Algebraic and Arithmetic Geometry

Lectures by Caucher Birkar
Notes by Tony Feng

Lent 2014
## Contents

1 Introduction ..................................................... 7
   1.1 Rational points on varieties .............................. 7
   1.2 Dimension one ........................................... 8
   1.3 Higher dimensions ...................................... 8
   1.4 General strategies ..................................... 9

2 Heights ......................................................... 11
   2.1 Valuations .................................................. 11
   2.2 Heights on projective space .............................. 13
   2.3 The Weil height machine on varieties .................... 16
   2.4 Height theory over function fields ....................... 21

3 Arakelov Geometry .............................................. 25
   3.1 Hermitian metrics on line bundles ...................... 25
   3.2 Line bundles on number fields .......................... 26

4 Abelian Varieties .............................................. 29
   4.1 Abelian varieties over algebraically closed fields .... 29
   4.2 Abelian varieties over number fields ................... 31
   4.3 Torsion points ........................................... 33
   4.4 Weak Mordell-Weil ..................................... 34

5 The Brauer-Manin Obstruction ................................ 37
   5.1 Chevalley's Theorem .................................... 37
   5.2 Tsen's Theorem ........................................ 38
   5.3 Brauer- Severi varieties ................................ 39
   5.4 The Brauer group ...................................... 41
   5.5 The Brauer-Manin obstruction .......................... 42

6 Birational Geomery ............................................. 45
   6.1 Potential density ....................................... 45
   6.2 Kodaira dimension ..................................... 46
   6.3 Surface fibrations ...................................... 46
## CONTENTS

### 7 Statistics of Rational Points
7.1 Counting on projective space ........................................ 51
7.2 Counting on abelian varieties ...................................... 53
7.3 Jacobians of curves .................................................. 54

### 8 Zeta functions
8.1 The Hasse-Weil zeta function ..................................... 55
8.2 The Frobenius Morphism ............................................. 58
8.3 The Weil conjectures for curves ................................... 58
8.4 Zeta functions of arithmetic schemes ............................. 61
Disclaimer

These are lecture notes originally "live-\TeX ed" for a course offered by Caucher Birkar at Cambridge University in Lent 2014. They have been very lightly edited by me. I take full responsibility for all errors.
Chapter 1

Introduction

1.1 Rational points on varieties

Algebraic geometry is about studying solutions of polynomials. Consider polynomials

\[ F_1, \ldots, F_m \in k[x_1, x_2, \ldots]. \]

Classically, mathematicians were most interested in the case \( k = \mathbb{Q} \), but they were naturally led to expand considerations to number fields, finite fields, function fields, etc. Diophantine geometry is the study of algebraic geometry over these special fields.

**Example 1.1.1.** Consider the polynomial \( F(x, y) = x^2 + y^2 \in \mathbb{Q}[x, y] \). Over \( \mathbb{Q} \), the only solution is \((0, 0)\). What happens if we extend our domain field? In this case, we get no additional points over \( \mathbb{R} \), but we do get lots of points over \( \mathbb{C} \).

**Example 1.1.2.** Consider the polynomial \( F(x, y, z) = x^2 + y^2 - 7z^2 \in \mathbb{Q}[x, y, z] \) cutting out a variety. What are its rational points?

We claim that over \( \mathbb{Q} \), the only solution is \((0, 0, 0)\). Why? Suppose that \((a, b, c)\) is a rational solution. By clearing denominators, we may assume that \(a, b, c \in \mathbb{Z}\). Reducing mod 7, we must have \(a^2 + b^2 \equiv 0 \pmod{7}\). The only squares in \( \mathbb{F}_7 \) are 0, 1, 4, so it must be the case that \(7 \mid a\) and \(7 \mid b\). Then \(7 \mid c\) as well, and we are done (e.g. by induction).

**Example 1.1.3.** Consider \( F(x, y, z) = x^5 + y^5 - 7z^5 \in \mathbb{Q}[x, y, z] \). It is an open problem whether or not this has nontrivial positive rational solutions.

**Example 1.1.4.** Consider \( F(x, y, z) = x^2 + y^2 - z^2 \in \mathbb{Q}[x, y, z] \). All rational solutions can be described explicitly. This is explained by the geometric fact that \( F \) cuts out \( \mathbb{P}_\mathbb{Q}^1 \) in the projective plane.

**General setup.** Let \( k \) be a field, \( X \subset \mathbb{P}_k^n \) a projective variety over \( k \). Then \( X = V(F_1, \ldots, F_m) \), where \( F_1, \ldots, F_m \in k[t_0, \ldots, t_n] \). We should think of \( X \) as a scheme, not just a set of solutions. For any field extension \( k'/k \), we can consider the \( k' \) points of \( X \), \( X(k') \). We are interested in the following questions:
1. Is $X(k')$ empty?

2. Is $X(k')$ is dense (in the Zariski topology)?

3. If $X(k')$ is dense, how are its points distributed?

### 1.2 Dimension one

Let $X$ be a smooth, projective variety of dimension one over a number field $K$. There is a very important invariant associated to $X$, which is the genus. This can be defined as

$$g = h^0(\omega_X) = h^1(O_X).$$

Let’s consider some possibilities for low genus.

1. $g = 0$. Either $X(K) = \emptyset$ or it is infinite, and infinite - in fact, isomorphic to $\mathbb{P}^1(K)$.

2. $g = 1$. $X$ is an elliptic curve, and $X(K)$ forms a finitely generated abelian group (this is the Mordell-Weil theorem).

3. $g \geq 2$. Then $X(K)$ is finite (a deep theorem of Faltings).

Note that if $g = 0$, $\omega_X^{-1}$ is ample. If $g = 1$, then $\omega_X$ is trivial, and if $g \geq 2$, then $\omega_X$ is ample. So we see that the geometric properties of $X$ seem to determine its arithmetic. This is a general philosophy.

### 1.3 Higher dimensions

The situation is much more complicated. There are a few kinds of varieties with extra structure that makes them more tractable:

1. Varieties “close to projective space.” For instance, rational varieties are those which (by definition) are birational to projective space.

2. Abelian varieties. This form the nicest case, and the Mordell-Weil theorem offers some control of $X(K)$. The next few lectures will be devoted to proving Mordell-Weil.

Here are a few conjectures that express the philosophy “geometry determines arithmetic.”

**Conjecture 1.3.1** (Lang). Let $X$ be a smooth, projective variety over a number field $K$. If $\omega_X$ is ample, then $X(K)$ is not dense.

Note that this implies Faltings's theorem in the case of a curve.
Conjecture 1.3.2 (Campana). If $\omega_X \simeq \Omega_X$ or $\omega_X$ is anti-ample, then $X(K')$ is dense for some finite extension $K'/K$.

Example 1.3.3. If $X = V(F)$ is a hypersurface in $\mathbb{P}^n_k$, then $\omega_X$ is ample if and only if $d > n + 1$, trivial if $d = n + 1$, and anti-ample if $d < n + 1$.

1.4 General strategies

It is difficult to provide a uniform theory for rational points on varieties. Here are some general strategies/remarks that can be useful. Let $X$ be a smooth projective variety over $\mathbb{Q}$. We are interested in $X(\mathbb{Q})$, which can be difficult to understand.

- One can study $X(\mathbb{R})$, which is a smooth manifold, by using the techniques of differential geometry. One can also look at $X(\mathbb{F}_p)$. This is described by the Weil conjectures. Sometimes, piecing this data together can give information about $X(\mathbb{Q})$ (the local-global principle).

- There is a natural action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $X(\overline{\mathbb{Q}})$. From this we get Galois representations, and we can try to think of $X(\mathbb{Q})$ as the fixed part.
CHAPTER 1. INTRODUCTION
Chapter 2

Heights

2.1 Valuations

Definition 2.1.1. Let $k$ be a field. An absolute value is a function $|·| : k \to \mathbb{R}^{\geq 0}$ such that

- $|x| = 0 \iff x = 0$,
- $|xy| = |x||y|$,
- $|x + y| \leq |x| + |y|$.

If the stronger condition $|x + y| \leq \max\{|x|, |y|\}$ holds, then we say that the absolute value is non-Archimedean. Otherwise, it is Archimedean.

Example 2.1.2. For $K = \mathbb{Q}$, we have the usual absolute value

$$|n|_{\infty} = \max\{x, -x\}.$$ 

This is archimedean. There are also non-archimedean absolute values, constructed as follows. Fix any prime $p \in \mathbb{Z}$. Then for $x = p^{k/a}b$, where $p \nmid ab$, we set $|x| = p^{-k}$.

We let

$$M_{\mathbb{Q}} = \{\text{places of } \mathbb{Q}\} = \{|·|_{\infty}, |·|_p : p \text{ prime}\}.$$ 

If $K$ is a number field, then there are $n = [K : \mathbb{Q}]$ embeddings $\sigma : K \hookrightarrow \mathbb{C}$. For each embedding $\sigma$, we get a different absolute value (the pullback of the complex absolute value). If $\sigma(K) \subset \mathbb{R}$, then $\sigma$ and $\overline{\sigma}$ are distinct embeddings with $|·|_\sigma = |·|_{\overline{\sigma}}$.

Let $R = \mathcal{O}_K$ be the ring of integers of $K$. Pick a non-zero prime ideal $\mathfrak{p} \subset R$. Since $\mathcal{O}_K$ is a Dedekind domain, $\mathfrak{p}$ is a maximal ideal. Moreover, $R_\mathfrak{p}$ is a discrete valuation ring, and its valuation extends to an order function

$$\text{ord}_\mathfrak{p} : K^* \to \mathbb{Z}$$.
Explicitly, if \( x \) is a uniformizer for \( R_p \), then any \( x \in K^* \) may be written as \( t^m u \) where \( u \in R^*_p \), and then \( \text{ord}_p(x) = m \). Now let \( (p) = \mathbb{Z} \cap P \) and let \( e = \text{ord}_p(p) \). Define

\[
|x|_p = \begin{cases} 
0 & \text{if } x = 0 \\
 p^{-\text{ord}_p(p)/e} & \text{if } x \neq 0.
\end{cases}
\]

We denote by \( M_K \) the places of \( K \), which include both archimedean and non-archimedean places. For \( v \in M_K \), the distance function

\[
d(x, y) := |x - y|_v
\]

makes \( K \) into a metric space. We let \( K_v \) to be the completion of \( K \) with respect to this metric. If \( v \) is archimedean corresponding to \( d : K \to \mathbb{C} \), then \( K_v = \mathbb{R} \) or \( \mathbb{C} \), depending on whether or not the corresponding embedding lands in \( \mathbb{R} \). If \( v \) is nonarchimedean, corresponding to some prime ideal \( p \subset R \), then \( R \subset R_p \subset K \). The completion is defined algebraically as

\[
\hat{R}_p = \lim_{\leftarrow} R_p / p^n
\]

and \( K_v = \text{Frac}(\hat{R}_p) \). This is equivalent to the analytic completion.

The algebraic geometry motivation is as follows: if \( X \) is a scheme and \( p \in X \) a point, then a Zariski open neighborhood of \( p \) is very coarse. In contrast, \( \text{Spec} \hat{O}_{X,p} \) behaves like an “analytic neighborhood,” capturing local data.

**Definition 2.1.3.** Let \( K \subset K' \) be number fields. Suppose that \( w \in M_K \), \( v \in M_{K'} \) are two places such that

\[
|\cdot|_{v, K} = |\cdot|_{w}.
\]

Then the **local degree** of \( v \) over \( w \) is \( [K'_v : K_w] \).

If \( R \) is the ring of integers of \( K \) and \( R' \) the ring of integers of \( K' \), then the geometric picture is that we have a map \( \pi : \text{Spec } R' \to \text{Spec } R \), sending \( v \mapsto w \). This induces a pullback map \( \pi^* \) on divisors, with the property that

\[
\deg \pi^* w = \sum_{v_i \mapsto w} [K'_{v_i} : K_w].
\]

This leads to the following result.

**Proposition 2.1.4.** If \( v_1, \ldots, v_r \in M_{K'} \) are the places of \( K' \) lying over a place \( w \) of \( K \), then

\[
[K' : K] = \sum_{i=1}^r [K'_{v_i} : K_w].
\]

**Definition 2.1.5.** Let \( K \) be a number field, \( v \in M_K \), lying over \( w \in M_{\mathbb{Q}} \). Let \( n_v = [K_v : \mathbb{Q}_w] \). Then we define the **normalized absolute value**

\[
||x||_v = |x|_v^{n_v}.
\]
It turns out that \( n_v = ef \), where \( f = [k_v : \mathbb{F}_p] \) is residue extension degree. So another way of writing the normalized absolute value is as
\[
||x||_v = (\#k_v)^{-\text{ord}_v(x)}.
\]

**Proposition 2.1.6 (Product formula).** Let \( K \) be a number field. Then for all non-zero \( x \in K \),
\[
\prod_{v \in M_K} ||x||_v = 1.
\]

**Proof sketch.** Fix \( w \in M_\mathbb{Q} \) and let \( v_1, \ldots, v_r \in M_K \) be the places lying over \( w \). Then we have
\[
\prod_{i=1}^{r} ||x||_{v_i} = ||N_{K/\mathbb{Q}}x||_w.
\]
The result then follows from the product formula for \( \mathbb{Q} \), which is trivial. \( \square \)

**Remark 2.1.7.** This is analogous to the geometric fact that if \( \pi : X \to Y \) is a map of schemes, then \( \pi_* \text{div}(f) = \text{div}(N_{X/Y}(f)) \)

## 2.2 Heights on projective space

Our goal is to define a **height**, which is a kind of measure of complexity, on the points of a variety.

**Definition 2.2.1.** Let \( K \) be a number field, \( x = [a_0 : \ldots : a_n] \in \mathbb{P}^n(K) \). We define the **naïve height** of \( x \) to be
\[
H_K(x) = \prod_{v \in M_K} \max\{||a_i||_v\}.
\]

By the product formula, this is well-defined. From this it is easy to see that \( H_K(x) \geq 1 \), because we can assume that \( a_i = 1 \) for some \( i \).

**Example 2.2.2.** Consider \( K = \mathbb{Q} \). Let \( x = [a_0 : \ldots : a_n] \in \mathbb{P}^n(\mathbb{Q}) \). By scaling appropriately, we can assume that the \( a_i \) are integers, with no common factor. Then for each non-archimedean place \( v \), \( \max\{||a_i||_v\} = 1 \). So at the end of the day, we have \( H_\mathbb{Q}(x) = \max |a_i|_\infty \). Thus we see that the height is very simple over \( \mathbb{Q} \).

**Theorem 2.2.3.** Let \( K \) be a number field, \( x = [a_0 : \ldots : a_n] \in \mathbb{P}^n(K) \). Let \( R \) be the ring of integers of \( K \), and assume without loss of generality that all \( a_i \in R \). Let \( I = (a_0, \ldots, a_n) \). Then we have
\[
\prod_{v \in M_K, v \nmid \infty} \max\{||a_i||_v\} = \frac{1}{N_{K/\mathbb{Q}}(I)}.
\]
Proof. For any nonarchimedean $v \in M_K$,

$$\max \{|a_i|_v\} = \max \left\{ \frac{1}{\sum_{v|w} n_v/ n_w} \right\} = \frac{1}{(\# k_v)_{\text{ord}_v}} = \frac{1}{(\# k_v)_{\text{ord}_v(I)}}.$$ 

Now, we have a unique prime factorization for ideals, $I = p_1^{m_1} \ldots p_r^{m_r}$. So

$$\prod_{p} \frac{1}{(\# k_v)_{\text{ord}_v(I)}} = \prod_{p} \frac{1}{(R/p^{m_r})} = \frac{1}{(R/I)}.$$ 

Of course, $(R/I) = N_{K'/\mathbb{Q}}(I)$.

**Example 2.2.4.** Consider $K = \mathbb{Q}$, $x = [1 : 2] \in \mathbb{P}^1(\mathbb{Q})$. Then the ideal is $I = (1, 2) = R$, so $N(I) = 1$ and $H_{\mathbb{Q}}(x) = 2$. The only contribution to the height is from the Archimedean places, which we already knew. More generally, this will be true for any field with class number 1.

**Example 2.2.5.** Consider $K = \mathbb{Q}(i)$, $x = [1 : 2] \in \mathbb{P}^1(K)$. Again we have $N(I) = 1$. For a complex place $v$, we have $|2|_v = |2|^2 = 4$ so that $H_K(x) = 2$. In particular, we see that the height of a point depends on the field we are considering.

**Theorem 2.2.6.** Let $K \subset K'$ be an extension of number fields, $x \in \mathbb{P}^n(K)$. Then we have

$$H_{K'}(x) = H_K(x)^{[K':K]}.$$ 

**Proof.** This is a simple application of the degree formula

$$[K':K] = \sum_{v|w} n_v.$$ 

We have

$$H_{K'}(x) = \prod_{v \in M_{K'}} \max \{|a_i|_v\} = \prod_{w \in M_K} \frac{\prod \max \{|a_i|_w^{n_v}\}}{\prod \max \{|a_i|_w^{n_w}\}} = \prod_{w \in M_K} \max \{|a_i|_w^{\sum_{v|w} n_v/n_w}\} = \left( \prod_{w \in M_K} \max \{|a_i|_w^n\} \right)^{[K':K]}.$$
2.2. HEIGHTS ON PROJECTIVE SPACE

This computation motivates the definition:

Definition 2.2.7 (Absolute height). If $K$ is a number field and $x \in \mathbb{P}^n(\mathbb{Q})$, then we define the absolute height of $x$ to be

$$H(x) = H_K(x)^{1/[K:Q]}$$

where $K$ is any number field over which $x$ is defined. By Theorem 2.2.6, this is well-defined.

We also define

$$h(x) := \log H(x)$$

which is an additive version of the height. Finally, for any $a \in K$ we define $h(a) := h(1:a)$.

Theorem 2.2.8 (Northcott). Let $B,D \in \mathbb{N}$. Then the set

$$\{x = [a_0: \ldots : a_n] \in \mathbb{P}^n(\mathbb{Q}) : H(x) \leq B, [\mathbb{Q}(x): \mathbb{Q}] \leq D\}$$

is finite, where $\mathbb{Q}(x) = \mathbb{Q}(\{a_i/a_j\})$.

Proof. We can assume that $a_j = 1$ for some $j$. Then for all $i$ and all $v \in M_K$, we have

$$B \geq \max\{||a_i||_v\} \geq \max\{||a_i||_v, 1\}.$$ 

Taking the product over $v$, we get $H(x) \geq H(a_i)$ for any individual $i$. Now, it suffices to show that there are finitely many possibilities for the $a_i$, i.e. for all $1 \leq \ell \leq D$ and all $B,D \in \mathbb{N}$,

$$\#\{a \in \mathbb{Q} | H(a) \leq B, [\mathbb{Q}(a): \mathbb{Q}] \leq \ell\} < \infty.$$

Let $K = \mathbb{Q}(a)$ and let $b_1 = a, \ldots, b_\ell$ be the $n$ conjugates of $a$, i.e. the roots of the minimal polynomial for $a$ over $\mathbb{Q}$,

$$f(t) = (t - b_1) \ldots (t - b_\ell).$$

To show that there are finitely many possibilities for the $a$’s, it suffices to show that there are finitely many possibilities for $f$. For that, it suffices in turn to show that there are finitely many possibilities for the coefficients of $f$. (This is basically a reduction to the case $K = \mathbb{Q}$.)

First of all, note that there are only finitely many coefficients, since the degree of $a$ is bounded. The coefficient of $t^r$ is $(-1)^r s_r(a)$, where $s_r(a)$ is the $r$th elementary symmetric polynomial in $b_1, \ldots, b_\ell$. We want to give a bound for coefficients.

$$|s_r(a)|_v = |\sum b_{i_1} \ldots b_{i_r}|_v \leq \sum |b_{i_1} \ldots b_{i_r}|_v \leq C(r,v) \max\{|b_i|_v^r\}.$$ 

The constant $C(r,v)$ can be taken to be $\binom{\ell}{r}$ if $v$ is Archimedean, and 1 otherwise. So then

$$\max\{|s_0(a)|_v^n, \ldots, |s_\ell(a)|_v^n\} \leq C(r,v)^n \max\{|b_i|_v^n, 1\}.$$ 

15
CHAPTER 2. HEIGHTS

Taking the product over all $v \in M_K$, we get an inequality of the form

$$H_K([s_0(a): \ldots: s_\ell(a)]) \leq C \prod H_K(b_i)^\ell.$$  

Since the $b_i$ are conjugates, $H(b_i) = H(b_0) = H(a)$ for all $i$.

This implies that the heights of the $s_i(a)$ are bounded, and it is easy to check that there are finitely many rational numbers with bounded height. \hfill \square

Example 2.2.9. If $K$ is a number field, $x = [a_0: \ldots : a_n] \in \mathbb{P}^n(K)$. Then $H(x) = 1 \iff$ all the $a_i$ are roots of unity.

2.3 The Weil height machine on varieties

We now extend the notion of height to more general settings.

Let $X$ be a projective variety over $\mathbb{Q}$ and $\varphi : X \to \mathbb{P}^n_{\mathbb{Q}}$ be a morphism. Set

$$h_{\varphi}(x) = h(\varphi(x)).$$

Theorem 2.3.1 (Weil). Let $X$ be smooth and projective over $\overline{\mathbb{Q}}$. Then we have a homomorphism of groups

$$\text{Pic}(X) \to \mathcal{H}(X) := \frac{\{\text{functions } f : X(\overline{\mathbb{Q}}) \to \mathbb{R}\}}{\{\text{bounded functions}\}}$$

denoted $L \mapsto h_L$, such that

1. if $\varphi : X \to \mathbb{P}^n$ is a morphism and $L = \varphi^*H$, where $H$ is a hyperplane, then $h_L = h\varphi$, and

2. if $\pi : Y \to X$ is a morphism of smooth, projective varieties, then the pullback diagram commutes:

$$\begin{CD}
\text{Pic}(X) @> \pi^* >> \text{Pic}(Y) \\
@V \mathcal{H}(X) VV @VV \mathcal{H}(Y) V \\
\mathcal{H}(X) @> \pi^* >> \mathcal{H}(Y)
\end{CD}$$

We work towards this result, first establishing some useful technical estimates.

Proposition 2.3.2. Let $\varphi : \mathbb{P}^n \to \mathbb{P}^m$ be a rational map of degree $d$, with base locus $Z$.

1. If $x \in \mathbb{P}^n \setminus Z(\overline{\mathbb{Q}})$,

$$h(\varphi(x)) \leq dh(x) + c_\varphi.$$
2. If $X \subset \mathbb{P}^n$ is a closed subvariety disjoint from $Z$, and $x \in X(\overline{\mathbb{Q}})$, then

$$h(\varphi(x)) = dh(x) + c'_{\varphi,X}.$$

**Proof.** Pick $x \in \mathbb{P}^n \setminus Z(\overline{\mathbb{Q}})$, say $x = [a_0 : \ldots : a_n]$. Take a number field $K$ over which constants relevant to situation, in particular $x$ and $\varphi$ (but also things will will be introduced later) are defined.

For any place $v \in M_K$, define

$$|x|_v = \max\{|a_i|_v\}$$

$$|F|_v = \max\{|\text{coefficients of } F|_v\}$$

$$\epsilon(v, r) = \begin{cases} r & v \mid \infty \\ 1 & v \nmid \infty. \end{cases}$$

By the triangle inequality,

$$|\varphi_i(x)|_v \leq \epsilon(v, \left(\frac{n + d}{n}\right))|\varphi_i|_v|x|_v^d.$$ 

Then

$$|\varphi(x)|_v = \max_i\{|\varphi_i(x)|_v\} \leq \epsilon(v, \left(\frac{n + d}{n}\right))\max\{|\varphi_i|_v\}|x|_v^d.$$ 

Now raising everything to the $\frac{n}{[\mathbb{K}: \mathbb{Q}]}$ power and taking the product over all $v$ (so everything is finally well-defined by the product rule), we get

$$H(\varphi(x)) \leq \left(\frac{n + d}{n}\right)^{\frac{n}{[\mathbb{K}: \mathbb{Q}]}} H(\varphi)H(x)^d$$

The reason that we get the constant $(\frac{n + d}{n})$ with exponent 1 comes from the degree formula applied to the archimedean places, since the constant is 1 for the non-archimedean places. Taking the logarithm, we get

$$h(\varphi(x)) \leq dh(x) + c\varphi.$$

(2.1)

To prove (2), let $I_X = \langle f_1, \ldots, f_r \rangle$ be the ideal of $X$ in $\mathbb{P}^n$. We assumed that $X \cap Z = \emptyset$, so there exists $\ell > 0$ such that $\langle t_{0}, \ldots, t_{n} \rangle^\ell \subset \langle \varphi_{0}, \ldots, \varphi_{m}, f_{1}, \ldots, f_{r} \rangle$.

In particular, for all $j$ we can write

$$t_j^\ell = \sum \psi_{i,j} \varphi_i + \sum g_{i,j} f_i.$$ 

We can assume that the $\psi_{i,j}$ are all homogeneous of the degree $\ell - d$. Evaluating this at the point $x$, we get

$$x_j^\ell = \sum_{i,j} \psi_{i,j}(x) \varphi_i(x).$$
Taking absolute values, we obtain
\[
|x_j|_v \leq \epsilon(v, m + 1) \max_{i,j} \{|\psi_{i,j}(x)|_v \} \max_i |\varphi_i(x)|_v \\
\leq \epsilon(v, m + 1) \epsilon(v, \binom{\ell - d + n}{n}) \max_{i,j} \{|\psi_{i,j}|_v \} |x|_v^{\ell - d} \max_i |\varphi_i(x)|_v.
\]
Raising everything to the \( n/v[K:Q] \) power and taking the product over \( v \in M_K \), we get
\[
H(x)^\ell \leq C'' H(x)^{\ell - d} H(\varphi(x)).
\]
Taking the logarithm we find that
\[
\frac{dh(x)}{x^\ell} \leq C' + h(\varphi(x)).
\]
Combining this with the earlier inequality (2.1), we deduce the result. \( \square \)

**Lemma 2.3.3.** Let \( X \) be a variety over \( \overline{Q} \) and \( \varphi, \psi \) be two morphisms to projective space such that
\[
\varphi^* H \sim \psi^* H'.
\]
Then \( h_\varphi = h_\psi \) in \( H(X) \).

**Proof.** Let \( \varphi: X \to \mathbb{P}^n \) and \( \psi: X \to \mathbb{P}^m \) be two maps such that \( \varphi^* H \sim \psi^* H' \sim D \). Then we can write in coordinates \( \varphi = [f_0: \ldots: f_n] \) and \( \psi = [g_0: \ldots: g_m] \) with \( f_i, g_i \in H^0(X,D) \).

Now, \( H^0(X,D) \) is finitely dimensional over \( \overline{Q} \), so we can pick a basis \( h_0, \ldots, h_N \) for it. This defines a morphism \( X \to \mathbb{P}^N \) (in other words, the morphism defined by the complete linear system \( |D| \)) and \( \varphi, \psi \) factor through it:

\[
\begin{array}{ccc}
X & \overset{\alpha}{\longrightarrow} & \mathbb{P}^N \\
\downarrow \psi & \overset{\gamma}{\longrightarrow} & \mathbb{P}^m \\
\downarrow \varphi & \overset{\beta}{\longrightarrow} & \mathbb{P}^n
\end{array}
\]

Then \( \gamma \) and \( \beta \) are rational maps of degree one (they are projections), so Lemma 2.3.2 implies that \( h_\alpha \) and \( h_\beta \) differ by a bounded function, and similarly for \( h_\alpha \) and \( h_\gamma \). \( \square \)

**Lemma 2.3.4.** Suppose that \( s: \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{n(m+1)(m+1) - 1} \) is the Segre embedding, i.e. \( s([a_0: \ldots: a_n], [b_0: \ldots: b_m]) = [a_i b_j] \), then \( h(s(x,y)) = h(x) + (y) \).

**Proof.** Easy exercise. \( \square \)

**Lemma 2.3.5.** Let \( \nu_d: \mathbb{P}^n \to \mathbb{P}^N \) be the Veronese embedding. Then \( h(\nu_d(x)) = dh(x) \).

**Proof.** Easy exercise. \( \square \)
2.3. THE WEIL HEIGHT MACHINE ON VARIETIES

Proof of Weil’s Theorem 2.3.1. If $L \in \text{Pic}(X)$ is basepoint-free (or equivalently, $\mathcal{O}_X(L)$ is generated by global sections), then $L \sim \varphi^*H$ for some morphism $\varphi : X \to \mathbb{P}^n$, then we put $h_L := h_\varphi$. This is well-defined by Lemma 2.3.3.

Now, any $L \in \text{Pic}(X)$ can be written as the difference of two basepoint-free divisors. In fact, any divisor is the difference of two very ample divisors by standard results on ample divisors. So we can write $L = M' - M''$ where $M', M''$ are basepoint-free. Extend by linearity: $h_L = h_{M'} - h_{M''}$.

Is this well-defined? If $L = M' - M'' = R' - R''$, then $M' + R'' = M'' + R'$. Then $h_{M' + R''}$ corresponds to the Segre embedding of $|M'|$ and $|R''|$, and similarly for $h_{M'' + R'}$. Lemma 2.3.4 shows that $h_{M' + R''} = h_{M'} + h_{R''}$ and also $h_{M'' + R'} = h_{M''} + h_{R'}$. Using Lemma 2.3.3 again, we see that this is indeed well-defined.

The second statement is obvious from the observation that for basepoint-free divisors $L$ on $X$, we have $\pi^*h_L = h_{\pi^*L}$.

For a line bundle $L$, denote by

$$B(L) = \bigcap_{D \in |L|} D$$

its base locus.

**Theorem 2.3.6 (Weil).** With the same notation as above, we have:

1. For any representative $h_L$ (from its class in $\mathcal{H}(X)$), there exists a constant $C$ such that for all $x \in X \setminus B_s(L)(\overline{\mathbb{Q}})$, we have $h_L(x) \geq C$.

2. Assume that $L$ is ample. For any representative $h_L$ and $B \in \mathbb{N}$, we have

$$\# \{x \in X(\overline{\mathbb{Q}}) : h_L(x) \leq B\} < \infty.$$  

The first assertion is an analogue of the fact that the intersection number of a divisor and a curve away from its base locus is non-negative. (We shall see soon that the height can be thought of as analogous to an intersection product.)

**Proof.** If $B(L) = X$, i.e. $H^0(X, L) = 0$, then there is nothing to prove. Otherwise, there is an effective divisor $D \sim L$. Replacing $L$ with $D$, we may assume that $L$ is effective. Then we can write $L$ as the difference of two basepoint-free divisors $M'$ and $M''$, so that $L = M' - M''$. We may also assume that $h_L = h_{\varphi'}^L - h_{\varphi''}^L$ where $\varphi' : X \to \mathbb{P}^{n'}$ and $\varphi'' : X \to \mathbb{P}^{n''}$ correspond to $M'$ and $M''$.

Since $M''$ and $L$ are effective, we have an inclusion

$$H^0(X, M'') \subset H^0(X, M').$$

19
CHAPTER 2. HEIGHTS

If $\varphi', \varphi''$ are the maps to projective space corresponding to $M', M''$, then we get a commutative diagram

$$
\begin{array}{cc}
X & \xrightarrow{\varphi'} & \mathbb{P}^{n'} \\
\downarrow{\varphi''} & & \downarrow{\pi} \\
& \mathbb{P}^{m'} &
\end{array}
$$

and we can take $\pi$ to be a projection.

It is easy to check from the definition of heights that

$$h_L(x) = h_{\varphi'}(x) - h_{\varphi''}(x) = h(\varphi'(x)) - h(\varphi''(x)) \geq 0 \text{ for } x \in X \setminus M'(\overline{\mathbb{Q}}).$$

Varying $h_{M'}$ and $h_L$ in their equivalence classes changes this only by a bounded amount, which establishes (1).

For the second part, note that since $L$ is ample some high multiple of $L$ is very ample. Since we know the effect on the (logarithmic) height of composing with a Veronese embedding is just multiplication by a scalar, we may assume that $L$ is very ample, hence gives an embedding of $X$ in $\mathbb{P}^n$, and then the result follows from Northcott’s Theorem.

\begin{definition}
Let $X$ be a smooth projective variety over $\overline{\mathbb{Q}}$, $L$ a divisor on $X$, and $\varphi : X \to X$ a morphism such that $\varphi^*L \sim \alpha L$ for some $\alpha > 1$. Define the \textit{canonical height} of $L$ by

$$\hat{h}(x) = \lim_{m \to \infty} \frac{h_L(\varphi^m(x))}{\alpha^m}.$$ 

\end{definition}

\begin{theorem}
A canonical height function $\hat{h} : X(\overline{\mathbb{Q}}) \to \mathbb{R}$ is well-defined (independent of the choice of representative $h_L$). Moreover,

1. $\hat{h} = h_L$ in $\mathcal{H}(X)$
2. $\hat{h}(\varphi(x)) = \alpha \hat{h}(x)$.

\end{theorem}

\begin{proof}
We show that $\hat{h}$ is well-defined. First note that we have

$$|h_L(\varphi(x)) - \alpha h_L(x)| = |h_{\alpha L}(x) - \alpha h_L(x)| < C$$

for some $C$ independent of $x$. Therefore,

$$\left| \frac{h_L(\varphi(x))}{\alpha} - h_L(x) \right| < \frac{C}{\alpha}.$$ 

We show that the sequence in the limit is a Cauchy sequence.

$$\left| \frac{h_L(\varphi^n(x))}{\alpha^n} - \frac{h_L(\varphi^m(x))}{\alpha^m} \right| \leq \sum_{i=m+1}^{n} \left| \frac{h_L(\varphi^i(x))}{\alpha^i} - \frac{h_L(\varphi^{i-1}(x))}{\alpha^{i-1}} \right| < \sum_{\alpha=m+1}^{n} \frac{C}{\alpha^i}. $$

20
Since $\alpha > 1$, and any two choices of $h_L$ differ by an absolutely bounded constant, it is also clear that the limit is independent of the choice of $h_L$. Also, property (2) is evident.

Exercise 2.3.9. With the same notation/assumptions, assume further that $L$ is ample. Then $\hat{h} \geq 0$. Show that for all $x \in X(\overline{\mathbb{Q}})$,

$$\hat{h}(x) = 0 \iff \varphi^m(x) = \varphi^n(x) \text{ for some } m \neq n.$$

2.4 Height theory over function fields

There is a strong analogy between number fields and function fields of curves, and we can develop the theory of heights over function fields as well.

Let $k$ be an algebraically closed field of characteristic 0, $C$ a smooth projective curve over $k$, and $K = k(C)$. Let $X$ be a smooth projective variety over $X$ (defined over $K$).

Let $L$ be a divisor on $X$. There is a projective variety $\overline{X}/k$ and a morphism $\overline{X} \to C$ whose generic fiber is $X$. This really takes the apparatus of scheme theory to understand properly, but we can do it in an ad hoc manner in this case. $X$ comes equipped with a projective structure morphism to $\text{Spec } K$, so we have an embedding

$$X \subset \mathbb{P}^n_k \to \mathbb{P}^n_C$$

We can then let $\overline{X}$ be the closure of $X$ in $\mathbb{P}^n_C$. We will assume that $\overline{X}$ is smooth. This choice is always possible over characteristic zero, by the theorem on resolution of singularities.

We can take the closure of $L$ in $\overline{X}$, getting a divisor $\sum m_i L_i$. A point $x \in X(K)$ corresponds to

$$\text{Spec } K \to X \to \text{Spec } K$$

Since $C$ is smooth and projective, this is equivalent to a $C$-point of $\overline{X}$,

$$C \to \overline{X} \to C$$

which we denote by $\overline{x}$. We then define

$$h_L(x) := \deg \overline{x}^* L.$$

21
CHAPTER 2. HEIGHTS

Now, this definition depends on our choice of model, $\overline{X}$. However, it turns out to be well-defined up to a bounded function. If $x \in X(K')$ where $K'/K$ is a finite extension, then we define $h_L(x) = \deg \frac{\pi'^*L}{[K':K]}$. Consider instead the diagram

\[
\begin{array}{ccc}
C' & \xrightarrow{\pi} & X \\
\downarrow & & \downarrow \\
C & \xrightarrow{\lambda} & X
\end{array}
\]

**Lemma 2.4.1.** If $\overline{X} \to C$ and $\overline{X}' \to C$ are models as above, then $h_L - h'_L$ is bounded on $X(\overline{K})$.

**Proof.** We can choose a smooth model $\overline{X}''$ dominating both $\overline{X}$ and $\overline{X}'$. For $x \in X(K)$, we get $C$-points of $\overline{X}, \overline{X}', \overline{X}''$.

\[
\begin{array}{ccc}
C & \xrightarrow{\pi''} & \overline{X}'' \\
\downarrow & & \downarrow \\
\overline{X} & \xrightarrow{\lambda} & \overline{X}''
\end{array}
\]

By definition,

\[
h_L(x) = \deg \pi^*L = \deg (\pi'')^*\alpha^*L \\
h'_L(x) = \deg (\pi')^*\beta^*L
\]

Let $G = \alpha^*L - \beta^*L$. Since $\overline{X} \to C$ and $\overline{X}' \to C$ are isomorphisms over the generic point of $C$ (both have generic fiber $X$), $G$ restricts to $0$ on the generic point of $C$. In other words, $G$ is mapped to a finite set of points by $\lambda : \overline{X}'' \to C$. Therefore, there is an effective divisor $D$ on $C$ such that $-\lambda^*D \leq G \leq \lambda^*D$. Then the pullback of $G$ via $\pi''$ has degree between $-\deg D$ and $\deg D$.

**Theorem 2.4.2.** There is a homomorphism

\[
\text{Pic}(X) \to H_Z(X) = \frac{\{\text{functions } X(\overline{k}) \to \mathbb{Z}\}}{\{\text{bounded functions}\}}
\]

such that

1. **(functoriality)** If $Y$ is smooth and projective over $K$ and $\pi : Y \to X$, then the diagram

\[
\begin{array}{ccc}
\text{Pic}(X) & \xrightarrow{\text{Pic}(\pi)} & \text{Pic}(Y) \\
\downarrow & & \downarrow \\
H_Z(X) & \xrightarrow{\text{H}_Z(\pi)} & H_Z(Y)
\end{array}
\]
commutes, and

2. If \( X = \mathbb{P}_K^n \) and \( L \) is a hypersurface, then \( h_L = h \) in \( H_\mathbb{Z}(X) \), where \( h \) is defined as follows: if \( x = [f_0 : \ldots : f_n] \in \mathbb{P}_K^n \), then

\[
h(x) = \sum_{c \in C} \max_i \{-\text{ord}_c(f_i)\}.
\]

3. If \( L \geq 0 \) and \( x \not\in L \), then \( h_L(x) \geq 0 \).

**Proof.** First we need to show that \( \text{Pic}(X) \to H_\mathbb{Z}(X) \) is well-defined, i.e. if \( L \sim 0 \) then \( h_L \) is bounded. If \( L \sim 0 \), then we may write \( L = \text{div}(f) \) for some rational function \( f \) on \( X \). But \( f \) can also be thought of as a rational function on \( X \), and \( L - \text{div}(f) \) is union of finitely many vertical fibers over \( C \) since it is not supported at the generic point. As in the proof of Lemma [2.4.1](#), that implies

\[
\deg \pi^*(L - \text{div}(f)) \text{ is a bounded function of } x.
\]

But \( \deg \pi^*(L - \text{div}(f)) = h_L(x) - \deg \text{div}(\pi^*f) \), and \( \deg \text{div}(\pi^*f) = 0 \).

1. If \( \overline{X} \to C \) and \( \overline{Y} \to C \) are models of \( X, Y \) we can choose \( Y \) so that we have a commutative diagram

\[
\begin{array}{ccc}
Y & \longrightarrow & X \\
\downarrow & & \downarrow \\
\overline{Y} & \longrightarrow & \overline{X}
\end{array}
\]

Then it becomes clear that \( \pi^*h_L = h_{\pi^*L} \).

2. It suffices to show the result when \( L \) is the divisor class represented by a hyperplane. Let \( H_i \) be the hyperplane cut out by \( t_i \). Now pick \( x \in X(K) \) and consider the diagram

\[
\begin{array}{ccc}
C & \longrightarrow & \overline{X} \\
\downarrow & & \downarrow \\
C & \longrightarrow &
\end{array}
\]

We can assume that the image of \( C \) is not contained in \( \overline{H}_i \), which is the locus cut by \( t_i \) on \( \overline{X} \). Let \( D_i = \pi^*H_i \). Then

\[
D_i - D_j = \pi^*(H_i - H_j) = \pi^*(\text{div}(t_i/t_j)) = \text{div}(f_i/f_j) = \text{div}(f_i) - \text{div}(f_j).
\]

Then for any \( c \in C \), we have

\[
\min_i \{\text{ord}_c D_i - \text{ord}_c D_j\} = \min_i \{\text{ord}_c(f_i) - \text{ord}_c(f_j)\}. \quad (2.2)
\]
Now, $\min \text{ord}_c D_i = 0$ because there is no base locus, so summing the left hand side of (2.2) over all $c$ gives $-\deg D_j$. On the right hand side, we get $\sum_c \text{ord}_c(f_j) = 0$ because $f_j$ is a rational function, so we conclude that

$$-h_L(x) = -\deg D_j = \sum_c \min \text{ord}_c(f_i)$$

if $L = H_j$.  

□
Chapter 3

Arakelov Geometry

In this section we will see a glimpse of Arakelov theory, which gives an intersection-theoretic interpretation of the height in number field settings analogous to that in the function field setting.

3.1 Hermitian metrics on line bundles

Let $M$ be a complex manifold and $L$ a locally free sheaf on $M$.

**Definition 3.1.1.** A hermitian metric on $L$ is a map

$$\langle -, - \rangle : L \times L \to \mathcal{C}^0 := \text{sheaf of } \mathbb{C}\text{-valued continuous functions}.$$  

such that

- $\langle af + bg, h \rangle = a \langle f, h \rangle + b \langle g, h \rangle$ for all $f, g, h \in L(U)$ and $a, b \in \mathcal{O}_M(U)$.
- $\langle f, h \rangle = \langle h, f \rangle$.
- $||f|| = \sqrt{\langle f, f \rangle} > 0$ if $f$ is nowhere vanishing.

If rank $L = 1$, then the norm determines the inner product.

**Example 3.1.2.** If $L = \mathcal{O}_M$, then we can define

$$\langle f, g \rangle = fg.$$

**Example 3.1.3.** If $M = \mathbb{P}^n$ and $L = \mathcal{O}(1)$, then $L$ is generated by global sections $t_0, \ldots, t_n$. We can then define the norm on the level of global sections. We set

$$||f||(x) = \frac{|f(x)|}{\max\{x_i\}}$$

A priori neither $f(x)$ nor $x_i$ is well-defined, but the ratio is homogeneous of degree 0 and hence well-defined.
CHAPTER 3. ARAKELOV GEOMETRY

Pullback. If $\varphi : M' \to M$ is a holomorphic map and we have a metric on $\mathcal{L}$ over $M$, then we get a metric on $\varphi^*\mathcal{L}$ by

$$\langle \varphi^*f, \varphi^*g \rangle = (f, g) \circ \varphi.$$ 

In particular, if $\{x\} \to M$ is the inclusion of a point, then $\varphi^*\mathcal{L}$ is a vector space with a hermitian form.

3.2 Line bundles on number fields

Let $K$ be a number field, $X$ a smooth projective variety over $K$, and $R$ the ring of integers of $K$. Let $C = \text{Spec} R$ and $\overline{X} \to C$ be a model of $X$ (a projective morphism whose generic fiber is $X$). Let $\mathcal{F}$ be a locally free sheaf on $\overline{X}$.

For every rational point $\sigma : K \to C$, we get a “fiber over $\sigma$,” $X_\sigma := \overline{X} \times_C \text{Spec} \mathbb{C}$.

$$\begin{array}{ccc}
X_\sigma & \to & X \\
\downarrow & & \downarrow \\
\text{Spec} \mathbb{C} & \to & \text{Spec} K \\
\end{array}$$

Since $X$ is smooth over $K$, $X_\sigma$ is a smooth variety over $\text{Spec} \mathbb{C}$. That means that it can be considered as a smooth manifold over $\mathbb{C}$. Let $\mathcal{L}_\sigma$ be the pullback of $\mathcal{F}$ to $X_\sigma$. $C$ is obviously not a proper curve, but we should view the infinite places as giving a “compactification” of it.

A Hermitian metric on $\mathcal{L}$ can be thought of as a collection of metrics on $\mathcal{L}_\sigma$ with a compatibility condition for conjugate embeddings:

$$\langle f_\sigma, g_\sigma \rangle(x) = (f_\pi, g_\pi)(x)$$

where $x \in X_\sigma$ is the image of $x \in X_\sigma$ under the isomorphism $X_\sigma \to X_\pi$ induced by complex conjugation.

Suppose that rank $\mathcal{F} = 1$ and $X = \text{Spec} K$, so $\overline{X} = C$. We want to define the notion of $\deg \mathcal{F}$. Normally this only makes sense for proper curves, but we recall that we think of $R$ as being “nearly proper” because of the infinite places.

Since $C = \text{Spec} R$, $\mathcal{F}$ corresponds to the $R$-module $L = H^0(C, \mathcal{F})$. Since $\mathcal{F}$ is locally free of rank one, $\mathcal{F}$ is flat (in fact, projective) over $C$.

Definition 3.2.1. Assume that $\mathcal{F}$ has a Hermitian metric (or equivalently, norm). Pick some non-zero $\ell \in \mathcal{L}$, and define

$$\deg \mathcal{F} = \log \#(L/R\ell) - \sum_{\sigma : K \to \mathbb{C}} \log ||\ell||_\sigma.$$

This seems like a wacky definition at first, but it is actually analogous to a formulation of the usual definition in terms of taking a global section (in this case
and add up the orders of vanishing. The quantity \(#(L/R\ell)\) can be thought of as \(\prod_p |\ell|_p^{-\text{ord}_p(\ell)}\), and the second term in the definition can be thought of as a contribution from the infinite places.

**Theorem 3.2.2.** \(\deg\mathcal{L}\) does not depend on the choice of \(\ell\).

**Proof.** Pick \(0 \neq \ell, \ell' \in L\). Then there exist \(a, a' \in R\) such that \(a\ell = a'\ell'\). So we reduce to the case where \(\ell' = a\ell\). By the product formula, we have

\[
\prod_{v \in M_K} ||a||_v = 1 \text{ for all } a \in K.
\]

Taking logarithms, we get (by some computations done earlier)

\[
0 = -\log #(R/a) + \sum_{v|\infty} \log ||a||_v.
\]

Therefore, it suffices to show that \(\log #(R/\ell') = \log #(R/\ell) + \log #(R/a)\). For that, we invoke the short exact sequence

\[
0 \to R\ell/Ra\ell \to L/Ra\ell \to L/R\ell \to 0
\]

and the observation that \(R\ell/Ra\ell \cong R/a\).

**Theorem 3.2.3.** With the same setup as before, let \(\mathcal{L}\) be an invertible sheaf on \(X\) with a given metric. Let \(L = \mathcal{L}|_X = \mathcal{O}_X(D)\). Then

\[
h_{\mathcal{L}} = h_D \text{ in } \mathcal{H}(X)
\]

where

\[
h_{\mathcal{L}}(x) = \frac{\text{deg } \pi^*\mathcal{L}}{|K' : K|} \text{ if } x \in X(K').
\]

First, some general remarks are in order about constructing metrics from given ones. Suppose \(M\) is a complex manifold and \(\mathcal{L}_1\) and \(\mathcal{L}_2\) are invertible sheaves with given metrics. Then:

- there exists a metric on \(\mathcal{L}_1 \otimes \mathcal{L}_2\) such that
  \[
  ||f \otimes g||_{\mathcal{L}_1 \otimes \mathcal{L}_2} = ||f||_{\mathcal{L}_1} ||g||_{\mathcal{L}_2}.
  \]

- there exists a metric on \(\mathcal{L}_2^{-1}\) such that \(||f||_{\mathcal{L}_2^{-1}} = \frac{1}{||f||_{\mathcal{L}_2}}\)

- If \(M\) is compact, any two metrics on \(\mathcal{L}_1\) are equivalent: there exist constants \(c_1, c_2 > 0\) such that
  \[
  c_1 ||f|| \leq ||f||' \leq c_2 ||f||.
  \]
Proof. Using the above remarks, we can see that if $\mathcal{N}_1$ and $\mathcal{N}_2$ are invertible sheaves on $M$ then $\deg(\mathcal{N}_1 \otimes \mathcal{N}_2) = \deg \mathcal{N}_1 + \deg \mathcal{N}_2$ and $\deg \mathcal{N}_1^{-1} = -\deg \mathcal{N}_1$. By tensoring with a large very ample divisor, we can assume that $\mathcal{L}$ is very ample. So we reduce to the case $X = \mathbb{P}^n, \overline{X} = \mathbb{P}^n \mathbb{C}, \mathcal{L} = \mathcal{O}_{\mathbb{P}^n}(1)$ with the metric given in our earlier example.

Pick $x = [a_0: \ldots : a_n] \in X(k)$. We can assume that $a_i \in R$. Pulling back $\mathcal{L}$ to $\mathcal{C} = \text{Spec} R$, we get a line bundle $L$ which is just the ideal $(a_0, \ldots, a_n)$. For each $\sigma : K \to \mathbb{C}$, we get a morphism $\text{Spec} \mathbb{C} \to \mathbb{P}^n \mathbb{C} = X_\sigma$ whose image is the point $[\sigma(a_0): \ldots : \sigma(a_n)]$. Assume without loss of generality that $a_0 \neq 0$. We then compute

\[
\deg \pi^* \mathcal{L} = \log \# L/(Ra_0) - \sum_\sigma \log ||a_0||_\sigma
\]

By the usual arguments, \(\log \# L/(Ra_0) = \log ||a_0|| - \log \#(R/L)\). Furthermore,

\[
||a_0||_\sigma = \log |\sigma(a_0)| + \log \max \{|\sigma(a_i)|\}.
\]

Now, $\log \#(R/Ra_0) - \sum_\sigma \log |\sigma(a_0)|$ is the degree of the trivial line bundle, which is zero. Cancelling this from $\deg \pi^* \mathcal{L}$, we are left with

\[
- \log \#(R/L) + \sum_\sigma \log \max \{||a_i||_\sigma\}.
\]

This is precisely $h_D(x)$, up to a bounded function. \qed
Chapter 4

Abelian Varieties

4.1 Abelian varieties over algebraically closed fields

Let $k$ be an algebraically closed field.

Definition 4.1.1. A quasiprojective group variety $X/k$ is a quasiprojective variety whose closed points have a group structure.

A better definition is that there are morphisms $X \times X \rightarrow X$, $X \rightarrow X$, Spec $k \rightarrow X$, satisfying the usual axioms.

Example 4.1.2. The additive group $\mathbb{G}_a$ has the underlying variety $\mathbb{A}^1$. The multiplicative group $\mathbb{G}_m$ has the underlying variety $\mathbb{A}^1 \setminus \{0\}$.

Definition 4.1.3. An abelian variety is a projective group variety.

Example 4.1.4. Abelian varieties of dimension 1 are elliptic curves. The group law on elliptic curves is well-known. On the other hand, the canonical bundle on an abelian variety must be trivial, which for curves forces $g = 1$.

Remark 4.1.5. It is well-known that if $k = \mathbb{C}$, any abelian variety $A$ is a complex torus, i.e. its analytification is $A = \mathbb{C}^n/\Lambda$ where $\Lambda$ is a lattice.

Lemma 4.1.6 (Rigidity). Assume that $X, Y, Z$ are varieties with $X$ projective. Let $\varphi : X \times Y \rightarrow Z$ be a morphism. If there exists $y_0 \in Y$ such that $\varphi|_{X \times y_0}$ is constant, then $\varphi|_{X \times y}$ is constant for all $y \in Y$.

If there exists $y_0 \in Y$ and $x_0 \in X$ such that $\varphi|_{x_0 \times Y}$ and $\varphi|_{X \times y_0}$ are constant, then $\varphi$ is constant.

Proof. Exercise. $\square$

Definition 4.1.7. Let $A, B$ be abelian varieties. A morphism $\varphi : A \rightarrow B$ is a group homomorphism which is also a morphism of varieties.

There are two distinguished kinds of morphisms from an abelian variety to itself:
• A translation is a morphism of the form $\psi(x) = x + a$ for all $x \in A$.

• There is a multiplication by $n$ morphism $\pi_n : A \to A$ sending $x \mapsto [n]x$.

**Theorem 4.1.8.** Suppose that $\varphi : A \to B$ is a morphism of abelian varieties. Then $\varphi$ is a composition of a translation and a homomorphism.

**Proof.** Composing with a translation, we may assume that $\varphi(0_A) = 0_B$. Consider the morphism $\psi : A \times A \to B$ defined by $\psi(x, x') = \varphi(x + x') - \varphi(x) - \varphi(x')$. By the group axioms, $\psi|_{A \times \{0_A\}} = 0_B$ and $\psi|_{\{0_A\} \times A} = 0_B$, so $\psi$ is constant, hence $\varphi$ is a homomorphism. \hfill $\Box$

**Theorem 4.1.9** (Theorem of the cube). Suppose that $X, Y, Z$ are varieties with $X, Y$ projective. Assume that $\mathcal{L}$ is an invertible sheaf on $X \times Y \times Z$. Suppose that there exist $x_0 \in X, y_0 \in Y, z_0 \in Z$ such that $\mathcal{L}|_{\{x_0\} \times Y \times Z}, \mathcal{L}|_{X \times \{y_0\} \times Z}, \mathcal{L}|_{X \times Y \times \{z_0\}}$ are all trivial.

Then $\mathcal{L}$ is trivial.

**Proof.** The proof is actually rather difficult, requiring the theorem on cohomology and base change. See Mumford’s book, page 55. \hfill $\Box$

**Theorem 4.1.10** (Theorem of the cube for abelian varieties). Let $A$ be an abelian variety, $\mathcal{L}$ a divisor on $A$. For $I \subset \{1, 2, 3\}$ let $\varphi_I : A \times A \to A$ be given by $\varphi_I(x_1, x_2, x_3) = \sum_{i \in I} x_i$. Then

$$\varphi_{123}^*L - \varphi_{12}^*L - \varphi_{13}^*L - \varphi_{23}^*L + \varphi_1^*L + \varphi_2^*L + \varphi_3^*L$$

is trivial.

**Proof.** Let $D$ be the divisor associated to the huge line bundle that we want to show is trivial. Consider $D|_{A \times A \times \{0\}}$. Well,

$$\varphi_{123}|_{A \times A \times \{0\}} = \varphi_{12}|_{A \times A \times \{0\}},$$

$$\varphi_{13}|_{A \times A \times \{0\}} = \varphi_{1}|_{A \times A \times \{0\}},$$

$$\varphi_{23}|_{A \times A \times \{0\}} = \varphi_{2}|_{A \times A \times \{0\}}$$

Since restriction commutes with pullbacks, we see that $D|_{A \times A \times \{0\}} \sim 0$. Now we can apply the theorem of the cube to get the result. \hfill $\Box$

**Corollary 4.1.11** (Mumford’s formula). Let $A$ be an abelian variety, $L$ a divisor on $A$, and $\pi_n : A \to A$ be the multiplication-by-$n$ map. Then

$$\pi_n^*L \sim \frac{n^2 + n}{2}L + \frac{n^2 - n}{2}\pi_{-1}^*L.$$
4.2. ABELIAN VARIETIES OVER NUMBER FIELDS

Proof. Consider the morphism $A \xrightarrow{\pi_n,\pi_1,\pi_{-1}} A \times A \times A$. Pull back the big trivial divisor from the theorem of the cube, to get

$$\pi_n^* L - \pi_{n+1}^* L - \pi_{n-1}^* L + \pi_n^* L + \pi_1^* L + \pi_{-1}^* L = 0.$$ 

Then apply induction to get the result. \qed

Remark 4.1.12. If $\pi_{-1}^* L = L$ (we say that $L$ is symmetric), then Corollary 4.1.11 implies that

$$\pi_n^* L \sim n^2 L.$$ 

On the other hand, if $\pi_{-1}^* L = -L$ (we say that $L$ is antisymmetric), then Corollary 4.1.11 implies that

$$\pi_1^* L \sim nL.$$ 

4.2 Abelian varieties over number fields

We say that $A$ is an abelian variety over a number field if $0 \in A(K)$ and all the structure morphisms are defined over $K$.

Consider the morphism $\pi_2 : A \to A$ (multiplication by 2). If $L$ is a symmetric divisor/line bundle, then $\pi_2^* L \sim 4L$. Recall that we defined a canonical height for divisors and morphisms with this property:

$$\hat{h}(x) = \lim_{n \to \infty} \frac{h_L(\pi_2^n(x))}{4^n}.$$ 

Recall that $\hat{h} = h_L$ in $\mathcal{H}(A)$.

Remark 4.2.1. Any group variety in characteristic 0 is smooth, by generic smoothness. We are implicitly using that here.

Theorem 4.2.2. The canonical height $\hat{h}$ satisfies the following properties:

1. $\hat{h}(mx) = m^2 \hat{h}(x),$
2. $\hat{h}(x+y) + \hat{h}(x-y) = 2\hat{h}(x) + 2\hat{h}(y)$
3. Define the pairing $\langle \cdot, \cdot \rangle : A(K) \times A(K) \to \mathbb{R}$ by

$$\langle x, y \rangle = \frac{\hat{h}(x+y) - \hat{h}(x) - \hat{h}(y)}{2}.$$ 

Then this pairing is bilinear.

4. If $L$ is ample, then for any $c$ the set $\{ x \in A(K) \mid \hat{h}(x) \leq c \}$ is finite.

Remark 4.2.3. This says that the height is actually a quadratic function: note that $\hat{h}(x) = \langle x, x \rangle$. 

31
Proof. 1. If \( \pi : A \to A \) is multiplication by \( r \), then

\[
\begin{align*}
    h_L(\pi_r(x)) &= h_{\pi^*L}(x) + O(1) \\
    &= h_{x^2L}(x) + O(1) \\
    &= r^2h_L(x) + O(1)
\end{align*}
\]

By definition, the canonical height is

\[
\hat{h}(mx) = \lim_{n \to \infty} \frac{m^2h_L(\pi^{2n}(x)) + O(1)}{4^n} = m^2\hat{h}(x).
\]

2. This comes from the Theorem of the cube. Consider the morphism \( A \times A \to A \times A \times A \) corresponding to \( (x, y) \mapsto (x, y, -y) \). The theorem of the cube says that

\[
\varphi_{123}^*L - \varphi_{12}^*L - \varphi_{23}^*L - \varphi_{13}^*L + \varphi_1^*L + \varphi_2^*L + \varphi_3^*L \sim 0.
\]

Note that \( \varphi_{123} \circ \theta(x, y) = x, \varphi_{12} \circ \theta(x, y) = x + y, \varphi_{23} \circ \theta = 0 \), etc. Using these, we can compute the pullback of the above line bundle to \( A \times A \), and we get

\[
h_L(x) - h_L(x + y) - h_L(x - y) + h_L(x) + h_L(y) + h_L(-y) = O(1).
\]

Since \( L \) is symmetric, \( h_L(-y) = h_L(y) \), and we get that

\[
2h_L(x) + 2h_L(y) = h_L(x + y) + h_L(x - y) + O(1).
\]

Then taking the limit for the canonical height, we get what we want.

3. By a similar calculation with the theorem of the cube,

\[
\hat{h}(x + y + z) - \hat{h}(x + y) - \hat{h}(x + z) - \hat{h}(y + z) + \hat{h}(x) + \hat{h}(y) + \hat{h}(z) = 0.
\]

This implies that

\[
\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle.
\]

4. This is immediate from Theorem 2.3.6

\[ \square \]

Theorem 4.2.4 (Mordell-Weil). If \( A \) is an abelian variety over a number field \( K \), then \( A(K) \) is a finitely generated abelian group.

First we prove:

Theorem 4.2.5 (Weak Mordell-Weil). If \( A \) is an abelian variety over a number field \( K \), and \( m \geq 2 \), then \( A(K)/mA(K) \) is finite.
4.3 TORSION POINTS

This is not hard if one admits some algebraic machinery (apply Galois cohomology to
\[ 0 \to A[m] \to A \xrightarrow{m} A \to 0 \]
and use general facts about Galois cohomology).

Obviously, Mordell-Weil implies the weak Mordell-Weil. We will show how to deduce the other direction.

Proof. Take an ample symmetric divisor \( L \) on \( A \), and let \( \hat{h} \) be the associated canonical height (as above). There exist \( y_1, \ldots, y_r \in A(K) \) such that their classes hit all elements of \( A(K)/mA(K) \). Let \( c = \max_i \{ \hat{h}(y_i) \} \). Let \( S = \{ x \in A(K) \mid \hat{h}(x) \leq c \} \). Now \( S \) is finite because \( \hat{h} = h_L \) in \( H(A) \), and then we can apply Northcott’s theorem.

Pick \( x \in A(K) \) with \( \hat{h}(x) > c \). Then there exists \( y_i \) and \( x' \) such that \( x - y_i = mx' \). We have
\[ \hat{h}(x - y_i) \leq \hat{h}(x + y_i) + \hat{h}(x - y_i) = 2\hat{h}(x) + 2\hat{h}(y_i) \]
(\( \hat{h} \) is non-negative because we chose \( L \) to be ample) and
\[ \hat{h}(x - y_i) = m^2 \hat{h}(x'). \]
Therefore, \( m^2 \hat{h}(x') \leq 2\hat{h}(x) + 2c \), which implies \( \hat{h}(x') < \hat{h}(x) \). Therefore, we have written \( x \) in terms of some \( y_i \) and a point with strictly smaller height. The theorem then follows by “infinite descent.”

4.3 Torsion points

Let \( A \) be an abelian variety over a number field \( K \). A point \( x \in A(\overline{K}) \) is called an \( m \)-torsion point if \( mx = 0 \). (This is the usual notion of torsion in a group.) We let \( A(\overline{K})_{\text{tors}} \) be the set (group) of all torsion elements of \( A \), or more generally \( A(F)_{\text{tors}} \) for the torsion points defined over \( F \).

The set of \( m \)-torsion points of \( A \) is the kernel of \( \pi_m \). In particular, it is a closed subscheme of \( A \).

Lemma 4.3.1. The \( m \)-torsion subgroup \( \pi_m \) is a finite subgroup of \( A \).

Proof. If not, then it contains a projective curve \( C \). Then \((\pi_m^* L) \cdot C = 0 \), since this is just the degree of the pullback via \( \pi_m \) of \( L \) to \( C \), and \( \pi_m \) restricts to a constant function on \( C \). On the other hand, \( \pi_m^* L \sim m^2 L \), which is ample if \( L \) is, and an ample divisor intersects any curve positively, which is a contradiction.

Corollary 4.3.2. The map \( \pi_m : A \to A \) is surjective.

Proof. This follows from the fact that \( \pi_m \) has zero-dimensional fibers, so its image is full-dimensional (hence dense by irreducibility of \( A \)), and is proper.
By Mordell-Weil, \( A(K)_\text{tors} \) is finite. We can prove this directly: if \( x \in A(K) \) is \( m \)-torsion, then \( mx = 0 \) so \( \hat{h}(mx) = \hat{h}(0) = m^2 \hat{h}(x) \), so \( \hat{h}(x) < \hat{h}(0) \) if \( m \neq 1 \). Then we can apply Northcott’s theorem to see that there can only be finitely many such points (height bounded by a constant).

### 4.4 Weak Mordell-Weil

We have reduced the Mordell-Weil theorem to the weak Mordell-Weil theorem.

Since the \( A(\mathbb{K})_m \) is finite, there is a finite extension \( K'/K \) such that \( A(\mathbb{K})_m \subset A(K') \). The Mordell-Weil theorem for \( K' \) implies that for \( K \), so it suffices to show the Mordell-Weil theorem for \( K' \). Therefore, in proving the Mordell-Weil theorem we may assume that \( A(\mathbb{K})_m \subset A(K) \).

**Lemma 4.4.1.** Let \( A \) be an abelian variety over a number field \( K \) such that \( A(\mathbb{K})_m \subset A(K) \) for \( m \geq 2 \). Then there exists a finite Galois extension \( K \subset L \) such that if \( y \in A(\mathbb{K}) \) and \( my \in A(K) \) then \( y \in A(L) \).

Let’s see how this implies the Weak Mordell-Weil theorem. Let \( G = \text{Gal}(L/K) \). By definition, this is the group of automorphisms of \( L \) fixing \( K \), so it acts on \( A(L) \). We then define a map \( \alpha : A(K) \to \text{Hom}(G, A(\mathbb{K})_m) \) as follows. For \( x \in A(K) \), pick \( y \) such that \( my = x \). Now sending \( g \mapsto g(y) - y \). There are a few details to check to see that this makes sense:

- \( g(y) - y \) is indeed an \( m \)-torsion point, since multiplying by \( m \) shows \( mg(y) - my = g(my) - my = g(x) - x = 0 \) since \( x \in A(K) \).

- This is well-defined since we have assumed that \( K \) contains all the \( m \)-torsion points. Indeed, any two choices of \( y \) differ by an \( m \)-torsion point, which \( g \) fixes.

- We should check that this is indeed a homomorphism. If \( g, g' \in G \), then \( g'g \mapsto g'g(y) - y = g'(g(y) - y) + g'(y) - y \). Since \( g(y) - y \) is an \( m \)-torsion point, it is fixed by \( g' \), so this is just equal to \( g(y) - y + g'(y) - y \).

Furthermore, it is obvious that \( \alpha \) is a homomorphism. Note that \( \ker \alpha = mA(K) \), since \( \alpha(x) = 0 \iff g(y) = y \) for all \( g \iff y \in A(K) \).

Therefore, \( A(K)/mA(K) \to \text{Hom}(G, A(\mathbb{K})_m) \). Since \( G \) and \( A(\mathbb{K})_m \) are both finite, the latter is finite so \( A(K)/mA(K) \) must be finite as well.

**Proof of Lemma 4.4.1.** We will just give a sketch.

1. Pick \( y \in A(\mathbb{K}) \) such that \( my \in A(K) \). Let \( K(y) \) be the field generated by \( y \), i.e. the residue field of the point \( y \). Then we claim that \( K(y)/K \) is Galois of exponent \( m \). Indeed, any two choices of \( y \) differ by an \( m \)-torsion point, which is defined over \( A(K) \), so that \( K(y) = K(g(y)) \) for any \( g \in \text{Gal}(\mathbb{K}/K) \).
4.4. WEAK MORDELL-WEIL

Now we define a map $\text{Gal}(\overline{K}/K) \to A(\overline{K})$ sending $g \mapsto g(y) - y$. The kernel is $\text{Gal}(\overline{K}/K(y))$, so we have a injection $\text{Gal}(K(y)/K) \to A(\overline{K})_m \cong (\mathbb{Z}/m\mathbb{Z})^{2 \dim A}$. We haven't proved the last isomorphism, but it is easy to see in characteristic zero from the “Lefschetz principle” (any algebraic geometric statement over $\mathbb{C}$ implies the same for any algebraically closed field of characteristic 0). Over $\mathbb{C}$, it is obvious from the complex torus description of abelian varieties as $\mathbb{C}^g/\Lambda$.

2. We can extend $A$ to an abelian scheme $B$ over some open subset $U = \text{Spec } R_S \subset \text{Spec } R$, where $R$ is the ring of integers of $K$.

\[
\begin{array}{ccc}
A & \longrightarrow & B \\
\downarrow & & \downarrow \\
\text{Spec } K & \longrightarrow & U
\end{array}
\]

We require $B \to \text{Spec } R_S$ to be smooth and projective. Suppose that $y \in A(\overline{K})$ satisfies $my \in A(K)$. This corresponds to a diagram

\[
\begin{array}{ccc}
\text{Spec } K(y) & \longrightarrow & A & \longrightarrow & B \\
\downarrow & & \downarrow \pi_m & & \downarrow \pi_m \\
\text{Spec } K & \longrightarrow & A & \longrightarrow & B \\
\downarrow & & \downarrow & & \downarrow \\
\text{Spec } R & \longrightarrow & U
\end{array}
\]

We can “spread” the morphism $\text{Spec } K(y) \to A$ to a morphism $U_y \to B$, where $U_y$ is the inverse image of $U$ under $\text{Spec } R_y \to \text{Spec } R$. In characteristic zero, $\pi_m$ is automatically étale since it is smooth of relative dimension 0. Localizing further if necessary, we may assume that the multiplication-by-$m$ map is also étale on $B$ also $U_y \to U$ is étale.

3. There are finitely many possibilities for $U_y \to U$ - this is a fact from algebraic number theory (Hermite’s theorem). Note that it is related to the finiteness of the $S$-class group, which class field theory tells us is the Galois group of the maximal extension unramified outside $S$. Hence there are only finitely many possible extensions $K \subset K(y)$, implying that the compositum of all the $K(y)$ is only a finite Galois extension.

☐
Chapter 5

The Brauer-Manin Obstruction

5.1 Chevalley’s Theorem

**Theorem 5.1.1** (Chevalley-Warning). Let \( P_1, \ldots, P_r \in F_q[t_0, \ldots, t_n] \) be polynomials. Assume that \( P_i(0, \ldots, 0) = 0 \) for all \( i \), and \( \sum d_i := P_i \leq n \). If \( Y = V(P_1, \ldots, P_r) \subset \mathbb{A}^{n+1}(F_q) \), then \( \#Y \equiv 0 \pmod{p} \). In particular, \( \#Y \geq 2 \).

**Proof.** Note that for \( a \in F_q \), we have \( a^{q-1} = 0 \) if \( a = 0 \) and 1 otherwise. In other words, the indicator function of \( F^*_q \subset F_q \) is \( a \mapsto a^{q-1} \).

Define \( \phi = \prod_i (1 - P_i^{q-1}) \). Then for \( (a_0, \ldots, a_n) \in \mathbb{A}^{n+1}(F_q) \), we have \( \phi(a_0, \ldots, a_n) = 1 \) if and only if \( (a_0, \ldots, a_n) \in Y \) and is 0 otherwise. Therefore,

\[
\#Y \equiv \sum_{(a_0, \ldots, a_n) \in \mathbb{A}^{n+1}(F_q)} \phi(a_0, \ldots, a_n) \pmod{p}.
\]

So it suffices to show that the right hand side is 0 (mod \( p \)). Let’s focus on a monomial \( t_0^{m_0} \cdots t_n^{m_n} \) appearing on the right hand side above, which necessarily has total degree \( \leq n(q-1) \). The contribution from such a monomial is

\[
\sum_{(a_0, \ldots, a_n)} a_0^{m_0} \cdots a_n^{m_n} = \prod_i \left( \sum_{a \in F_q} a^{m_i} \right).
\]

Since \( \sum m_i \leq n(q-1) \), there is some \( j \) such that \( q - 1 \nmid m_j \) or \( m_j = 0 \). If \( q - 1 \nmid m_j \), then \( \sum_{a \in F_q} a^{m_j} \equiv 0 \pmod{p} \).

If the \( P_i \) are homogeneous, then Theorem 5.1.1 implies that they cut out an algebraic set \( X \) in \( \mathbb{P}^n \) with a rational point.

**Example 5.1.2.** If \( X \) is smooth, \( I_X = \langle P_1, \ldots, P_r \rangle \) and \( \dim X = n - r \) (i.e. \( X \) is a complete intersection), then \( X \) is a Fano variety (i.e. \( -K_X \) is ample). It is a general fact that if \( X \) is a Fano variety, then \( X(F_q) \neq \emptyset \). In fact, this is true even if \( X \) is rationally connected (a much more general condition).
5.2 Tsen’s Theorem

We now consider a similar setup over the function field of a curve.

**Theorem 5.2.1** (Tsen). Let $k$ be an algebraically closed field, $K$ the function field of a curve $C/k$, and $P_1, \ldots, P_r \in K[t_0, \ldots, t_n]$ be homogeneous of degree $\deg P_i = d_i$ such that $\sum d_i \leq n$. Then if $Y = V(\{P_i\}) \subset K^{n+1}(K)$, $\# Y \geq 2$.

In particular, if the $P_i$ are homogeneous then this is saying that the corresponding projective variety has a rational point.

**Proof.** We’ll show the result with a weaker estimate.

By assumption, the transcendence degree of $K/k$ is 1. Therefore, there exists $s \in K$ such that $K/k(s)$ is a finite extension. Let $R$ be the integral closure of $k[s]$ inside $K$. Then $R$ is a finite $k[s]$-module by commutative algebra. Therefore, there exist elements $\alpha_1, \ldots, \alpha_a \in R$ such that $R$ is generated by the $\alpha_i$ as a module over $K[s]$. We can write $\alpha_i \alpha_j = \sum g_{i,j,\ell} \alpha_\ell$. Let $d' = \max \{\deg g_{i,j,\ell}\}$.

The $P_i$ are polynomials over $K = \text{Frac}(R)$, and by clearing denominators we may assume that their coefficients lie in $R$. Now for a multi-index $I = (m_0, \ldots, m_n)$ we denote (as usual) $t^I = t_0^{m_0} \ldots t_n^{m_n}$. Then we can express

$$P_i = \sum_I \beta_{i,I} t^I \quad b_{i,I} \in R.$$ 

By the earlier comments, we can write

$$\beta_{i,I} = \sum_\ell f_{i,I,\ell} \alpha_\ell \quad f_{i,j,\ell} \in k[s].$$

Let $d'' = \max \{\deg f_{i,1,\ell}\}$.

If $h_{i,j} \in k[s]$ is of degree $\leq d''$, then

$$P_i(\sum_\ell h_{0,\ell} \alpha_\ell, \ldots, \sum h_{n,\ell} \alpha_\ell) = \sum e_{i,\ell} \alpha_\ell \quad (5.1)$$

where the $e_{i,\ell} \in k[s]$ are determined by the $h_{ij}$ and $P_i$. From all the bounds we have, we can get bounds on the degree of the $e_{i,\ell}$, e.g.,

$$\deg e_{i,\ell} \leq (d'' + d')d_i + d''.$$ 

Now we can treat the coefficients of all $h_{ij}$ as points in $\mathbb{P}^{a(n+1)(d''+1)−1}(k)$. So the condition that $(5.1)$ is 0 involves a bunch of equations over $k$ (one for each coefficient), specifically

$$\sum_{i=1}^r ((d'' + d')d_i + d'' + 1) \leq (d'' + d')n + rd'' + r.$$ 

38
5.3. BRAUER-SEVERI VARIETIES

Considering these as equations on $\mathbb{P}^{(n+1)(d''+1)-1}$, we see that if $d''$ is sufficiently large then the projective space has much larger dimension than the number of equations, so there must be some solutions. That corresponds to choices of the $h_{ij}$ solving (5.1).

**Remark 5.2.2.** If the $P_i$ cut out a smooth complete intersection, then it is Fano. It is a fact due to Grabborr-Harris-Star that if $X$ is a Fano variety over such a field $K$, then $X(K) \neq \emptyset$. Again, the statement holds even for $X$ rationally connected, which is stronger.

**Example 5.2.3.** The equation $t_0^2 + t_1^2 + t_2^2$ has no solutions in $\mathbb{P}^2(\mathbb{Q})$. This is a Fano variety with no rational points over $K$, so the result certainly doesn’t hold for number fields.

**Conjecture 5.2.4.** If $X$ is a Fano variety over some number field $K$, then there exists a finite extension $K \subset K'$ is dense in $X$ (in the Zariski topology).

5.3 Brauer-Severi varieties

Let $k$ be any field. A very basic comment is that if $\varphi : X \to Y$ is a morphism defined over $k$ and $x \in X(k)$ then $\varphi(x) \in Y(k)$. The cleanest way of looking at this is to think of it in terms of the functor of points: a point $X(k)$ is the same as a morphism $\text{Spec } k \to X$, and composing with $\varphi$ gives a morphism $\text{Spec } k \to Y$.

**Lemma 5.3.1.** Suppose that $\varphi : X \dashrightarrow Y$ is a rational map defined over $k$, where there exists a smooth $x \in X(k)$ and $Y$ is projective. Then $Y(k) \neq \emptyset$.

**Proof.** Let $\pi : X' \to X$ be the blowup of $X$ at $x$. Since $X$ is smooth at $x$. Let $E$ be the exceptional divisor, which is isomorphic to $\mathbb{P}^{\dim X-1}$. Now $X'$ is smooth near the generic point of $E$, and $Y$ is projective. The obvious rational map $\varphi' : X' \to Y$ is defined near the generic point of $E$. Thus we get an induced rational map $E \dashrightarrow Y$. Applying induction, we reduce to the case $\dim X = 1$, and $\varphi$ will be regular at any smooth point (since the image is projective).

**Corollary 5.3.2.** If $\varphi : X \dashrightarrow Y$ is a birational map (defined over $k$) and $X,Y$ are smooth and projective, then $X(k) \neq \emptyset \iff Y(k) \neq \emptyset$.

**Corollary 5.3.3.** If $X \dashrightarrow \mathbb{P}^n$ is birational (over $k$) and $X$ is smooth and projective, then $X(k) \neq \emptyset$.

**Definition 5.3.4.** A variety $X/K$ is called a Brauer-Severi variety if $X_k \simeq \mathbb{P}^n_k$.

**Example 5.3.5.** Suppose $k = \mathbb{Q}$ and $X = V(t_0^2 + t_1^2 + t_2^2) \subset \mathbb{P}^2_{\mathbb{Q}}$. This is evidently not isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$, but it is after base-changing to the algebraic closure.

**Theorem 5.3.6** (Châtelet). Suppose that $X$ is a Brauer-Severi variety over $k$. Then $X(k) \neq \emptyset \iff X \simeq \mathbb{P}^n_k$. 

39
\textbf{CHAPTER 5. THE BRAUER-MANIN OBSTRUCTION}

\textit{Proof.} One direction is obvious, so suppose that $X$ is Brauer-Severi with a rational point $x \in X(k)$. Since $X$ is geometrically smooth, $X$ is certainly smooth over $k$. In particular, $x$ is a smooth point. That implies that if $\pi : Y \to X$ is the blowup of $X$ at $x$, then the exceptional divisor $E$ is isomorphic to $\mathbb{P}^{n-1}_k$. Then we have $Y \subset X \times \mathbb{P}^{n-1}_k$.

The projection defines a map $Y \to \mathbb{P}^{n-1}_k$. If $L$ is the hyperplane divisor on $\mathbb{P}^{n-1}_k$, then $\pi_*\psi^*L$ is a divisor on $X$, which after base change to $\overline{k}$ becomes the class of the hyperplane divisor (by our understanding of the situation over an algebraically closed field). Therefore, it is base-point free already, and defines a map $X \to \mathbb{P}^{n-1}_k$. We know that this is an isomorphism after base-change to $\overline{k}$, so it is already an isomorphism. \qed

\textit{Definition 5.3.7.} Let $X$ be a variety defined over a number field $K$. We say that $X$ satisfies the Hasse principle if $X(K) \neq \emptyset \iff X(K_v) \neq \emptyset$ for all $v \in M_K$.

\textit{Example 5.3.8.} If $K = \mathbb{Q}$, this is saying that $X$ has a rational point over $\mathbb{Q}$ if and only if it has one in $\mathbb{R}$ and mod $p$ for all $p$.

It is a (very nontrivial) theorem that the Hasse principle holds for Brauer-Severi varieties. It also holds for smooth projective hypersurfaces of degree 2, but fails for some elliptic curves and some projective hypersurfaces of degree 3.

\textit{Example 5.3.9.} We present a variety which violates the Hasse principle.

Let $K = \mathbb{Q}$ and $X = V(t_0^3 - 5t_1^2 - t_3t_4, t_0^2 - 5t_2^3 - (t_3 + t_4)(t_3 + 2t_4)) \subset \mathbb{P}^4$. This is a smooth surface in $\mathbb{P}^4$. (In fact, it is a Fano variety.) Let $x_1 = (1 : 0 : \sqrt{-1} : 1 : 1)$, $x_2 = (5 : 5 : \sqrt{5} : 10 : -10)$, $x_3 = (0 : 0 : \sqrt{-5} : 5 : 0)$, and $x_4 = (0 : 5 : 2\sqrt{-15} : -25 : 5)$. At least one of these is defined over each $\mathbb{Q}_p$. More precisely, if $v \neq (2)$, then one of $x_1, x_2, x_3 \in X(\mathbb{Q}_p)$ and $x_4 \in X(\mathbb{Q}_2)$. It also clearly has real points.

We claim that $X(\mathbb{Q}) = \emptyset$. Suppose for the sake of contradiction that $x = (a : b : c : d : e) \in X(\mathbb{Q})$. We can assume that $d, e \in \mathbb{Z}$ and $(d, e) = 1$. If $p$ is a prime $\equiv \pm 2 \pmod{5}$, then we claim that $\text{ord}_p(de)$ is even. If not, then there are integers $\alpha, \beta, \gamma, \delta, \epsilon$ such that

$$\delta \epsilon = \alpha^2 - 5\beta^2, \text{ord}_p(\delta \epsilon) \text{ is odd, and } p \nmid \alpha \beta.$$ \nonumber

Then $\alpha^2 \equiv 5\beta^2(p) \implies 5$ is a square in $\mathbb{F}_p$. By quadratic reciprocity, this force $p \equiv \pm 1 \pmod{p}$.

Continuing in this way, we get $d \equiv \pm 1 \pmod{5}$ and $e \equiv \pm 1 \pmod{5}$. Similarly, we can show that $d + e \equiv \pm 1 \pmod{5}$ and $d + 2e \equiv \pm 1 \pmod{5}$. 

40
5.4 The Brauer group

The Brauer group is a natural abelian group associated to field $k$.

Definition 5.4.1. A central simple algebra (CSA) over $k$ is a finite dimensional, associative $k$-algebra with center $k$ with no non-zero proper two-sided ideals.

Example 5.4.2. The trivial CSA over $k$ is $A = k$.

Example 5.4.3. $M_n(k)$, the algebra of $n \times n$ matrices, is a CSA over $k$. The only non-obvious conditions are the “central” and “simple.” The “central” is familiar, and the “simple” is not too difficult to check either.

Example 5.4.4. Let $k$ be a field and $a, b \in K \setminus \{0\}$. Let $(a, b)_k$ be the associative $k$-algebra generated by $s, t$ such that $s^2 = a, t^2 = b, ts = -st$. $A = k \oplus k(s) \oplus k(t) \oplus k(st)$. For obvious reasons, this is called a “quaternion algebra.” If char $k \neq 2$, this is a central simple algebra.

A special class of central simple algebras consists of division algebras.

Definition 5.4.5. A central division algebra (CDA) over $k$ is a CSA over $k$ such that all non-zero elements are invertible.

Example 5.4.6. If $k = \mathbb{R}$, then the usual quaternions $\mathbb{H} = (-1, -1)_{\mathbb{R}}$ is a CDA/$k$.

Example 5.4.7. If $k$ is any field of characteristic not 2, then $(a^2, b)_k$ is not a CDA/$k$. Indeed, $(s + a)(s - a) = 0$ so $s + a$ is not invertible.

Theorem 5.4.8 (Wedderburn). If $A$ is a central simple algebra / $k$, then there exists a unique CDA $D / k$ such that $A \simeq M_n(D)$.

Remark 5.4.9. If $A$ and $B$ are CSAs / $k$ then $A \otimes_k B$ is a CSA / $k$. If $A$ is a CSA / $k$, then one can form a CSA algebra $A^{op}$ (this comes from the natural way of viewing a ring as a category), in which $a \cdot b$ is $b \cdot a$ in $A$. It is a fact that $A \otimes_k A^{op} \simeq M_n(k)$ for some $n$. The idea of this identification is define a map $A \otimes A^{op} \to \text{Hom}_k(A, A)$ sending $a \otimes b \mapsto (\alpha \mapsto a\alpha b)$. The kernel is a two-sided ideal, hence trivial. Surjectivity follows from dimension counting.

Definition 5.4.10. Let $k$ be a field. If $A, B$ are CSAs over $k$, we say that $A$ and $B$ are equivalent if there exists a CDA $D$ and integers $m, n$ such that $A \simeq M_m(D)$ and $B \simeq M_n(D)$.

Now the Brauer group of $k$, denoted $\text{Br}(k)$, is defined to be the set of equivalence classes of central simple algebras, with product $[A] \cdot [B] = [A \otimes_k B]$, inverse $[A]^{-1} = [A^{op}]$, and identity $k$.

Example 5.4.11. If $k$ is algebraically closed, then $\text{Br}(k) = 0$. Indeed, we claim that any CDA over $k$ is $k$. If $\alpha \in D \setminus k$, then $k \subset k[\alpha] \subset D$. Since $D$ is finite-dimensional, so is $k[\alpha]$. Moreover, this is an integral domain, hence a finite field extension of $k$. Since $k$ is algebraically closed that means $k \cong k[\alpha]$. 

41
Example 5.4.12. There is a result of Frobenius which says that the there are only two CDAs over \( \mathbb{R} \): \( \mathbb{R} \) and \( \mathbb{H} \). (There are three division algebras, the third being \( \mathbb{C} \) - but this is not central over \( \mathbb{R} \)). Therefore, \( \text{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z} \).

Example 5.4.13. \( \text{Br}(\mathbb{F}_q) = 0 \). The reason is that if \( D \) is a CDA over \( k \), then \( D \) is finite. Another result of Wedderburn implies that a finite CDA is a field. That forces \( D = \mathbb{F}_q \), and then the centrality forces \( q = p \).

5.5 The Brauer-Manin obstruction

Theorem 5.5.1. There is an isomorphism \( \text{inv}_p : \text{Br}(\mathbb{Q}_p) = \mathbb{Q}/\mathbb{Z} \). Moreover, there exists an exact sequence

\[
0 \to \text{Br}(\mathbb{Q}) \to \bigoplus_{v \in M_K} \text{Br}(\mathbb{Q}_v) \overset{\text{inv}_v}{\longrightarrow} \mathbb{Q}/\mathbb{Z} \to 0.
\]

There exists a similar exact sequence for any number field.

More generally, you can actually define Brauer groups for schemes. Suppose \( X \) is a scheme.

Definition 5.5.2. An Azumaya algebra over \( X \) is a locally free \( \mathcal{O}_X \)-algebra \( A \) of finite rank if for all \( x \in X \), \( A(x) \) is a central simple algebra over \( \kappa(x) \).

This is like a family of CSAs over the points of \( X \). Now if \( A \) and \( B \) is an Azumaya algebra over \( X \), then \( A \otimes_{\mathcal{O}_X} B \) is an Azumaya algebra over \( X \). We can similarly define the “opposite” of an Azumaya algebra. We can define an equivalence relation by \( A \sim B \) if there exist locally free sheaves \( \mathcal{E} \) and \( \mathcal{F} \) such that

\[
A \otimes \text{Hom}(\mathcal{E}, \mathcal{E}) \simeq B \otimes \text{Hom}(\mathcal{F}, \mathcal{F}).
\]

In addition, one checks that \( A \otimes A^{\text{op}} \) is equivalent to \( \mathcal{O}_X \). The Brauer group of \( X \) is the group given by the above equivalence classes.

Suppose that \( X \) is a variety over \( k \). We have a natural morphism

\[
\text{Spec } K \to X
\]

where \( K \) is the function field of \( X \). So we have a natural homomorphism \( \text{Br}(X) \to \text{Br}(K) \). If \( X \) is smooth over \( k \), it turns out that this is injective.

Remark 5.5.3. If \( k \) is a field, then \( \text{Br}(k) \) is equivalently defined as

- \( H^2_{\text{ét}}(\text{Spec } k, \mathbb{G}_m) \), or

- \( \text{Br}(K) = H^2(G, K^* \setminus \{0\}) \) where \( G = \text{Gal}(k^s/k) \). The first statement is basically a repackaging of this one.

- \( \text{Br}(K) \) is the “group of Brauer-Severi varieties over \( k \).”
Suppose that $X$ is a projective variety over $k$. Let $A_K$ be the ring of adeles for $k$. The adelic points of $X$ are $X(A_K)$, and any point can be written as a sequence of $(x_v \in X(k_v))$ such that all but finitely many of the coordinates are integers (in their respective fields).

For each $v \in M_K$, and for each $[A] \in Br(k)$, we obtain a map $X(k_v) \to Br(k_v)$ by pullback. Indeed, an element of $Br(X)$ is an Azumaya algebra on $X$, and we can pull it back via $x_v \in X(k_v)$ to get some $k_v$-algebra, which is a CSA by construction. Therefore, for each $A) \in Br(X)$ this fits into a commutative diagram

$$
\begin{array}{c}
X(k) \ar[r] \ar[d] & X(A_K) \ar[d] \\
0 \ar[r] & Br(k) \ar[r] & \bigoplus_{v \in M_K} Br(k_v) \ar[r] & \mathbb{Q}/\mathbb{Z} \ar[r] & 0
\end{array}
$$

The fact that this map is actually well defined is nontrivial (why does an Azumaya algebra restrict to the trivial CSA in $Br(k_v)$ for all but finitely many $v$?).

So we see that a necessary condition for $(x_v) \in X(A_K)$ to come from a global solution (i.e. from $X(k)$) is that $(x_v) \to 0$ in $\mathbb{Q}/\mathbb{Z}$. For any $B \subset Br(X)$, we define

$$X(A_K)^B = \{(x_v) \in X(A_K) \mid (x_v) \to 0 \in \mathbb{Q}/\mathbb{Z} \text{ for all } [A] \in B\}.$$

**Definition 5.5.4.** Note that we always have $X(K) \subset X(A_K)^{Br(X)} \subset X(A_K)$. If $X(A_K) \neq \emptyset$ but $X(A_K)^{Br(X)} = \emptyset$, then we say that there is a Brauer-Manin obstruction to the Hasse principle.

**Example 5.5.5.** Recall that $X = V(t_0^2 - 5t_1^2 - t_3t_4, t_0^2 - 5t_2^2 - (t_3 + t_4)(t_3 + 2t_4)) \subset \mathbb{P}^4_Q$ is a counterexample to the Hasse principle (it has local solutions, but no global solutions). We did this by elementary, explicit arguments. What if we try to find a Brauer-Manin obstruction?

Let $K$ be the function field of $X$ and recall that we have an injection $Br(X) \hookrightarrow Br(K)$. Let $[A_1], \ldots, [A_r] \in Br(K)$. Then for each $i$ there is an open subset $U_i \subset X$ such that the functions and elements involved in a multiplication table for $A_i$ are defined and non-zero on $U_i \subset X$. The $A_i$ determine an Azumaya algebra over $U_i$, if $U_i$ is small enough. If $X = \bigcup U_i$ and the $A_{U_i}$ agree on overlaps (in particular, they are the same class in $Br(K)$), then they glue together to define an Azumaya algebra $A/X$.

In our particular example, consider the following quaternion algebras over $K$:

$$\left(\frac{5}{t_3 + t_4}\right)_K, \left(\frac{t_3}{t_3 + t_4}\right)_K, \left(\frac{t_4}{t_3 + t_4}\right)_K, \left(\frac{t_3}{t_3 + 2t_4}\right)_K, \left(\frac{5_4}{t_3 + 2t_4}\right)_K.$$

A relatively easy calculation reveals that these are all isomorphic as CSAs over $K$. This list can be extended to a list that determines an Azumaya algebra on $X$.

We will try to describe the maps $X(Q_v) \to Br(Q_v) \to \mathbb{Q}/\mathbb{Z}$. This is a case-by-case analysis. Suppose $v$ is archimedean (the standard real place of $\mathbb{Q}$), so $\mathbb{Q}_v = \mathbb{R}$. Pick
CHAPTER 5. THE BRAUER-MANIN OBSTRUCTION

$x_v \in X(\mathbb{R})$. If $f = \frac{t^3}{t^3+t^4}$ is regular at $x_v$ and non-zero, so $\mathcal{A}(x_v) = (5, f(x_v))_{\mathbb{Q}_v=\mathbb{R}}$ is trivial in $\text{Br}(\mathbb{R})$ because 5 is a square. In particular, its image is zero in $\mathbb{Q}/\mathbb{Z}$. To show that the map is trivial for all $x_v$, either extend the list of algebras or use some continuity argument.

Now suppose $v$ is a nonarchimedean place. Assume $p \neq 2$ and 5 is a square in $\mathbb{Q}_p$. The same arguments as in the case $\mathbb{Q}_v = \mathbb{R}$ show that $X(\mathbb{Q}_p) \rightarrow \mathbb{Q}/\mathbb{Z}$ is zero. Suppose $p \neq 2, 5$ but 5 is not a square in $\mathbb{Q}_p$. Then 5 is not a square in $\mathbb{F}_p$, by Hensel’s Lemma. If $x_v = (a_0 : \ldots : a_4) \in X(\mathbb{Q}_p)$, $a_i \in \mathbb{Z}_p$, then by looking at the equations defining $X$ we can assume that $a_3 \neq 0 \pmod{p}$ or $a_4 \neq 0 \pmod{p}$. Then $\mathcal{A}(x_v) = (5, b)_{\mathbb{Q}_p}$ where $b \in \mathbb{Z}_p \setminus \{0\}$. By class field theory, that means that $\text{inv}_v(\mathcal{A}(x_v)) = \frac{1}{2}$.

The case $p = 2$ is similar, and we find that the invariant map is trivial again.

Finally, we consider the case $p = 5$. Considering the equations of $X$ mod 5, we see that

$$(a_3 - a_4)(a_3 - 2a_4) \equiv 0 \pmod{5} \text{ and } \pm a_0 \equiv a_3 \equiv a_4 \pmod{5}.$$

Now if $x_v \in X(\mathbb{Q}_5)$, $\text{inv}_v(\mathcal{A}(x_v)) = (5, 3)_{\mathbb{Q}_2} = \frac{1}{2}$ again by class field theory (since $\frac{a_3}{a_3+a_4} \equiv 3 \pmod{5}$). This gives a Brauer-Manin obstruction.
Chapter 6

Birational Geomery

6.1 Potential density

For this section, we will assume that all varieties are geometrically irreducible.

Definition 6.1.1. If $X$ is a variety over a field $k$, we say that the $k$-rational points are dense if $X(k)$ is dense in $X$ (in the Zariski topology). We say that the rational points are potentially dense if $X(k')$ is dense for some finite extension $k'/k$.

Remark 6.1.2. Density is hard to analyze; potential density is easier.

Example 6.1.3. Suppose $X$ is a Brauer-Severi variety over $k$. If $X(k) \neq \emptyset$, then $X \simeq \mathbb{P}^n_k$ so $X(k)$ is dense if $k$ is a number field, and $X(k)$ is not dense if $k$ is a finite field. (In fact, we never get density for finite fields for positive-dimensional varieties.) So any Brauer-Severi variety over any number field is potentially dense.

Example 6.1.4. Suppose that $X$ is a smooth projective variety of dimension 1. If $g(X) = 0$, then $X$ is a Brauer-Severi variety.

If $g(X) = 1$, then $X(k)$ may be finite or infinite (i.e. not dense or dense). But potentially density always holds.

If $g(X) \geq 2$, and we are over a number field, then potential density never holds since $X(k)$ is always finite (Faltings).

Example 6.1.5. Suppose $X = C \times Y$ where $C$ is a smooth projective curve of genus $g \geq 2$ and $Y$ is a smooth projective variety over $K$, a number field. Then potential density fails for $X$ because it does for $C$.

Example 6.1.6. Suppose $X$ is an abelian variety of dimension $> 1$ over $k$ a number field. Let $\Gamma$ be the torsion subgroup of $X(\overline{k})$. In trying to show that potential density holds for $X$, we can pass to a finite extension. Then we may assume that there exists a smooth projective curve $C \subset X$ defined over $k$ with $g(C) \geq 2$. By the Manin-Mumford conjecture (proved by Raynaud), $\Gamma \cap C(\overline{k})$ is finite. Pick $x \in C \setminus \Gamma(k)$. Then $G = \mathbb{Z}x \subset X(k)$ is infinite.
First assume that \( A \) is simple (i.e. has no nontrivial abelian subvarieties). Let \( Y = \overline{G} \) in the Zariski topology. By a result of Faltings, \( Y \) is a finite union of abelian subvarieties, so \( Y = X \).

If \( X \) is not simple, then by the theory of abelian varieties \( X \) is a product \( X = X' \times X'' \) of abelian varieties. Then we apply induction. If \( X' \) or \( X'' \) has dimension one, \( G \) shows that \( X'(k) \) or \( X''(k) \) is dense (since it’s infinite). If \( X \) has dimension one, then we get potential density for \( X \times X \), hence potential density for \( X \).

\[ \textbf{6.2 Kodaira dimension} \]

Suppose \( X \) is a smooth projective variety over a field \( k \). Let \( K_X \) be the canonical divisor of \( X \).

**Definition 6.2.1.** We define the Kodaira dimension of \( X \) as follows: if \( h^0(X, mK_X) = 0 \) for all \( m > 0 \), then define \( \kappa(X) = -\infty \). If \( h^0(X, mK_X) > 0 \) for some \( m > 0 \), let \( \kappa(X) \) be the largest \( \ell \) such that

\[
0 < \limsup_{m \to \infty} \frac{h^0(X, mK_X)}{m^\ell} < \infty.
\]

In other words, \( h^0(X, mK_X) \) grows like \( m^\ell \). It is a fact that this \( \ell \) exists. Think of \( h^0(X, mK_X) \) as being like a polynomial, and the Kodaira dimension as being the degree. (Aside: \( \chi(mK_X) \) is a polynomial, and if we have some sort of positivity condition on \( K_X \) that kills the higher cohomology, then it is a polynomial for \( m \gg 0 \).) It turns out that \( \kappa(X) \in \{-\infty, 0, 1, \ldots, \dim X\} \).

**Definition 6.2.2.** If \( \kappa(X) = \dim X \), we say that \( X \) is of “general type.”

**Example 6.2.3.** If \( X \) is a curve, then

\[
\kappa(X) = -\infty \iff g(X) = 0 \\
\kappa(X) = 0 \iff g(X) = 1 \\
\kappa(X) = 1 \iff g(X) \geq 2
\]

**Conjecture 6.2.4.** If \( X \) is a smooth, projective variety over \( k \) a number field. Then if \( \kappa(X) = \dim X \), potential density fails. If \( \kappa(x) = 0 \), then potential density holds.

We know that if \( X \) is Fano (\( -K_X \) is ample, so \( \kappa(X) = -\infty \)), then potential density holds.

\[ \textbf{6.3 Surface fibrations} \]

We assume that \( X \) is a smooth projective surface over \( k \) an algebraically closed field.

**Definition 6.3.1.** We say that a curve \( E \subset X \) is a \((-1)\)-curve if \( E \simeq \mathbb{P}^1 \) and \( E^2 = E \cdot E = -1 \).
If $E$ is a $(-1)$-curve, then Castelnuovo’s theorem says that $E$ is the exceptional divisor of a blowup $X \xrightarrow{\pi_1} X_1$. Repeating, we obtain a sequence

$$X \rightarrow X_1 \rightarrow \ldots \rightarrow X_n = Y$$

where $Y$ has no $-1$ curves.

The classification of surfaces.

- If $\kappa(X) = \kappa(Y) = -\infty$ then $Y \cong \mathbb{P}^2$ or a conic fibration $Y \rightarrow C$ where the general fiber $\mathbb{P}^1$ and $C$ is a smooth projective curve.
- If $\kappa(X) = \kappa(Y) = 0$ then $Y$ is an abelian variety or a $K_3$ surface (the canonical bundle is trivial) or a finite quotient of one of these.
- If $\kappa(X) = \kappa(Y) = 1$ then there exists an elliptic fibration $X \rightarrow C$ (a map to a smooth projective curve whose general fiber is an elliptic curve).
- If $\kappa(X) = \kappa(Y) = 2$ then $X$ and $Y$ are of general type.

Note that $\kappa(X) = \kappa(Y)$ since the Kodaira dimension is a birational invariant, so this covers all cases.

If $k$ is not algebraically closed, then the same holds after replacing by a finite extension (another reason why it’s nicer to consider potential density).

Example 6.3.2. Let $X$ be a smooth projective surface over a number field $k$, with $\kappa(X) = -\infty$. We can assume that $X = \mathbb{P}^2$ or there exists a conic bundle $X \rightarrow C$. The case $X = \mathbb{P}^2$ is clear, so we consider the other case. After passing to an extension, we get a morphism to a smooth projective curve whose fibers are smooth projective curves of genus 0 (in particular, the generic fiber is such.) By a variant of Tsen’s Theorem applied to the generic fiber (thinking of the generic fiber as a curve over the function field), there is a section

$$C \longrightarrow X \quad \longrightarrow C$$

This lets us lift rational points from $C$ to $X$. There are several cases to consider:

- if $g(C) = 0$, then we can assume that $C \cong \mathbb{P}^1$ (after passing to a finite extension). For almost all $s \in C(k)$, the fiber $X_s$ over $s$ is a smooth projective curve of genus 0. Now, using $\varphi$ we get $X_s(k) \neq \emptyset$, so $|X_s(k)|$ is infinite. Putting these all together, we get a dense set of rational points for $X$.
- if $g(C) = 1$, the same argument applies after passing to a finite extension to obtain infinitely many rational points for $C$.  

47
• if $g(C) \geq 2$, then potential density fails for $X$ because it fails for $C$.

In view of the classification of surfaces, it is natural to ask the following: suppose $\varphi : X \to C$ is an elliptic fibration over a number field $K$, where $C$ is a smooth projective curve and $X$ is a smooth projective surface. Does potential density hold for $X$?

Example 6.3.3. Let’s thinking about the triviale example: $X = E \times C$ where $E$ is an elliptic curve over $k$ and $C$ is a smooth projective curve over $k$. Let $\varphi : X \to C$ denote the projection. If $g(C) = 0$ or 1, then potential density holds because it does for both factors. If $g(C) \geq 2$, then potential density fails because it fails for $C$.

Before going on, let’s remind ourselves of a fact (cf. Hindry-Silverman, “Diophantine geometry” exercise C7):

Theorem 6.3.4 (Chevalley-Weil). Suppose $\pi : X' \to X$ is an étale morphism between smooth (or just normal) projective varieties over $k$ a number field. Then there exists a finite extension $k'/k$ such that $\pi^{-1}(X(k)) \subset X'(k')$.

This is analogous to the “monodromy theorem” in topology, which says that if $X' \to X$ is a covering space, then any path in $X$ lifts to $X'$.

Example 6.3.5. Suppose $k$ is a number field, $E$ is an elliptic curve over $k$, and $C$ is a smooth projective curve. Assume that $E(k)$ contains a nontrivial 2-torsion point $\alpha$. Define $\sigma : E \to E$ by $\sigma(e) = e + \alpha$. This is an involution, since $\alpha$ is 2-torison. Assume that we also have an involution on $C$, say $\tau : C \to C$, and suppose the quotient $C/\langle \tau \rangle$ is $\mathbb{P}^1$. (In other words, $C$ is hyperelliptic: any two degree two map to $\mathbb{P}^1$ gives such an involution.)

Now we can define an involution on $\mu : E \times C \to E \times C$ by $(e, c) \mapsto (\sigma(e), \tau(c))$. This has no fixed points (since translation on $E$ already doesn’t). Therefore, the map $E \times C \to E \times C/\langle \mu \rangle$ is étale.

\[
\begin{array}{ccc}
E \times C & \xrightarrow{\varphi} & C \\
\downarrow & & \downarrow \\
E \times C/\langle \mu \rangle & \xrightarrow{\psi} & C/\langle \tau \rangle = \mathbb{P}^1
\end{array}
\]

• If $g(C) = 0$, then potential density for $E \times C$ implies it for $X$. (Potential density is always preserved under dominant morphisms.) $[\kappa(X) = -\infty]$

• If $g(C) = 1$, then potential density for $E \times C$ implies it for $X$, by the same argument. $[\kappa(X) = 0]$

• If $g(C) \geq 2$, then potential density fails for $C$, hence fails for $E \times C$, hence fails for $X$ by Chevalley-Weil. $[\kappa(X) = 1]$
6.3. SURFACE FIBRATIONS

Remark 6.3.6. If $X \to Y$ is a morphism and $Y$ is of general type, then Lang's conjecture says that potential density fails for $Y$. Therefore, it fails for $X$ as well. You might think that having a map to a variety of general type is the only obstruction to potential density. However, in the above example with $g(C) \geq 2$, you can show that there is no surjective map $X \to Y$ where $Y$ is of general type ($X$ is an elliptic fibration over $\mathbb{P}^1$, so you can’t have such a map to a curve of genus $g \geq 2$.)

General methods for elliptic fibrations. Suppose there exists a section

\[
\begin{array}{ccc}
C & \longrightarrow & X \\
\downarrow & & \downarrow \varphi \\
C & \longrightarrow & \\
\end{array}
\]

and a multisection

\[
\begin{array}{ccc}
M & \longrightarrow & X \\
\downarrow & & \downarrow \varphi \\
C & \longrightarrow & \\
\end{array}
\]

where $M$ is a smooth projective curve mapping surjectively to $C$. The existence of a section says that the general fiber has a rational point, and is therefore an elliptic curve (over $k$). Suppose $C(k)$ is dense and $M(k)$ is dense. (We can think of the section as the $0$-section, picking out the identity along each fiber and making $X$ an abelian scheme over $C$.)

Each $x \in M(k)$ gives a rational point on some fiber of $\varphi$. If most of these points are non-torsion, then we get potential density for $X$ (since we thus get infinitely many points on these fibers). However, this non-torsion condition is kind of weird - we should explore what kind of nice geometric conditions imply this.

Lemma 6.3.7. If there exists $c \in C$ such that $\varphi$ is smooth over $c$, and $M \to C$ is not smooth over $c$, then the non-torsion condition holds on $\varphi^{-1}(c)$.

Proof sketch. Here’s a sketch of the proof. For any $m \in \mathbb{N}$, there exists a divisor $D_m \subset X$ such that torsion points of order $m$ are all inside $D_m$.

First assume that there exists $m$ such that $M \subset D_m$. Then if $X_C \to C_C, M_C, (D_m)_C$ denote the base-changes to $\mathbb{C}$, there exists a sequence $c_1, c_2, \ldots \to c$ such that $M \to C$ is étale over $c_i$. Since $M \to C$ is not étale, the degree of the map is at least 2. Over $c_i$, we get at least two points $p_i, p'_i$ in $M_C$ both converging to the same point. But we also have that $p_i - p'_i$ is $m$-torsion for each $i$, which is a contradiction.

On the other hand, if $M \not\subset D_m$ for any $m$ then most of the points in $M(k)$ are non-torsion by Merel’s theorem (for any fixed number field $k$, there exists $m_0$ depending (only) on $k$ such that any elliptic curve over $k$ has no torsion points of order $m \geq m_0$).
Suppose that you have a multisection $M$, but no section $C$. We can base change by $M$ to a family over $M$ with a section.

\[ M \times_C M \longrightarrow M \times_C X \longrightarrow X \]

\[ \downarrow \quad \downarrow \quad \downarrow \]

\[ M \longrightarrow C \]

Then you can apply techniques that we have already discussed.
Chapter 7

Statistics of Rational Points

7.1 Counting on projective space

Let $k$ be a number field, $X \subset \mathbb{P}^n_k$ a projective variety over $k$. Let $H_k$ be the usual height function on $\mathbb{P}^n_k$. Define a counting function on $X(k)$:

$$N(X(k), B) = \#\{x \in X(k) \mid H_k(x) \leq B\}.$$ 

The general question is what it looks like, e.g. does it grow like a polynomial?

It is difficult to say anything in general, but for special classes of varieties we can say something.

**Theorem 7.1.1.** Assume $X \subset \mathbb{P}^n_k$ is a smooth projective curve such that $X(k) \neq \emptyset$. Then there are constants $a, b$ depending on $k$ and the embedding such that

$$N(X(k), B) = \begin{cases} 
  aB^b + o(B^b) & g = 0 \\
  a \log B + o(\log B) & g = 1 \\
  a + o(1) & g \geq 2
\end{cases}$$

**Proof.** If $g(X) = 0$, then $X \simeq \mathbb{P}^1_k$, and the result will follow from the next theorem.

If $g(X) = 1$, then $X$ is an elliptic curve, and the result will follow from next lecture.

If $g(X) \geq 2$, then the result follows from Falting’s theorem. \hfill \Box

**Theorem 7.1.2** (Schanuel). If $X = \mathbb{P}^n_k$, then there exists a constant $a$ depending on $k, n$ such that

$$N(X(k), B) = aB^{n+1} + o(B^{n+1}).$$

Moreover,

$$a = \frac{hR}{\omega \zeta_K(n+1)} \left( \frac{2r_1(2\pi)^{r_2}}{\sqrt{D}} \right)^{n+1} (n+1)^{r_1+r_2-1}.$$
Remark 7.1.3. Here we use the standard notation of algebraic number theory: $h$ is the class number of $\mathcal{O}_k$, $R$ is the regulator, $\omega$ is the number of roots of unity, $\zeta_k$ is the (Dedekind) zeta function of $k$, $r_1$ is the number of real embeddings, $r_2$ is the number of conjugate pairs of complex embeddings, and $D$ is the absolute value of discriminant of $K/\mathbb{Q}$.

Proof. We treat only $K = \mathbb{Q}$, where we have $h = 1, R = 1, \omega_2, r_1 = 1, r_2 = 0, D = 1$.

If $x = (a_0, \ldots, a_n) \in \mathbb{A}^{n+1}(\mathbb{Z})$, put $|x| = \max\{|a_i|\}$ and $\gcd(x) = \gcd(a_0, \ldots, a_n)$.

Define functions

$$M(B) = \# \{ x \in \mathbb{A}^{n+1}(\mathbb{Z}) \mid x \neq 0, |x| \leq B \}.$$ 

Also set

$$M(B, d) = \# \{ x \in \mathbb{A}^{n+1}(\mathbb{Z}) \mid \gcd(x) = d, |x| \leq B \}.$$

There are various relations among these, e.g. $M(B, d) = M(B/d, 1)$ because if $x$ is counted in $M(B, d)$, then dividing through all coordinates by $d$ gives an element of $M(B/d, 1)$.

Since

$$M(B) = \sum_{d \in \mathbb{N}} M(B, d) = \sum_{d \in \mathbb{N}} M(B/d, 1)$$

the Möbius inversion formula says

$$M(B, 1) = \sum_{d \in \mathbb{N}} \mu(d) M(B/d).$$

Now

$$M(B) = \# \{ a \in \mathbb{Z} \mid |a| \leq B \}^{n+1} - 1 = (2|B| + 1)^{n+1} - 1.$$ 

If we plug this in to the Möbius inversion formula, we get

$$M(B, 1) = \sum_{d \in \mathbb{N}} \mu(d) \left( (2|B/d| + 1)^{n+1} - 1 \right)$$

$$= \sum_{1 \leq d \leq B} \mu(d) \left( \left( \frac{2B}{d} \right)^{n+1} + O \left( \left( \frac{B}{d} \right)^n \right) \right)$$

$$= (2B)^{n+1} \frac{1}{\zeta(n+1)} + O(B^{n+1})$$

because

$$\sum_{d \in \mathbb{N}} \frac{\mu(d)}{d^{n+1}} = \frac{1}{\zeta(n+1)}.$$

Finally, note that $N(\mathbb{P}^n(\mathbb{Q}), B) = \frac{1}{2} M(B, 1)$, since any point in $\mathbb{P}^n(\mathbb{Q})$ has a unique representative with integer coordinates whose gcd is 1, except up to multiplying everything by $-1$. $\Box$
Example 7.1.4. Let $X = \mathbb{P}_k^n$ and consider the $l$-tuple Segre embedding $X \subset \mathbb{P}_k^m$ (here $m = \binom{n+l}{l} - 1$).

The previous theorem says that the counting function for $X(k)$ with respect to the embedding $X = \mathbb{P}_k^n$ is $N(X(k), B) = aB^{n+1} + o(B^{n+1})$.

Under the Segre embedding, we get instead $\tilde{N}(X(k), B) = aB^{n+1} + o(B^{n+1})$ as $B \to \infty$. The degree is smaller, which is to be expected because the coordinates are “bigger.” How can we see this?

Recall that $H_{\mathbb{P}_k^n}(x) = \prod_{v \in M_k} \max \{ ||a_i||_v \}$ and $H_{\mathbb{P}_k^m}(x) = \prod_{v \in M_k} \max_j \{ ||\phi_j(x)||_v \}$

where the $\phi_j$ are a basis for $\ell$-degree polynomials, so this is exactly $H_{\mathbb{P}_k^n}(x)^\ell$. Therefore,

$$\tilde{N}(X(k), B) = \# \{ x \in X(k) \mid H_{\mathbb{P}_k^n}(x) \leq B \} = N(X(k), B^{1/\ell}).$$

Remark 7.1.5. We could take a height function $H_L$ with respect to some ample divisor and we can define a counting function $N(X(k), B, L) = \# \{ x \in X(k) \mid H_L(x) \leq B \}$. The most interesting case is when $X$ is a Fano variety, and we have the natural choice $L = -K_X$. For instance, this applies to hypersurfaces $X \subset \mathbb{P}^n$ of degree $\leq n$.

7.2 Counting on abelian varieties

Let $X \subset \mathbb{P}_k^n$ be an abelian variety over $k$ a number field. Suppose that $\Gamma$ is a subgroup of $X(k)$, and let $r = \text{rank } \Gamma$.

Theorem 7.2.1. Let $L$ be the hyperplane divisor on $\mathbb{P}_k^n$, so $L|_X$ is a symmetric ample divisor. Then

$$N(\Gamma, B) = N(X(k), B)|_\Gamma = a \log^{r/2}(B) + o(\log^{r/2} B).$$

Proof. Let $\hat{h}$ be the canonical height function associated to $L|_X$. Recall that

$$h_{\mathbb{P}_k^n} = \hat{h} + \text{ bounded function}.$$ 

It is enough to show that $N'(\Gamma, B) = aB^{r/2} + o(B^{r/2})$, where

$$N'(\Gamma, B) = \# \{ x \in \Gamma \mid \hat{h}(x) \leq B \}.$$ 

This canonical height is nice to work with: recall in particular we proved that it is a quadratic form. Tensoring with $\mathbb{R}$, we get a quadratic form $\hat{h} : \Gamma \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}$. (This is non-trivial, but left as an exercise.) Now let $\Lambda \subset \mathbb{R}^r$ be the image of $\Gamma$ (it will be a lattice). It then suffices to show that

$$\# \{ \lambda \in \Lambda \mid q(\lambda) \leq B \} = aB^{1/2} + o(B^{1/2}).$$

This is more or less obvious: the number of lattice points inside a region of radius $\sqrt{B}$ is about $B^{r/2}$. Details are left as an exercise.
CHAPTER 7. STATISTICS OF RATIONAL POINTS

7.3 Jacobians of curves

How do you get abelian varieties (of dimension $\geq 1$)? The easiest way is to take the Jacobian of a curve.

Suppose $X$ is a smooth projective curve over field $k$ which is geometrically irreducible. Then $\text{Pic}(X_k)$ is an abelian group, and there is an exact sequence

$$0 \to \text{Pic}^0(X_k) \to \text{Pic}(X_k) \xrightarrow{\text{deg}} \mathbb{Z} \to 0.$$  

So $\text{Pic}^0(X)$ is also an abelian group. It turns out that $\text{Pic}^0(X_k)$ is a variety, and this group structure makes it into an abelian variety. This is denoted $J_k$. We have a morphism

$$X_k \to J_k$$

sending $y$ to the class of $y - x$, for any fixed point $x \in X_k$.

- If $g(X) = 0$, then $X_k = \mathbb{P}^1_k$ and $\text{Pic}^0(X_k) = 0$.
- If $g(X) = 1$, then $\text{Pic}^0(X) \simeq X$.
- If $g(X) \geq 2$, then $X_k \to J_k$ is an embedding.

It is always the case that $\dim J_k = g(X)$.

If $X(k) \neq \emptyset$, then there is an abelian variety $J$ over $k$ and a morphism $X \to J$ whose base change to the algebraic closure recovers $X_k \to J_k$. From now aone, we assume that $g(X) \geq 2$ and $k$ is a number field, so we get an embedding $X(k) \subset J(k)$.

By the theorem we just proved,

$$N(X(k), B) \leq a(\log B)^{r/2}$$  

where $r = \text{rank } J(k)$.

This seems silly, since Faltings proved that $X$ has finitely many points. But that result is very difficult. Mumford proved a stronger estimate $N(X(k), B) \leq c \log \log B$, and this was further developed to give an alternate proof of Faltings’ Theorem.

Now assume that $k = \mathbb{C}$. We have an exact sequence

$$0 \to \mathbb{Z} \to \mathbb{C} \xrightarrow{\exp} \mathbb{C}^* \to 0.$$  

There is an associated short exact sequence of sheaves,

$$0 \to \mathcal{O}_X \to \mathcal{O}_X^* \to 0.$$  

The long exact sequence of cohomology then gives

$$0 \to H^1(\mathbb{Z}_X) \to H^1(\mathcal{O}_X) \to H^1(\mathcal{O}_X^*) \to H^2(\mathbb{Z}_X) \to \ldots$$  

and $H^1(\mathcal{O}_X^*) \cong \text{Pic}(X)$, the boundary homomorphism being the degree (or first Chern class). The kernel is $\text{Pic}^0(X)$, which by exactness is $\text{Pic}^0(X) \cong H^1(\mathcal{O}_X) / H^1(\mathbb{Z}_X)$. This is a complex torus.
Chapter 8

Zeta functions

8.1 The Hasse-Weil zeta function

Definition 8.1.1. Let $X$ be a variety over $\mathbb{F}_q$. Let $N_m = \# X(\mathbb{F}_q^m)$ for $m \geq 1$. The Hasse-Weil zeta function of $X$ is defined to be

$$Z_X(t) := \exp \left( \sum_{m=1}^{\infty} \frac{N_m t^m}{m} \right) \in \mathbb{Q}[[t]].$$

Example 8.1.2. Suppose $X = \mathbb{A}^n_{\mathbb{F}_q}$. Then $N_m = \# X(\mathbb{F}_q^m) = q^{mn}$. So

$$Z_X(t) = \exp \left( \sum_{m=1}^{\infty} \frac{q^{mn} t^m}{m} \right)$$

$$= \exp \left( \sum_{m=1}^{\infty} \frac{(q^n t)^m}{m} \right)$$

$$= \exp \left( - \log(1 - q^n t) \right)$$

$$= \frac{1}{1 - q^n t}.$$

Example 8.1.3. Say $X = \mathbb{A}^n_{\mathbb{F}_q}$ and $Y$ is a variety over $\mathbb{F}_q$. We try to compute $Z_{X \times Y}(t)$. Well,

$$\#(X \times Y)(\mathbb{F}_q^m) = \# X(\mathbb{F}_q^m) \# Y(\mathbb{F}_q^m).$$
So
\[
Z_{X \times Y}(t) = \exp \left( \sum_{m \geq 1} \frac{\#X(F_q^m)\#Y(F_q^m)}{m} t^m \right)
\]
\[
= \exp \left( \sum_{m \geq 1} \frac{\#Y(F_q^m)}{m} (q^m t)^m \right)
\]
\[
= Z_Y(q^m t).
\]

Lemma 8.1.4. Suppose $X$ is a variety over $\mathbb{F}_q$ and $Y \subset X$ is a closed subset, $U = X \setminus Y$. Then
\[
Z_X(t) = Z_Y(t)Z_U(t).
\]

Proof. \#$X(F_q^m) = \#Y(F_q^m) + \#U(F_q^m)$. When we take the exponential, the addition is turned into multiplication:
\[
Z_X(t) = \exp \left( \sum_{m \geq 1} \frac{\#Y(F_q^m) + \#U(F_q^m)}{m} t^m \right) = Z_Y(t)Z_U(t).
\]

Example 8.1.5. Let $X = \mathbb{P}_q^n$. Let $Y$ be a hyperplane, e.g. $V(t_0)$. Then $Y \simeq \mathbb{P}_{q}^{n-1}$ and $U \simeq A_{q}^{n}$, so
\[
Z_X(t) = Z_Y(t)Z_U(t) = Z_Y(t) \frac{1}{1-q^m t},
\]
so we see (e.g. by induction) that
\[
Z_X(t) = \prod_{k=1}^{n} \frac{1}{(1-t)(1-qt)\ldots(1-q^mt)}.
\]

Theorem 8.1.6. Let $X$ be a variety over $\mathbb{F}_q$. Then we have the formula
\[
Z_X(t) = \prod_{x \text{ closed } \in X} \frac{1}{1-t^{\deg(x)}}.
\]

Proof. Suppose $a_r$ is the number of closed points $x \in X$ having degree $r$. Consider the base change
\[
X_{\mathbb{F}_q^m} \longrightarrow X
\]
\[
\text{Spec } \mathbb{F}_q^m \longrightarrow \text{Spec } \mathbb{F}_q.
\]
Now, there is a natural bijection $X(\mathbb{F}_q^m) \leftrightarrow X_{\mathbb{F}_q^m}(\mathbb{F}_q^m)$ by the definition of base change. If $x' \in X_{\mathbb{F}_q^m}(\mathbb{F}_q^m)$ and $x$ is the image of $x'$ in $X$, then $\deg x \mid m$, since $\mathbb{F}_q \subset \kappa(x) \subset \kappa(x') = \mathbb{F}_q^m$. 

56
If deg $x = r$, then Aut($\mathbb{F}_{q^r}/\mathbb{F}_q$) acts on $x'$ if $x' \in X_{q^m}(\mathbb{F}_{q^r})$. That is, the base-change of $x = \text{Spec} \mathbb{F}_q$ has degree $r$ in $X_{q^m}$. We conclude that

$$N_m = \#X(\mathbb{F}_{q^m}) = \#X_{q^m}(\mathbb{F}_{q^m}) = \sum_{r|m} ra_r.$$ 

Now, consider

$$\sum_{m \geq 1} \frac{N_m}{m} t^m = \sum_{m \geq 1} \frac{\sum_{r|m} ra_r}{m} t^m$$

$$= \sum_{r \geq 1} a_r \sum_{\ell \geq 1} \frac{1}{\ell^r \ell}$$

$$= \sum_{r \geq 1} a_r \log \left(\frac{1}{1 - t^r}\right)$$

Corollary 8.1.7. If $X$ is a variety over $\mathbb{F}_q$, then $Z_X(t) \in \mathbb{Z}[[t]]$.

Theorem 8.1.8 (Weil conjecture). Let $X$ be a smooth projective variety, which is geometrically irreducible. Then the zeta function $Z_X(t)$ satisfies:

1. $Z_X(t) \in \mathbb{Q}(t)$ is a rational function.
2. $Z_X(t)$ satisfies the functional equation

$$Z_X\left(\frac{1}{q^n t}\right) = \pm q^{ne/2} t^e Z_X(t) \text{ for some } e.$$

3. (“Riemann Hypothesis”) We have

$$Z_X(t) = \frac{P_1(t)P_3(t)\ldots P_{2n-1}(t)}{P_0(t)\ldots P_{2n}(t)}$$

where $P_i(t) \in \mathbb{Z}[t]$, $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$, and for $1 \leq i \leq 2n - 1$,

$$P_i(t) = \prod (1 - \alpha_{i,j} t)$$

where $\alpha_{i,j}$ are algebraic integers with $|\alpha_{i,j}| = q^{i/2}$.
8.2 The Frobenius Morphism

Let $\mathbb{F} = \overline{\mathbb{F}}_q$. Then we can define a Frobenius homomorphism $F : \mathbb{F} \rightarrow \mathbb{F}$ by sending $a \mapsto a^q$. The key point is that

$$\mathbb{F}_q^m = \{ a \in \mathbb{F} \mid F^m(a) = a \}.$$

Suppose $X$ is a variety over $\mathbb{F}_q \subset \mathbb{P}^n_{\mathbb{F}_q}$. Then $F^m$ induces a morphism $\mathbb{P}^n_{\mathbb{F}_q} \rightarrow \mathbb{P}^n_{\mathbb{F}_q}$. Since $\mathbb{F}_q$ is fixed by $F^m$, this is an endomorphism of $X$. That gives an interpretation

$$N_m = \#X(\mathbb{F}_q^m) = \#{\{x \in X \mid F^m(x) = x\}}.$$ 

The motivation for the Weil conjectures is an analogy to the Lefschetz Fixed Point Theorem, applied to the Frobenius.

8.3 The Weil conjectures for curves

We assume throughout that $X$ is a smooth projective curve over $\mathbb{F}_q$. Recall that a divisor on $X$ is an expression of the form

$$D = \sum d_i D_i$$

where the $d_i \in \mathbb{Z}$ and the $D_i$ are closed points on $X$. The degree of $D$ is $\sum d_i \deg D_i$, where $\deg D_i := [\kappa(D_i) : \mathbb{F}_q]$. (By the Nullstellensatz, $\deg D_i = 1$ if we are working over an algebraically closed field.) So this gives a homomorphism $\text{Pic}(X) \rightarrow \mathbb{Z}$.

Fix $L \in \text{Pic}(X)$. Define the linear system of $L$ to be

$$|L| = \{ D \geq 0 \mid D \sim L \}.$$ 

This is precisely the projectivization of $H^0(X, L) := H^0(X, \mathcal{O}(L))$. So

$$\#|L| = q^{h^0(L)} - 1.$$ 

By Riemann-Roch,

$$h^0(L) = \deg L + 1 - g + h^1(L).$$

By Serre duality, $h^1(L) = h^0(K - L)$, so in particular $h^1(L)$ vanishes if $\deg L > 2g - 2$.

Define $\text{Pic}^r(X) = \{ L \in \text{Pic}(X) \mid \deg L = r \}$. It is easy to see that there is a bijection $\text{Pic}^0(X) \leftrightarrow \text{Pic}^1(X)$ if $\text{Pic}^r(X) \neq \emptyset$ (so the $\text{Pic}^r(X)$ are $\text{Pic}^0(X)$-torsors). It is also a nontrivial fact that $\text{Pic}^r(X)$ is nonempty for all $r$.

Let $J$ be the Jacobian of $X$. An important property of $J$ is that there is a natural bijection

$$J(\mathbb{F}_q) \leftrightarrow \text{Pic}^0(X).$$

(Really, this should be by definition, i.e. the Jacobian should be defined as the scheme that represents the Picard functor). This implies that $\# \text{Pic}^r(X) = \#J(\mathbb{F}_q)$. 

58
8.3. THE WEIL CONJECTURES FOR CURVES

Theorem 8.3.1. The rationality statement in the Weil conjectures holds if \( \dim X = 1 \).

Proof. Recall that we proved an “Euler product” factorization

\[
Z_X(t) = \prod_{x \text{ closed } \in X} \frac{1}{1 - t^{\deg x}}.
\]

Expanding this out as a formal power series, this is

\[
Z_X(t) = \prod_{x \text{ closed } \in X} \sum_{m \geq 0} t^{m \deg x} = \sum_{D \geq 0} \sum_{\deg D = d} t^d = \sum_{D \geq 0 \deg D \leq 2g - 2} t^d + \sum_{D \geq 0 \deg D \geq 2g - 1} t^d.
\]

Now we group divisors into linear systems. Let \( \alpha = \#J(\mathbb{F}_q) = \# \text{Pic}^0(X) \). The first sum is a polynomial because there are only finitely many non-empty linear systems of bounded degree, and the second sum is nice because Riemann-Roch tells us exactly what \( h^0(D) \) is, namely \( d + 1 - g \), which in turn tells us \( \#|D| \). So we can rewrite

\[
Z_X(t) = \sum_{r=0}^{2g-2} \left( \sum_{L \in \text{Pic}^r(X)} \frac{q^{h_0(L)} - 1}{q - 1} \right) t^r + \sum_{r \geq 2g-1} \left( \sum_{L \in \text{Pic}^r(X)} \frac{q^{r+1-g} - 1}{q - 1} \right) t^r
\]

\[
= \text{polynomial in } t + \text{geometric series}
\]

\[
= \frac{P(t)}{(1-t)(1-qt)}.
\]

\( \square \)

Theorem 8.3.2. The functional equation holds for \( \dim X = 1 \). More precisely,

\[
Z_X \left( \frac{1}{qt} \right) = q^{1-g} t^{2-2g} Z_X(t).
\]

Proof. If \( g = 0 \), this follows from the formula we computed earlier for projective space. Henceforth, we assume that \( g \geq 1 \).

We can write \( Z_X(t) = S_1 + S_2 \), where

\[
S_1 = \sum_{r=0}^{2g-2} \left( \sum_{L \in \text{Pic}^r(X)} \frac{q^{h_0(L)}}{q - 1} \right) t^r.
\]

59
(this is very similar to the polynomial term we obtained above, but without the $-1$ in the numerator) and

$$S_2 = \sum_{r=0}^{2g-2} \left( \sum_{L \in \text{Pic}^0(X)} \frac{q^r}{q - 1} \right) t^r + \sum_{r \geq 2g-1} \alpha \frac{q^{r+1-g-1} - 1}{q - 1} t^r$$

$$= -\frac{\alpha}{(q-1)(1-t)} + \frac{\alpha q^2 t^{2g-1}}{(q-1)(1-qt)}.$$

We will actually check the functional equation for $S_1$ and $S_2$ separately. For $S_2$, we just have to plug stuff in to our formula:

$$S_2 \left( \frac{1}{qt} \right) = \frac{\alpha qt}{(q-1)(1-qt)} - \frac{\alpha q^{1-g} t^{2g}}{(q-1)(1-t)} = q^{1-g} t^{2g} S_2(t).$$

For $S_1$, we use the fact that $L \mapsto K_X - L$ gives a bijection on the set

$$\Lambda = \{ L \in \text{Pic}(X) \mid 0 \leq \text{deg} L \leq 2g - 2 \}.$$

By Serre duality and Riemann-Roch, $h^0(L) + g - 1 - \text{deg} L = h^0(K - L)$. So

$$S_1 \left( \frac{1}{qt} \right) = \sum_{r=0}^{2g-2} \left( \sum_{L \in \text{Pic}^0(X)} \frac{q^{h_0(L)} (1 - \alpha^r t)}{q - 1} \right) \frac{1}{q^r t^r}$$

$$= \sum_{r=0}^{2g-2} \left( \sum_{L \in \text{Pic}^0(X)} \frac{q^{h_0(K - L)} (1 - \alpha^r t)}{q - 1} \right) \frac{1}{(qr)^{2g-2-r}}$$

$$= \sum_{r=0}^{2g-2} \left( \sum_{L \in \text{Pic}^0(X)} \frac{q^{h_0(L) - (r+1-g)} (1 - \alpha^r t)}{q - 1} \right) \frac{1}{(qr)^{2g-2-r}}$$

$$= q^{1-g} t^{2g} \left( \sum_{L \in \text{Pic}^0(X)} \frac{q^{h_0(L)} (1 - \alpha^r t)}{q - 1} \right) t^r$$

$$= q^{1-g} t^{2g} S_1(t).$$

\[ \square \]

**Remark 8.3.3.** Recall that $Z_X(t) = \frac{P(t)}{(1-t)(1-qt)}$. By definition of $Z_X(t)$, $Z_X(0) = 1$. We can write

$$P(t) = \prod_{j=1}^{2g} (1 - \alpha_j t)$$

60
where the $\alpha_j$ might a priori be 0, since it follows from the proof that 
\[ \text{deg } P \leq 2g. \]
By the functional equation, 
\[ Z_X \left( \frac{1}{qt} \right) = q^{1-g} t^{2g} Z_X(t) \]
so 
\[ \prod_{j=1}^{2g} (qt - \alpha_j) = q^g \prod_{j=1}^{2g} (1 - \alpha - jt) \]
and since $Z_X(0) = 1 \implies P(0) = 1$, none of the $\alpha_j$ are zero. Therefore, we in fact have $\text{deg } P = 2g$.

8.4 Zeta functions of arithmetic schemes

Definition 8.4.1. An arithmetic scheme is a scheme of finite type over $\mathbb{Z}$.

Lemma 8.4.2. Suppose $X$ is an arithmetic scheme. Then $x \in X$ is a closed point if and only if $\kappa(x)$ is finite.

Proof. Pick $x \in X$, and suppose that $\kappa(x)$ is finite. Let $y$ be the image of $x$ in $\text{Spec } \mathbb{Z}$ so the residue field of $y$ is finite. Then $y = (p)$ for some prime $p$. So $x$ lies in the fiber of $X$ over $(p)$

Now, $X_p$ is a scheme of finite type over $\mathbb{F}_p$. Then $x$ is a closed point in $X_p$, since otherwise $\kappa(x)$ would be the function field of a positive-dimensional variety. Since $X_p \to X$ is a closed embedding, $x$ is closed in $X$.

Conversely, suppose that $x$ is a closed point. With the same notation as before, if $y$ is closed then the result is obvious. If $y$ is not closed, then it is the generic point $(0)$ of $\text{Spec } \mathbb{Z}$. Shrinking, we can assume that $X = \text{Spec } B$ and there exist some $\text{Spec } A \subset \text{Spec } \mathbb{Z}$ such that $B$ is finitely generated as an $A$-algebra. Algebraically, we have a diagram

Now $\kappa(x)$ is finitely generated over $B$ (since it is closed), hence over $A$. But it is also a field extension of $\mathbb{Q}$, which makes this impossible. $\square$
Definition 8.4.3. Let $X$ be an arithmetic scheme. For any closed $x \in X$, let $N(x) = \# \kappa(x)$. Define the zeta function

$$
\zeta_X(s) = \prod_{x \text{ closed} \in X} \frac{1}{1 - N(x)^{-s}}.
$$

Remark 8.4.4. One could think of this as a product over all points with the convention that $\infty^{-s} = 0$.

Since $X$ is of finite type over $\mathbb{Z}$, for any $n \in \mathbb{N}$ the set

$$
\#\{x \in X \mid N(x) \leq n\}
$$

is finite. This implies that we can expand $\zeta_X(s)$ as a Dirichlet series $\sum_{n \geq 1} a_n n^{-s}$ that converges for $\text{Re} s \gg 0$.

Example 8.4.5. Let $X = \text{Spec} \mathbb{Z}$. Then $\zeta_X(s)$ is the Riemann zeta function

$$
\zeta(s) = \prod_p (1 - p^{-s})^{-1} = \sum_n n^{-s}.
$$

More generally, if $K$ is a number field and $X = \text{Spec} \mathcal{O}_K$, then $\zeta_X(s)$ is the Dedekind zeta function.

Remark 8.4.6. If $X$ is an arithmetic scheme, then $\zeta_X(s) = \zeta_{X,\text{red}}(x)$ (the closed points are the same). If the set of closed points can be written as a union closed points in subschemes $X_i$, where the $X_i$ are closed or open, then

$$
\zeta_X(s) = \prod_i \zeta_{X_i}(s).
$$

Example 8.4.7. Let $X$ be an arithmetic scheme such that $X \to \text{Spec} \mathbb{Z}$ maps $X$ to one point $(p) \in \text{Spec} \mathbb{Z}$. Then $X$ is a scheme over $\mathbb{F}_p$. For simplicity, assume that $X$ is a variety over $\mathbb{F}_p$. Then

$$
\zeta_X(s) = \prod_{x \text{ closed} \in X} \frac{1}{1 - N(x)^{-s}}.
$$

Now, $N(x) = p^{\deg x}$. So this coincides with $Z_X(p^{-s})$, where $Z_X$ is the Hasse-Weil zeta function.

Example 8.4.8. Suppose $X = \mathbb{A}^n_{\mathbb{Z}}$. Then

$$
\zeta_X(s) = \prod_p \zeta_{X_p}(s) = \prod_p Z_{X_p}(p^{-s}).
$$

and we already computed the Hasse-Weil zeta function for $X_p = \mathbb{A}_{\mathbb{F}_p}$. The conclusion is that

$$
Z_X(s) = \prod_p \frac{1}{1 - p^{s-n}}.
$$
This is just a translated version of the Riemann $\zeta$ function.

By using our earlier comment, we can compute the zeta function for projective space by using the decomposition $\mathbb{P}^n_{\mathbb{Z}} = \mathbb{A}^n_{\mathbb{Z}} \cup \mathbb{P}^n_{\mathbb{Z}}$.

**Theorem 8.4.9.** Let $X$ be an arithmetic scheme. Varying $s \in \mathbb{C}$, $\zeta_X(s)$ is absolutely convergent (as a product) if $\text{Re} \; s > \dim x$.

**Proof.** If $X = X_1 \cup X_2$, then it suffices to show that the result holds for two out of three of $(X_1, X_2, X)$. Then one can reduce to the case $X = \text{Spec} \; B$, where $B$ is a finitely $A$ algebra and $\text{Spec} \; A \subset \text{Spec} \; \mathbb{Z}$ is an open subset. Using Noether normalization, $B$ is a finite extension of $A[x_1, \ldots, x_n]$, which reduces to the case of affine space.

It is a theorem that $\zeta_X(s)$ can be meromorphically continued to $\text{Re} \; s > n - \frac{1}{2}$.

**Fact.** Assume $X$ is integral and let $K$ be the function field of $X$, i.e. $K = \kappa(\eta)$, where $\eta$ is the generic point of $X$. If $K$ has characteristic 0 (i.e. $X \to \text{Spec} \; \mathbb{Z}$ is dominant) then $\zeta_X(s)$ has a simple pole at $s = n$. If $K$ has characteristic $p \neq 0$, then $\zeta_X(s)$ has simple poles at the complex numbers $n + 2\pi i \frac{m}{\log q}$ where $m \in \mathbb{Z}$ and $q$ is the largest power of $p$ such that $\mathbb{F}_q \subset K$ (i.e. the algebraic closure of $\mathbb{F}_p$ in $K$, or the “field of constants” of $K$).

**Conjecture.** $\zeta_X(s)$ has a meromorphic continuation to the entire complex plane. (Possibly with some regularity assumptions on $X$.)

This is known in certain cases, e.g. $\dim X = 1$, $\mathbb{A}^n$, $\mathbb{P}^n$, or positive characteristic (this last case following from the Weil conjectures).

**Conjecture.** Assuming $X$ is regular, the zeta function $\zeta_X(s)$ in the region $0 < \text{Re} \; s \leq n$ has zeros only on the line $\text{Re} \; s = \frac{1}{2}, \frac{3}{2}, \ldots$ and poles only on the vertical lines $1, 2, \ldots, n$.

Again, in positive characteristic this is implied by the Weil conjectures.