obtain

$$Y(\mathbb{A}_k)^B \subset X(\mathbb{A}_k)^{B \cap \mathrm{Br}(X)} \subset X_c(\mathbb{A}_k)^{B \cap \mathrm{Br}(X_c)},$$

and hence it will be sufficient to show that $X_c(\mathbb{A}_k)^{B \cap \mathrm{Br}(X_c)} \neq \emptyset$ implies $Y(\mathbb{A}_k)^B \neq \emptyset$. Let $A_1, \ldots, A_n \in B$ be a set of representatives for $B/(B \cap \mathrm{Br}_0(Y))$. Over a dense open subset $U \subset \mathrm{Spec}\, \mathcal{O}_k$, Y has a smooth integral model $\mathcal{Y}$ over U such that $\mathcal{Y}(\mathcal{O}_v) \neq \emptyset$ for each $v \in U$ and such that each A_i is contained in $\mathrm{Br}(\mathcal{Y}) \subset \mathrm{Br}(Y)$. Let $(P_v)_{v \in \Omega} \in X_c(\mathbb{A}_k)^{B \cap \mathrm{Br}(X)}$. Let S be a finite set of places not in U, (hence contains the archimedean places). For each place $v \in S$, let $U_v \in X(k_v)$ be an open set. Harari's formal lemma implies that there is a finite set T of places of k such that $S \cap T = \emptyset$, and points $P_v \in Y(k_v)$ for $v \in S \cup T$, with $P_v \in U_v$ for $v \in S$, such that

$$\sum_{v \in S \cup T} \mathrm{inv}_v(A_i(P_v)) = 0$$

for $i = 1, \ldots, n$. Now pick up any set of integral points $P_v \in \mathcal{Y}(\mathcal{O}_v)$ for $v \notin S \cup T$. Then $A_i(P_v) \in \mathrm{Br}(\mathcal{O}_v) = 0$ implies $\sum_{v \in \Omega} \mathrm{inv}_v(A(P_v)) = 0$ for any $A \in B$. This means that $(P_v)_{v \in \Omega} \in Y(\mathbb{A}_k)^B$. This proves the first part of the proposition. The second part also follows because if X is proper over k, hence $X = X_c$, then a basis of open sets for the topology of $X(\mathbb{A}_k)$ is given by sets $\prod_{v \in S} U_v \times \prod_{v \notin S} X(k_v)$. □

Proposition 5.2.9. *Let X be a smooth, proper and geometrically integral variety over a number field k. Let $f : X \to \mathbb{P}^1_k$ be a dominant morphism with geometrically split fibres and geometrically integral generic fibre. Let $Y \subset X$ be a dense open set such that the composite map $Y \to X \to \mathbb{P}^1_k$ is surjective and has geometrically split fibres at closed points of $\mathbb{P}^1_k$. Then $Y(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(Y)}$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)} \subset X(\mathbb{A}_k)$.*

Proof. Now $\mathrm{Br}_{\mathrm{vert}}(X) = \mathrm{Br}(X) \cap \mathrm{Br}_{\mathrm{vert}}(Y)$ and $\mathrm{Br}_{\mathrm{vert}}(Y)/\mathrm{Br}_0(Y)$ is finite by (5.2.7). The above proposition implies $Y(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(Y)}$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)}$. □

In our situation below, $Y \to \mathbb{P}^1$ is a smooth surjective morphism with geometrically split fibres at points of $\mathbb{P}^1$ of codimension 1 and with geometrically integral generic fibre. Then we claim $\mathrm{Br}_{\mathrm{vert}}(Y)/\pi^* \mathrm{Br}(\mathbb{P}^1)$ is finite.

Theorem 5.2.10. *Let X be a smooth, proper and geometrically integral variety over $\mathbb{Q}$ with a surjective morphism $\pi : X \to \mathbb{P}^1$ such that*

(1) each fibre of π contains a geometrically integral irreducible component of multiplicity one except finitely many $\mathbb{Q}$-fibres $X_1, \dots, X_r$,

(2) for all i, the fibre X_i contains an irreducible component of multiplicity one such that the algebraic closure of $\mathbb{Q}$ in its function field is an abelian extension of $\mathbb{Q}$.

Then $\mathbb{P}^1(\mathbb{Q}) \cap \pi(X(\mathbb{A}_{\mathbb{Q}}))$ is dense in $\pi(X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}) \subset \mathbb{P}^1(\mathbb{A}_{\mathbb{Q}}) = \prod_v \mathbb{P}^1(\mathbb{Q}_v)$. If all but finitely many $\mathbb{Q}$-fibres of π satisfy the Hasse principle and weak approximation, then $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}$.

Proof. Let $Y \subset X$ be the smooth locus of π. Then by assumption, each fibre of π contains an irreducible component of multiplicity one. In particular, each fibre of π contains a smooth point and hence $\pi : Y \to \mathbb{P}^1$ is surjective. Now $\pi : Y \to \mathbb{P}^1$ is a smooth and surjective morphism, so we can apply (5.2.3). It follows that $\mathbb{P}^1(\mathbb{Q}) \cap \pi(Y(\mathbb{A}_{\mathbb{Q}}))$ is dense in $\pi(Y(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}(Y)})$. By applying (5.2.6), we conclude $Y(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}(Y)}$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}(X)}$. Hence $\mathbb{P}^1(\mathbb{Q}) \cap \pi(Y(\mathbb{A}_{\mathbb{Q}}))$ is dense in $\pi(X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}(X)})$. In particular, the first assertion holds. By weak approximation, we conclude that all but finitely many fibres X_τ verify $X_\tau(\mathbb{Q}) \subset X_\tau(\mathbb{A}_{\mathbb{Q}})$ is dense. Thus applying (5.2.4), it follows $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}$. □

Application to pencils of Severi-Brauer and similar varieties

Corollary 5.2.11. *Let X be a smooth, proper and geometrically integral variety over $\mathbb{Q}$ with a morphism $\pi : X \to \mathbb{P}^1$. Suppose the generic fibre of π is a Severi-Brauer variety, a 2-dimensional quadric, or a product of such. If all the fibres of π that are not geometrically integral are $\mathbb{Q}$-fibres, then $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}$.*

Proof. The assumptions of (5.2.10) are satisfied by [45] and [17] and hence the assertion holds. □

5.3 Application to norm forms

5.3.1 Cyclic extensions

Consider the following system of Diophantine equations:

$$N_{K_i|\mathbb{Q}}(\mathbf{x}_i) = P_i(t)$$

for $i = 1, \dots, r$, where $K_i|\mathbb{Q}$ are cyclic extensions and the polynomials $P_i(t)$ are products of (possibly repeated) linear factors over $\mathbb{Q}$.

Corollary 5.3.1. *Let X be a smooth, proper and geometrically integral variety over $\mathbb{Q}$ with a surjective morphism $\pi : X \to \mathbb{P}^1$ such that the generic fibre of π is birationally equivalent to the affine variety*

$$N_{K_i|\mathbb{Q}}(\mathbf{x}_i) = P_i(t)$$

over $\mathbb{Q}(\mathbb{P}^1) = \mathbb{Q}(t)$. Then $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}$.

Proof. We want to show the assumptions (1) and (2) of (5.2.10) hold for π and all but finitely many $\mathbb{Q}$-fibres of π satisfy the Hasse principle and weak approximation.

Each fibre of π outside infinity and the zero set of $P_1(t) \dots P_r(t) = 0$ contains a geometrically integral irreducible component of multiplicity one. Hence (1) holds. Since π has a section over the composite $K_1 \dots K_r$ which is abelian extension of $\mathbb{Q}$, (2) holds. By Hasse's norm theorem, the varieties $N_{K|\mathbb{Q}}(\mathbf{z}) = c$ satisfies the Hasse principle where $K|\mathbb{Q}$ is a cyclic extension and $c \in \mathbb{Q}^\times$. Moreover, smooth and proper models of principal homogeneous spaces of cyclic norm tori satisfy the Hasse principle and weak approximation, by chapter 8 in [41]. It follows that all but finitely many fibres of π verifies the Hasse principle. We conclude by (5.2.10). □

Remark 5.3.2. For any cyclic extension of fields $K|k$ the affine variety $N_{K|k}(\mathbf{x}) = c \in k^\times$ is birationally equivalent to the Severi-Brauer variety defined by the cyclic algebra $(K|k, c)$. Thus corollary (5.3.1) can be seen as a particular case of corollary (5.2.11).

When each $P_i(t)$ is linear, we have the following consequence of (5.3.1).

Corollary 5.3.3. *Let K_i be a cyclic extension of $\mathbb{Q}$ of degree d_i for $i = 1, \dots, r$. Let $b_i \in \mathbb{Q}^\times$ and $e_i \in \mathbb{Q}$, $i = 1, \dots, r$. Then the variety X over $\mathbb{Q}$ defined by*

$$b_i(t - e_i) = N_{K_i|\mathbb{Q}}(\mathbf{x}) \neq 0$$

for $i = 1, \dots, r$, satisfies the Hasse principle and weak approximation.

Proof. By calculation the rank of the Jacobian matrix, it follows that the variety X is smooth. By (5.3.1), it will be sufficient to show $\mathrm{Br}_{\mathrm{vert}}(X) = \mathrm{Br}_0(X)$. In step 1 of the proof of (5.2.3), we saw that for any $A \in \mathrm{Br}(\mathbb{Q}(t))$ such that $\pi^* A \in \mathrm{Br}(X) \subset \mathrm{Br}(\mathbb{Q}(X))$ there exists $A_0 \in \mathrm{Br}(\mathbb{Q})$ for which we can write

$$A = \sum_{i=1}^{r} n_i (K_i|\mathbb{Q}, t - e_i) + A_0.$$

Since $(K_i|\mathbb{Q}, N_{K_i|\mathbb{Q}}(\mathbf{x}_i)) = 0$ in $\mathrm{Br}(\mathbb{Q}(X))$ ($N_{K_i|\mathbb{Q}}(\mathbf{x}_i)$ is a norm form), the element $\pi^* A \in \mathrm{Br}(X)$ can be written as

$$\pi^* A = -\sum_{i=1}^{r} n_i (K_i|\mathbb{Q}, b_i) + A_0 \in \mathrm{Br}_0(X).$$

It follows $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_0(X)} = X(\mathbb{A}_\mathbb{Q})$, i.e. X satisfies the weak approximation. $\square$

We can use (5.3.1) and the fibration method in the form of Theorem 3.2.1 in [25] to deduce the following:

Corollary 5.3.4. *Let X be a smooth and proper model of the variety over $\mathbb{Q}$ defined by the system of equations*

$$N_{K_i|\mathbb{Q}}(\mathbf{x}_i) = P_i(t_1, \dots, t_n)$$

for $i = 1, \dots, r$, where each K_i is a cyclic extension of $\mathbb{Q}$ and each $P_i(t_1, \dots, t_n)$ is a product of polynomials of degree 1 over $\mathbb{Q}$. Then $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$.

5.3.2 Products of norms

We can consider a product of norm forms associated to field extensions of $\mathbb{Q}$ satisfying certain conditions. We can apply (5.2.10) to deduce:

Corollary 5.3.5. *Let $P(t)$ be a product of (possibly repeated) linear factors over $\mathbb{Q}$. Let $L_1, \dots, L_n$ be $n \geq 2$ finite filed extensions of $\mathbb{Q}$ such that $L_1|\mathbb{Q}$ is abelian and linearly disjoint from the composite $L_2 \dots L_n$. Let X be a smooth, proper and geometrically integral variety over $\mathbb{Q}$ with a morphism $\pi : X \to \mathbb{P}^1$ such that the generic fibre of π is birationally equivalent to the affine variety*

$$N_{L_1|\mathbb{Q}}(\mathbf{x}_1) \dots N_{L_n|\mathbb{Q}}(\mathbf{x}_n) = P(t)$$

over $\mathbb{Q}(\mathbb{P}^1) = \mathbb{Q}(t)$. Then X satisfies the Hasse principle and weak approximation.

Proof. By the same argument as in (5.3.1), assumptions (1) and (2) of Theorem (5.2.10) are satisfied since $L_1|\mathbb{Q}$ is abelian. By chapter 8 in [41], $Ш^2_\omega(\mathbb{Q}, \hat{T}) = 0$ will imply almost all $\mathbb{Q}$-fibres satisfy the Hasse principle and weak approximation. Here T is the multinorm torus over $\mathbb{Q}$ attached to the fields $L_1, \dots, L_n$. This is theorem 1 in [16] which is proved by Demarche and Wei. It follows that $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\mathrm{vert}}}$ by (5.2.10).

We claim $\mathrm{Br}_{\mathrm{vert}}(X) = \mathrm{Br}_0(X)$. Take $A \in \mathrm{Br}(\mathbb{Q}(t))$ such that $\pi^* A \in \mathrm{Br}(X)$, hence $\pi^* A \in \mathrm{Br}(X) \cap \pi^* \mathrm{Br}(\mathbb{Q}(t)) = \mathrm{Br}_{\mathrm{vert}}(X)$. We want to show that $\pi^* A$ comes from $\mathrm{Br}(\mathbb{Q})$. The morphism π has a section $s_i : \mathbb{P}^1_{L_i} \to X \times_\mathbb{Q} L_i$ defined over L_i for each $i = 1, \dots, n$. By considering the image of π^*A under $\mathrm{Br}(X) \to \mathrm{Br}(X \times_{\mathbb{Q}} L_i) \to \mathrm{Br}(\mathbb{P}^1_{L_i})$, we see the restriction of π^*A to $\mathrm{Br}(L_i(t))$ comes from $\mathrm{Br}(\mathbb{P}^1_{L_i}) = \mathrm{Br}(L_i)$. In particular, the residues of A at the roots of $P(t)$ are in the kernel of the map $H^1(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \to H^1(L_i, \mathbb{Q}/\mathbb{Z})$. Since $L_1 \cap L_2 \dots L_n = \mathbb{Q}$ by assumption, there is no non-trivial cyclic extension of $\mathbb{Q}$ contained in all of the L_i. This implies that A is not ramified at the zero set of $P(t)$. (2.2.20) shows that A is unramified away from the zero set of $P(t)$. Hence $A \in \mathrm{Br}(\mathbb{A}^1) = \mathrm{Br}(\mathbb{Q})$. It follows that $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_0(X)} = X(\mathbb{A}_{\mathbb{Q}})$ and we are done. ☐

Proposition 5.3.6. *Let $P(t)$ be a product of (possibly repeated) linear factors over $\mathbb{Q}$, and let $a, b \in \mathbb{Q}^\times$. Let X be a smooth, proper and geometrically integral variety over $\mathbb{Q}$ with a morphism $\pi : X \to \mathbb{P}^1$ such that the generic fibre of π is binationally equivalent to the affine variety*

$$N_{\mathbb{Q}(\sqrt{a})|\mathbb{Q}}(\mathbf{x}) N_{\mathbb{Q}(\sqrt{b})|\mathbb{Q}}(\mathbf{y}) N_{\mathbb{Q}(\sqrt{ab})|\mathbb{Q}}(\mathbf{z}) = P(t)$$

over $\mathbb{Q}(\mathbb{P}^1) = \mathbb{Q}(t)$. Then $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$.

Proof. We can assume $\mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$ are quadratic fields, otherwise the variety X is rational and the statement is clear. Let V be the smooth locus of the affine variety $N_{\mathbb{Q}(\sqrt{a})|\mathbb{Q}}(\mathbf{x}) N_{\mathbb{Q}(\sqrt{b})|\mathbb{Q}}(\mathbf{y}) N_{\mathbb{Q}(\sqrt{ab})|\mathbb{Q}}(\mathbf{z}) = P(t)$ and let U be the image of V by the projection to the coordinate t. Then $\mathbb{P}^1 - U$ is a finite union of $\mathbb{Q}$-points. The fibres of $V \to U$ are principal homogeneous spaces of the torus T that is given by

$$N_{\mathbb{Q}(\sqrt{a})|\mathbb{Q}}(\mathbf{x}) N_{\mathbb{Q}(\sqrt{b})|\mathbb{Q}}(\mathbf{y}) N_{\mathbb{Q}(\sqrt{ab})|\mathbb{Q}}(\mathbf{z}) = 1.$$

Let E be a smooth equivariant compactification of T (which exists by [7]), and let $V^c = V \times^T E$ be the contracted product. Then $V^c \to U$ is a fibrewise smooth compactification of $V \to U$. We take $\pi : X \to \mathbb{P}^1$ such that $X \times_{\mathbb{P}^1} U = V^c$. We compose π with an automorphism of $\mathbb{P}^1$ to ensure that the fibre at infinity is smooth and is close to the real point that we need to approximate. In particular, the fibre at infinity contains a real point. A change of variables shows that X contains an open set which is the smooth locus of the affine variety given by

$$N_{\mathbb{Q}(\sqrt{a})|\mathbb{Q}}(\mathbf{x}) N_{\mathbb{Q}(\sqrt{b})|\mathbb{Q}}(\mathbf{y}) N_{\mathbb{Q}(\sqrt{ab})|\mathbb{Q}}(\mathbf{z}) = Q(t),$$

where $Q(t)$ is a polynomial with rational roots $e_1, \dots, e_r$ such that U is the complement to $\{e_1, \dots, e_r\}$ in $\mathbb{P}^1$. Note that for any $\tau \in U(\mathbb{Q})$, we have $X_\tau(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ by Proposition 5.1 in [5].

The quaternion algebra $A = (N_{\mathbb{Q}(\sqrt{a})|\mathbb{Q}}(\mathbf{x}), b)$ defines an element of $\mathrm{Br}(\pi^{-1}(U))$.

We are given points $(M_p) \in X(\mathbb{Q}_p)$ for all primes p and $M_0 \in X(\mathbb{R})$ such that $(M_p) \in X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_{\mathrm{vert}}}$. Since $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ is finite, we can replace (M_p) by a point arbitrarily close to it such that $\pi(M_p)$ is a point in $U \cap \mathbb{A}^1$ where t equals $\tau_p \in \mathbb{Q}_p$.

Let S_0 be the finite set of places of $\mathbb{Q}$ where we need to approximate. We can find a finite set S of places of $\mathbb{Q}$ containing S_0 and the real place such that $\pi : X \to \mathbb{P}^1$ extends to a proper morphism $\pi : \mathcal{X} \to \mathbb{P}^1_{\mathbb{Z}_S}$ with $\mathcal{X}$ regular. By doing so we can ensure that $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$ are unramified outside S, and that we have $a, b \in \mathbb{Z}_S$, $Q(t) \in \mathbb{Z}_S[t]$, and $e_i \in \mathbb{Z}_S$ for $i = 1, \dots, r$. By (2.4.12), we can further enlarge S such that

$$\sum_{p \in S} \mathrm{inv}_p(A(M_p)) = 0, \quad \sum_{p \in S} \mathrm{inv}_p(b, \tau_p - e_i) = 0, \; i = 1, \dots, r.$$

(For this we need to modify the points M_p for $p \in S - S_0$.) Let $\mathcal{U}$ be the complement to the Zariski closure of $e_1 \cup \dots \cup e_r$ in $\mathbb{P}^1_{\mathbb{Z}_S}$. The same algebra A defines a class in $\mathrm{Br}(\pi(\mathcal{U}))$. An application of (5.1.4) gives a $\mathbb{Q}$-point τ in $U \cap \mathbb{A}^1$ that is arbitrarily large in the real topology and is close to τ_p in the p-adic topology for the primes $p \in S$. For $p \notin S \cup \{p_1, \dots, p_r\}$ we see from property (3) of (5.1.4) that the Zariski closure of τ in $\mathbb{P}^1_{\mathbb{Z}_S}$ is contained in $\mathcal{U} \times_{\mathbb{Z}_S} \mathbb{Z}_p$. This implies that for any $N_p \in X_\tau(\mathbb{Q}_p)$ the value $A(N_p) \in \mathrm{Br}(\mathbb{Q}_p)$ comes from $\mathrm{Br}(\mathbb{Z}_p)$. From property (5) we see that for each $i = 1, \dots, r$, the primes p_i splits in $\mathbb{Q}(\sqrt{b})$ and hence $A(N_{p_i}) = 0$ for any $N_{p_i} \in X_\tau(\mathbb{Q}_{p_i})$. By continuity and the inverse function theorem we can find $N_p \in X_\tau(\mathbb{Q}_p)$

arbitrarily close to M_p for $p \in S$, so that $\sum_{p\in S} \mathrm{inv}_p(A(N_p)) = 0$. Summing over all places of $\mathbb{Q}$ we now have $\sum_p \mathrm{inv}_p(A(N_p)) = 0$ for any choice of N_p, $p \notin S$. By Theorem 4.1 in [5], the algebra A generated $\mathrm{Br}(X_\tau)$ modulo the image of $\mathrm{Br}(\mathbb{Q})$. By Chapter 8 in [41], the set $X_\tau(\mathbb{Q})$ is dense in $X_\tau(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$, so we can find a $\mathbb{Q}$-point in X_τ arbitrarily close to M_p for $p \in S$. $\square$

5.3.3 Non-cyclic extensions of prime degree

Theorem 5.3.7. *Let $P(t)$ be a product of (possibly repeated) linear forms over $\mathbb{Q}$. Let K be a non-cyclic extension of $\mathbb{Q}$ of prime degree such that the Galois group of the normal closure of K over $\mathbb{Q}$ has a non-trivial abelian quotient. Let X be a smooth, proper and geometrically integral variety over $\mathbb{Q}$ with a morphism $\pi : X \to \mathbb{P}^1$ such that the generic fibre of π is birationally equivalent to the affine variety $N_{K|\mathbb{Q}}(\mathbf{x}) = P(t)$ over $\mathbb{Q}(t)$. Then X satisfies the Hasse principle and weak approximation.*

Proof. We can assume that X contains an open set which is the smooth locus of the affine variety $N_{K|\mathbb{Q}}(\mathbf{x}) = Q(t)$, where $Q(t)$ is a product of powers of $t - e_i$ for $i = 1, \dots, r$ with the additional assumption that the fibre at infinity is smooth and contains a real point close to the real point that we want to approximate.

Step 1. We claim $\mathrm{Br}(X) = \mathrm{Br}_0(X)$.

Let T be the norm torus $N_{K|\mathbb{Q}}(\mathbf{x}) = 1$. Since $\ell = [K : \mathbb{Q}]$ is a prime number, it follows by [10] (Prop. 9.1 and Prop. 9.5) that

$$H^1(F, \mathrm{Pic}(Z \times_F \overline{F}) = Ш^2_\omega(F, \hat{T}) = 0$$

for any smooth and proper variety Z over a field F such that a dense open subset of Z is a principal homogeneous space of T. Applying this to the generic fibre of $\pi : X \to \mathbb{P}^1$, we see that $\mathrm{Br}(X) = \mathrm{Br}_{\mathrm{vert}}(X)$.

Now let $A \in \mathrm{Br}(\mathbb{Q}(t))$ be such that $\pi^* A \in \mathrm{Br}(X)$. The morphism π has a section defined over K. By restricting to it we see that the image of A in $\mathrm{Br}(K(t))$ belongs to the injective image of $\mathrm{Br}(\mathbb{P}^1_K) = \mathrm{Br}(K)$. In particular, the residue of A at e_i lies in the kernel of the map

$$H^1(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \to H^1(K, \mathbb{Q}/\mathbb{Z}).$$

Since $[K : \mathbb{Q}] = \ell$ is a prime number, K contains no cyclic extension of $\mathbb{Q}$ and hence the above kernel is zero. Thus A is not ramified at the zero set of $Q(t)$. Since A is also unramified outside the zero set of $Q(t)$, we conclude $A \in \mathrm{Br}(\mathbb{Q})$. $\square$

Let L be the normal closure of $K|\mathbb{Q}$. By assumption there exists a cyclic extension $k|\mathbb{Q}$ of prime degree such that $k \subset L$. Let $q = [k : \mathbb{Q}]$. Since $\mathrm{Gal}(L|\mathbb{Q}) \subset S_\ell$ and $k \neq K$, it follows $q < l$.

Step 2. Let $a \in \mathbb{Q}^\times$. If p is a prime unramified in L and inert in k, then the equation $N_{K|\mathbb{Q}}(\mathbf{x}) = a$ is solvable in $\mathbb{Q}_p$.

Write $K \otimes_\mathbb{Q} \mathbb{Q}_p = K_{v_1} \oplus \cdots \oplus K_{v_s}$ and let $d_i = [K_{v_i} : \mathbb{Q}_p]$.

If $s > 1$, then $\ell = d_1 + \cdots + d_s$ is a prime number implies there exist integers $n_1, \dots, n_s$ such that $1 = n_1 d_1 + \cdots + n_s d_s$. If follows that

$$a = \prod_{i=1}^{s} N_{K_{v_i}|\mathbb{Q}_p}(a^{n_i}) \in N_{K|\mathbb{Q}}(K \otimes_\mathbb{Q} \mathbb{Q}_p),$$

so we are done.

If $s = 1$, then $K \otimes_\mathbb{Q} \mathbb{Q}_p = K_v$ is a field extension of $\mathbb{Q}_p$ of degree ℓ. By assumption p is inert in k, so that $k \otimes_\mathbb{Q} \mathbb{Q}_p = k_w$ is a field. Since $[k_w : \mathbb{Q}_p] = q$ is a prime less than ℓ, the fields k_w and K_v are linearly disjoint over $\mathbb{Q}_p$, so that $k_w K_v$ is a field. Thus p is inert in $kK \subset L$, which implies that the Frobenius at p in $\mathrm{Gal}(L|\mathbb{Q})$ is an element of order divisible by ℓq. However, S_ℓ contains no such elements, so the case $s = 1$ is impossible. $\square$

Step 3. Now we conclude the assertion. Let the point M given by $M_p \in X(\mathbb{Q}_p)$ for all primes p and $M_0 \in X(\mathbb{R})$ be the point we need to approximate. By replacing M with a point arbitrarily close to M, we may assume $\pi(M_p) \in U \cap \mathbb{A}^1$ where t equals $\tau_p \in \mathbb{Q}_p$. Let S be the finite set of places of $\mathbb{Q}$ where we need to approximate, containing the real place and the primes of bad reduction for X. We also assume that L is unramified over any $p \notin S$. Consider the cyclic algebras

$$A_i = (k|\mathbb{Q}, t - e_i) \in \mathrm{Br}(\mathbb{Q}(X))$$

for $i = 1, \ldots, r$. By Harari's formal lemma and Step 1, we can enlarge S to S' and choose $M_p \in X(\mathbb{Q}_p)$ for $p \in S' - S$ such that

$$\sum_{p \in S} \mathrm{inv}_p(A_i(\tau_p)) \neq 0$$

for $i = 1, \ldots, r$. Now we apply (5.1.4) and we obtain a $\mathbb{Q}$-point τ in $U \cap \mathbb{A}^1$ that is arbitrarily large in the real topology and is arbitrarily close to τ_p in the p-adic topology for the primes $p \in S$. This ensures that $X_\tau(\mathbb{R}) \neq \emptyset$ and $X_\tau(\mathbb{Q}_p) \neq \emptyset$ for all $p \in S$. For $p \notin S \cup \{p_1, \ldots, p_r\}$, we see from property (3) of (5.1.4) that τ reduces modulo p to a point of $\mathbb{P}^1(\mathbb{F}_p)$ other that the reduction of any of $e_1, \ldots, e_r$. The corresponding fibre over $\mathbb{F}_p$ contains a principal homogeneous space of a torus over a finite field, and hence an $\mathbb{F}_p$-point by Lang's theorem. By Hensel's lemma it gives rise to a $\mathbb{Q}_p$-point in X_τ. Finally, property (5) of (5.1.4) implies that $\mathrm{inv}_{p_i}(A_i(\tau)) \neq 0$. By property (4), this implies that p_i is inert in k. Now Step 2 applies and we conclude $X_\tau(\mathbb{Q}_{p_i}) \neq \emptyset$. This holds for all $i = 1, \ldots, r$ and hence $X_\tau(\mathbb{A}_\mathbb{Q}) \neq \emptyset$. $Ш^2_\omega(\mathbb{Q}, \hat{T}) = 0$ implies that the principal homogeneous space of T over $\mathbb{Q}$ satisfy the Hasse principle and weak approximation by Chapter 8 in [41]. $\square$

Index

Bibliography

[1] M. Borovoi. *Abelian Galois cohomology of reductive groups*. Number 626. American Mathematical Society, 1998.

[2] S. Bosch, W. Lütkebohmert, and M. Raynaud. Néron models, ergeb. math. grenzgeb. 21, 1990.

[3] T.D. Browning, L. Matthiesen, and A.N. Skorobogatov. Rational points on pencils of conics and quadrics with many degenerate fibres. *Annals of Mathematics*, 180:381–402, 2014.

[4] J.W.S. Cassels and A. Fröhlich. Algebraic number theory. 1967.

[5] J.-L. Colliot-Thélène. Groupe de Brauer non ramifié d'espaces homogènes de tores. *Journal de Théorie des Nombres de Bordeaux*, 26(1):69–83, 2014.

[6] J.-L. Colliot-Thélène, D. Coray, and J.-J. Sansuc. Descente et principe de Hasse pour certaines variétés rationnelles. *Journal für die reine und angewandte Mathematik*, 320:150–191, 1980.

[7] J.-L. Colliot-Thélène, D. Harari, and A.N. Skorobogatov. Compactification équivariante d'un tore (d'apres Brylinski et Künnemann). *Expositiones mathematicae*, 23(2):161–170, 2005.

[8] J.-L. Colliot-Thélène and M. Ojanguren. Variétés unirationnelles non rationnelles: au-delà de l'exemple d'Artin et Mumford. *Inventiones mathematicae*, 97(1):141–158, 1989.

[9] J.-L. Colliot-Thélène and J.-J. Sansuc. La descente sur les variétés rationnelles, II. *Duke Mathematical Journal*, 54(2):375–492, 1987.

[10] J.-L. Colliot-Thélène and J.-J. Sansuc. Principal homogeneous spaces under flasque tori: applications. *Journal of Algebra*, 106(1):148–205, 1987.

[11] J.-L. Colliot-Thélène, J.-J. Sansuc, and P Swinnerton-Dyer. Intersections of two quadrics and Châtelet surfaces. I. *Journal für die reine und angewandte Mathematik*, 373:37–107, 1987.

[12] J.-L. Colliot-Thélène and A.N. Skorobogatov. Descent on fibrations over $\mathbb{P}^1_k$ revisited. 128(03):383–393, 2000.

[13] J.-L. Colliot-Thélène, A.N. Skorobogatov, and P. Swinnerton-Dyer. Rational points and zero-cycles on fibred varieties: Schinzel's hypothesis and Salberger's device. *Journal für die reine und angewandte Mathematik*, 495:1–28, 1998.

[14] J.-L. Colliot-Thélène and P. Swinnerton-Dyer. Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties. *Journal für die reine und angewandte Mathematik*, 453:49–112, 1994.

[15] A.J. de Jong. A result of Gabber. Preprint with missing references about $\mathrm{Br} = \mathrm{Br}'$ on quasi-projective schemes.

[16] C. Demarche and D. Wei. Hasse principle and weak approximation for multinorm equations. *Israel Journal of Mathematics*, 202(1):275–293, 2014.

[17] E. Frossard. Fibres dégénérées des schémas de Severi–Brauer d'ordres. *Journal of Algebra*, 198(2):362–387, 1997.

[18] L. Fu. *Étale cohomology theory*, volume 13. World Scientific, 2011.

[19] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 165. Cambridge University Press, 2017.

[20] B. Green and T. Tao. Linear equations in primes. *Annals of Mathematics*, pages 1753–1850, 2010.

[21] B. Green and T. Tao. The Möbius function is strongly orthogonal to nilsequences. *Annals of Mathematics*, 175(2):541–566, 2012.

[22] B. Green, T. Tao, and T. Ziegler. An inverse theorem for the gowers $u^{s+1}[n]$-norm. *Annals of Mathematics*, 176(2):1231–1372, 2012.

[23] A. Grothendieck. *Le groupe de Brauer. I, II, III. In: Dix exposés sur la cohomologie des schémas.* N. H. Kuipers, eds. North-Holland, 1968.

[24] D. Harari. Méthods des fibrations et obstruction de Manin. *Duke Mathematical Journal*, 75(1):221–260, 1994.

[25] D. Harari. Flèches de spécialisation en cohomologie étale et applications arithmétiques. *Bulletin de la Société Mathématique de France*, 125(2):143–166, 1997.

[26] Y. Harpaz, A.N. Skorobogatov, and O. Wittenberg. The Hardy-Littlewood conjecture and rational points. *Compositio Mathematica*, 150(12):2095–2111, 2014.

[27] Y. Harpaz and O. Wittenberg. On the fibration method for zero-cycles and rational points. *Annals of Mathematics*, 183(1):229–295, 2016.

[28] R. Hartshorne. *Algebraic Geometry.* Number 52. Springer Science & Business Media, 1977.

[29] V.A. Iskovskih. Rational surfaces with a pencil of rational curves and with positive square of the canonical class. *Mathematics of the USSR-Sbornik*, 12(1):91–117, 1970.

[30] J. Kollár. *Lectures on resolution of singularities (AM-166).* Princeton University Press, 2009.

[31] S. Lang. On quasi algebraic closure. *Annals of Mathematics*, pages 373–390, 1952.

[32] S. Lang. Algebraic groups over finite fields. *American Journal of Mathematics*, 78(3):555–563, 1956.

[33] S. Lang. *Algebraic number theory*, volume 110. Springer, 2013.

[34] Q. Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6. Oxford University Press, 2006.

[35] L. Matthiesen. Linear correlations amongst numbers represented by positive definite binary quadratic forms. *Acta Arithmetica*, 3(154):235–306, 2012.

[36] L. Matthiesen. Correlations of representation functions of binary quadratic forms. *Acta Arithmetica*, 3(158):245–252, 2013.

[37] J.S. Milne. *Étale Cohomology (PMS-33).* Number 33. Princeton University Press, 1980.

[38] J.S. Milne. *Arithmetic duality theorems.* Citeseer, 2006.

[39] J. Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[40] B. Poonen. *Rational points on varieties.* Available on https://math.mit.edu/ poonen/papers.

[41] J.-J. Sansuc. Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. *Journal für die reine und angewandte Mathematik*, 327:12–80, 1981.

[42] J.-P. Serre. *Lie Algebras and Lie Groups: 1964 Lectures Given at Harvard University*, volume 1500. Springer, 1965.

[43] J.-P. Serre. *Local fields.* Springer, 1979.

[44] J.-P. Serre. *Cohomologie galoisienne*, volume 5. Springer, 1997.

[45] A.N. Skorobogatov. Arithmetic on certain quadric bundles of relative dimension 2. I. *Journal für die reine und angewandte Mathematik*, 407:57–74, 1990.

[46] A.N. Skorobogatov. Descent on fibrations over the projective line. *American Journal of Mathematics*, pages 905–923, 1996.

[47] A.N. Skorobogatov. *Torsors and rational points*, volume 144. Cambridge University Press, 2001.

[48] G. Tamme. *Introduction to Étale cohomology.* Springer, 1994.

[49] C. Weibel. *An introduction to homological algebra.* Number 38. Cambridge university press, 1995.