The goal of this seminar is to study some classical results from diophantine geometry. We will follow "Heights in Diophantine Geometry" as the main reference. The rough structure of the seminar (which will definitely take more than one term) consists two parts, first one being the tools we need:

1. we do naive heights in projective space, then Weil height for projective varieties
2. we study some results we need about abelian varieties
3. then we move to Neron-Tate heights, which can be thought as the "best model" of Weil's height we introduced above

once we have those tools, we move to the proof of Mordel-Weil, and Falting. I expect, if we go fast enough, that we can finish Mordel-Weil by the end of this term. After we get the two theorems, to motivative Vojta's conjecture, we need to go into a little bit about abc-conjecture, as well as Nevanlinna theory.

So, in this talk, we will study heights in projective space.

1 A Bit Number Theory

Moral: Height of a number=algebraic complication (I dont want to use the word algebraic complexity as its already been taken by CS people).

Throughtout the seminar, it is safe to assume all the fields we encounter are number fields, unless we specifically mention otherwise.

Definition 1.1

Let K be a field. A ***place*** v is an equivalence class of non-trivial absolute value on K, where $v \sim v'$ iff they induce the same topology on K.

For a place v, we define K_v its completion under the topology induced by v. Now let L/K be field extension, w a place on L and v a place on K, then we write $w \mid v$ to mean $w|_K = v$. Then, the completion K_v of K satisfies three basic properties:

1. K_v/K is a field extension
2. there is unique w on K_v so $w \mid v$
3. K_v is complete with respect to w
4. K is dense open in K_v

Example 1.2

Let $K = \mathbb{Q}$, then we have two kind of absolute values.

1. archimedean one, which is just the usual absolute value
2. non-archimedean ones, defined for each prime p, so that $|q|_p = 1$ if $q \neq p$ and $1/p$ if $p = q$ for all primes, then extend naturally

Here non-archimedean means $|x + y| \leq \max(|x|, |y|)$ for all $x, y \in K$.

It is well-known the only complete archimedean fields are $\mathbb{R}$ and $\mathbb{C}$, while for non-archimedean places, p-adic numbers $\mathbb{Q}_p$ are the complete fields.

Recall for L/K, we define $N_{L/K}(x) = \det(m_x)$ where $m_x : L \to L$ is the K-linear map defined by multplication by x. Then we have the following result:

Proposition 1.3

Let L/K be finite extension and v an absolute value on K that is complete. Then there is unique extension w on L of v, such that

$$|x|_w = |N_{L/K}(x)|_v^{1/[L:K]}$$

In particular L is complete with respect to $|\cdot|_w$.

Now, given non-archimedean place v on K, we can define its valuation ring

$$R_v = \{x \in K : |x|_v \leq 1\}$$

and the unique maximal ideal $\mathfrak{m}_v = \{x \in K : |x|_v = 1\}$. Its residue field is denoted by $\kappa(v)$.

Definition 1.4

Let L/K be finite extension, v non-archimedean place on K and w on L extends v. Then we define:

1. the ***residue degree*** $f_{w/v}$ as the dimension of $\kappa(w)$ as $\kappa(v)$-vector space
2. the ***ramification index*** $e_{w/v}$ as the index of the subgroup $|K^\times|_v$ in $|L^\times|_w$

One of the main basic result about this is that

$$[L:K] = \sum_{w|v} f_{w/v} e_{w/v}$$

provided L/K are number field extensions. Geometrically, the ramification index keep track of how the prime ideal assocaited with v ramifies in L, i.e. say $w_1, \dots, w_r$ are all the prime ideals lying over the prime ideal $\mathfrak{p}$ of v, then $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_r^{e_r}$ where $e_i := e_{w_i/v}$.

In particular, the above can also be phrased as the following result:

Lemma 1.5

If L is a finite separable extension of K, then

$$\sum_{w|v} [L_w : K_v] = [L:K]$$

The number $[L_w : K_v]$ is called the local degree of L/K in w.

For place w on L that extends v on K, we will, by assumption, take the representative that is normalized with respect to v, which are defined as follows:

$$\|x\|_w := |N_{L_w/K_v}(x)|_v$$

$$|x|_w = \|x\|_w^{1/[L:K]}$$

Lemma 1.6

For $0 \neq x \in K, 0 \neq y \in L$, we have

$$\sum_{w|v} \log |x|_w = \log |x|_v$$

$$\sum_{w|v} \log \|y\|_w = \log |N_{L/K}(y)|_v$$

2 Product Formula

Let K be a field, M_K a set of non-trivial places so $\{|\cdot|_v \in M_K : |x|_v \neq 1\}$ is finite for all $0 \neq x \in K$. Then we say M_K satisfies product formula if

$$\prod_{v \in M_K} \|x|_v = 1$$

for all $0 \neq x \in K$.

Lemma 2.1

Suppose M_K satisfies product formula and $M_L := \{\|\cdot\|_w^{1/[L:K]} : v \in M_K, w \mid v\}$. Then M_L satisfies product formula.

Now suppose K is a number field, then when we write M_K, we always mean the set of places extending $M_{\mathbb{Q}} := \{|\cdot|_p : p \text{ prime or } \infty\}$ as defined above.

Lemma 2.2

Let K be a number field, then M_K satisfies product formula.

The proof follows from the fact every integer admits prime factorization.

Now we describe more explicitly what M_K is for a degree n number field K.

First assume $v \in M_K$ extends $\infty \in M_{\mathbb{Q}}$. In this case, K_v must be either $\mathbb{R}$ or $\mathbb{C}$. By number theory we know we only have n many embeddings $K \hookrightarrow \mathbb{C}$. If $K_v = \mathbb{R}$, then this means it corresponds to a real embedding $\sigma : K \to \mathbb{C}$, i.e. $\mathrm{im}(\sigma) \subseteq \mathbb{R}$. On the other hand, if $K_v = \mathbb{C}$, then we see it gives a complex embedding. In this case, we see σ and $\overline{\sigma}$ gives the same absolute value. Thus, we see $v \in M_K$ extending ∞ consists of r_1 many real embeddings, and r_2 many pairs of conjugate complex embeddings.

On the other hand, $v \in M_K$ that extends p are precisely given by the prime factorization of $p\mathcal{O}_K$, i.e. it consists of all the primes in $\mathcal{O}_K$ lying above p.

3 Heights in Projective Space

Choose $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and we denote $\mathbb{P}^n := \mathbb{P}^n_{\overline{\mathbb{Q}}}$.

Now let $P \in \mathbb{P}^n$ be represented by homogeneous coordinate $(P_0 : \ldots : P_n)$, and assume $P_i \in K$ for a number field K, then we define

$$h(P) = \sum_{v \in M_K} \max_j \log |P_j|_v$$

Lemma 3.1

$h(P)$ is independent of the choice of K.

Proof. Let L be another field containing P_i, then WLOG assume $K \subseteq L$. In this case, we know

$$\sum_{w \in M_L} \max_j \log |P_j|_w = \sum_{v \in M_K} \sum_{w|v} \max_j \log |P_j|_w$$

But by a lemma, we know $\sum_{w|v} \log |x|_w = \log |x|_v$, and hence we are done.

Lemma 3.2

$h(P)$ is independent of the choice of coordinates.

Proof. Suppose Q is another representative, i.e. there is K so $Q, P \in \mathbb{P}^n_K$, and $0 \neq \lambda \in K$ so $Q = \lambda P$. But then

$$h(Q) = \sum_{v \in M_K} \log |\lambda|_v + \sum_{v \in M_K} \max_j \log |P_j|_v$$

where $\sum_{v \in M_k} \log |\lambda|_v = 0$ by product formula.

Definition 3.3

We call $h(P)$ the ***absolute log height*** (briefly, ***height***) of P. We also define the ***multiplicative height*** $H(P)$ by $e^{h(P)}$.

Throughout we will identify $\mathbb{A}^n$ as a subset of $\mathbb{P}^n$ via $(x_1, \ldots, x_n) \mapsto (1 : x_1 : \ldots : x_n)$.

Example 3.4

Let α be an algebraic integer in a number field K of degree n. Then it can be identified as the point $(1 : \alpha) \in \mathbb{P}^1$. Thus

$$h(\alpha) = \sum_{v \in M_K} \log(\max(|\alpha|_v, 1))$$

However, $\alpha\mathcal{O}_K$ factors into prime ideals of $\mathcal{O}_K$ with all exponent non-negative. Hence for all $v \mid p$ we must have $|\alpha|_v \leq 1$. This shows

$$h(\alpha) = \sum_{v \mid \infty} \log(\max(|\alpha|_v, 1))$$

Now take $\alpha = i$, then we see there are two embeddings $\mathbb{C} \hookrightarrow \mathbb{C}$, and thus

$$h(i) = \log(\max(|i|_\infty, 1)) + \log(\max(|-i|_\infty, 1)) = 0$$

On the other hand, take $\alpha = 1 + \sqrt{2}$, then we see

$$h(\sqrt{2} + 1) = \frac{1}{2} \log(1 + \sqrt{2})$$

because we have two embeddings $a + b\sqrt{2} \mapsto a + b\sqrt{2}$ and $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

If we still have time, let us conclude with the following result:

Theorem 3.5: Kronecker

The height $\xi \in \overline{\mathbb{Q}}^\times$ is zero if and only if ξ is a root of unity.

Proof. First, if ξ is a root of unity, then its absolute values are all equal to 1, and hence its height is 0. Thus it suffices to show the converse.

Suppose $h(\xi) = 0$, then we must have $|\xi|_v \leq 1$ for all $v \in M_K$. This implies ξ must be algebraic integer because $|\xi|_v \leq 1$ for all finite places indicates $\xi\mathcal{O}_K$ factors as positive product of primes in $\mathcal{O}_K$, i.e. $\xi \in \mathcal{O}_K$.

Now let d be the degree of ξ, and denote $\mathbf{x} := (\xi_1, \ldots, \xi_d)$ be a vector consists of all the conjugates of ξ. We write $\mathbf{x}^m$ to denote $(\xi_1^m, \ldots, \xi_d^m)$.

Now let s_i be the ith elementary symmetric polynomial with d variables. This gives

$$(x - \xi_1^m) \ldots (x - \xi_d^m) = \sum_{i=0}^{d} (-1)^i s_i(\mathbf{x}^m) x^d$$

and in particular since $\xi \in \mathcal{O}_K$ we see $s_i(\mathbf{x}^m) \in \mathbb{Z}$.

Now, $|\xi_j|_v \leq 1$ for all j and v, and s_i consists of $\binom{d}{i}$ monomials, we see

$$\sum_{i=0}^{d} |s_i(\mathbf{x}^m)| \leq \sum_{i=0}^{d} \binom{d}{i} = 2^d$$

The above bound says that $\{(s_0(\mathbf{x}^m), ..., s_n(\mathbf{x}^m)) : m \geq 1\}$ must be a finite set, and hence by pigeonhole principle, there exists $m \neq n$, so $s_i(\mathbf{x}^m) = s_i(\mathbf{x}^n)$ for $i = 0, ..., d$. By defining property of elementary symmetric functions, we see this happens if and only if $\mathbf{x}^m = \sigma(\mathbf{x}^n)$ for some permutation σ on d letters. WLOG assume $m > n$. Repeat this argument $\mathrm{ord}(\sigma)$ many times, we may assume $\sigma = \mathrm{Id}$, and this gives $\xi^{m^{\mathrm{ord}(\sigma)}} = \xi^{n^{\mathrm{ord}(\sigma)}}$, showing ξ is a root of unity.