

Notes on Diophantine Geometry

February 28, 2008

Lecture by Felipe Voloch

Notes by Nick Rauh

Heights

Recall: To complete our proof of the Mordell-Weil Theorem, we need a function

$$h : A(K) \rightarrow [0, \infty)$$

such that

- (i) For all $c > 0$, $\{P \in A(K) : h(P) \leq c\}$ is finite,
- (ii) $h(mP) = m^2h(P) + O(1)$,
- (iii) $\forall P_0 \in A(K), \exists c(P_0) > 0, h(P + P_0) \leq 2h(P) + c(P_0)$.

By definition, an abelian variety is in projective space, so it is natural to start with heights defined on projective space $\mathbb{P}^n(K)$. For the remainder of these notes, let K denote a global field (i.e. a finite extension of \mathbb{Q} or $\mathbb{F}_q(x)$) and let M_K be the set of places of K . Then for each $v \in M_K$ we choose an absolute value $|\cdot|_v$ and number n_v such that the product formula holds for all $x \in K^*$. This means that for all $x \in K^*$,

$$\prod_v |x|_v^{n_v} = 1.$$

If $a \in \mathbb{P}^n(K)$, write $a = (a_0 : \cdots : a_n)$. Then we define

$$h(a) = \sum_v n_v \log \max_{0 \leq i \leq n} \{|a_i|_v\}.$$

Remark: Sometimes the function

$$H(a) = \prod_v \max_{0 \leq i \leq n} \{|a_i|_v\}^{n_v}$$

is used. These heights are related by $h(a) = \log H(a)$.

Lemma: If $a \sim b$, then $h(a) = h(b)$.

Proof: By definition, $a \sim b$ if there exists some $\lambda \in K^*$ such that $a_i = \lambda b_i$ for each i . We then observe that

$$\begin{aligned} \max_{0 \leq i \leq n} \{|a_i|_v\} &= \max_{0 \leq i \leq n} \{|\lambda|_v |b_i|_v\} \\ &= |\lambda|_v \max_{0 \leq i \leq n} \{|b_i|_v\}. \end{aligned}$$

Summing each side over all $v \in M_K$, we have

$$h(a) = h(b) + \sum_v n_v \log |\lambda|_v.$$

However, the sum on the right vanishes by the product formula:

$$\begin{aligned} \sum_v n_v \log |\lambda|_v &= \log \left(\prod_v |\lambda|_v^{n_v} \right) \\ &= \log 1 = 0. \end{aligned}$$

■

Example: $K = \mathbb{Q}$.

Every point $a \in \mathbb{P}^n(\mathbb{Q})$ can be represented by $a = (a_0 : \cdots : a_n)$ with $a_i \in \mathbb{Z}$, $\gcd(a_0, \dots, a_n) = 1$. If p is prime, then we have that, for this representation,

$$\max_{0 \leq i \leq n} \{|a_i|_p\} = 1.$$

To see this, note that there must be some a_i not divisible by p . For this a_i , $|a_i|_p = 1$. For the rest, we note that each other a_j is of the form $a_j = p^s m$ with $p \nmid m$ and $s \geq 0$, so $|a_j|_p = p^{-s} \leq 1$. Hence we see that

$$h(a) = \log \max_{0 \leq i \leq n} \{|a_i|_\infty\}.$$

Theorem: If K is a global field, given integers $n, c \geq 1$, the set

$$\{a \in \mathbb{P}^n(K) : h(a) \leq c\}$$

is finite.

Before we give the proof of this theorem, the following two propositions are left as exercises:

Proposition 1: Define $h(\alpha) = h(1 : \alpha)$ for $\alpha \in K$. Then, for $\alpha_1, \dots, \alpha_n \in K$ we have

$$\max_{0 \leq i \leq n} \{h(\alpha_i)\} \leq h((1 : \alpha_1 : \dots : \alpha_n)) \leq h(\alpha_1) + \dots + h(\alpha_n).$$

Proposition 2: For $p/q \in \mathbb{Q}$, $\gcd(p, q) = 1$

$$h(p/q) = \max\{\log |p|_\infty, \log |q|_\infty\}.$$

We also adopt the following notation:

Notation: $\log^+ x := \log \max\{1, x\}$.

Proof of Theorem: We handle the case where K is a finite extension of \mathbb{Q} (the case for function fields is similar). Using the first proposition, we may reduce the problem to demonstrating that each set

$$\{\alpha \in K : h(\alpha) \leq c\}$$

is finite. If $\alpha \in K$, let $m_\alpha(x) \in \mathbb{Z}[x]$ be its minimal polynomial. It is then enough to show a bound for the coefficients of $m_\alpha(x)$ if $h(\alpha) \leq c$. Since each finite extension of \mathbb{Q} is contained in some Galois extension, we may assume that K/\mathbb{Q} is Galois. Then $m_\alpha(x)$ divides the polynomial

$$\prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} (x - \sigma(\alpha)).$$

It is then enough to bound the heights of the coefficients of this polynomial, i.e. the symmetric functions in $\{\sigma(\alpha) : \sigma \in \text{Gal}(K/\mathbb{Q})\}$. Defining

$$\beta = \sum_{i_1 \leq \dots \leq i_k} \sigma_{i_1}(\alpha) \cdots \sigma_{i_k}(\alpha),$$

we note that

$$h(\beta) = \sum_{p \leq \infty} \log^+ |\beta|_p.$$

We then estimate each $|\beta|_p$. If $v|p$, then

$$\begin{aligned} |\beta|_p &= |\beta|_v \\ &= \left| \sum_{i_1 \leq \dots \leq i_k} \sigma_{i_1}(\alpha) \cdots \sigma_{i_k}(\alpha) \right|_v \\ &\leq \sum_{i_1 \leq \dots \leq i_k} |\sigma_{i_1}(\alpha) \cdots \sigma_{i_k}(\alpha)|_v \\ &= \sum_{i_1 \leq \dots \leq i_k} |\sigma_{i_1}(\alpha)|_v \cdots |\sigma_{i_k}(\alpha)|_v. \end{aligned}$$

Since the function $|\sigma_{i_j}(\cdot)|_v$ is yet another absolute value restricting to $|\cdot|_p$ on \mathbb{Q} , label it $|\cdot|_{v_{i_j}}$. Continuing our estimates,

$$\begin{aligned} \sum_{i_1 \leq \dots \leq i_k} |\sigma_{i_1}(\alpha)|_v \cdots |\sigma_{i_k}(\alpha)|_v &= \sum_{i_1 \leq \dots \leq i_k} |\alpha|_{v_{i_1}} \cdots |\alpha|_{v_{i_k}} \\ &\leq \binom{n}{k} \max\{1, |\alpha|_{v_1}, \dots, |\alpha|_{v_n}\}^k. \end{aligned}$$

By the strong triangle inequality, we don't need the combinatorial coefficient in the non-archimedean case. Combining the estimates at each place,

$$\begin{aligned} h(\beta) &= \sum_{p \leq \infty} \log^+ |\beta|_p \\ &\leq \binom{n}{k} + k \sum_{p \leq \infty} \log \max_{v_i, \dots, v_n | p} \{1, |\alpha|_{v_1}, \dots, |\alpha|_{v_n}\} \\ &\leq \binom{n}{k} + kh(\alpha). \end{aligned}$$



There is a stronger version of the theorem due to Northcott:

Theorem: For fixed integers $d, n \geq 1$, the set

$$\{a \in \mathbb{P}^n(\overline{\mathbb{Q}}) : [\mathbb{Q}(a) : \mathbb{Q}] \leq d, h(a) \leq c\}$$

is finite.

In defining the height h on $\mathbb{P}^n(\overline{\mathbb{Q}})$, it is necessary to make the right choice of $|\cdot|_v, n_v$ such that if $a \in \mathbb{P}^n(K)$ and L/K , then $h(a)$ is the same value regardless whether it is computed in K or L .

Theorem: Suppose K is a global field, $\phi_0, \dots, \phi_r \in K[x_0, \dots, x_n]$ are homogeneous all of degree d . Then, on the set of $a \in \mathbb{P}^n(K)$ such that some $\phi_i(a) \neq 0$, define the function Φ by

$$\Phi : (a_0 : \dots : a_n) \mapsto (\phi_0(a) : \dots : \phi_r(a)) \in \mathbb{P}^r(K).$$

Then $h(\Phi(a)) \leq h(a) + O(1)$.

Proof: By definition,

$$h(\Phi(a)) = \sum_v n_v \log \max_{0 \leq i \leq r} |\phi_i(a)|_v.$$

If we write $\phi_i(a)$ as

$$\phi_i(a) = \sum_{d_1 + \dots + d_n = d} c_{d_0, \dots, d_n}^i a_0^{d_0} \dots a_n^{d_n},$$

then we have

$$\begin{aligned} \log |\phi_i(a)|_v &\leq \log \left(\sum_{d_1+\dots+d_n=d} |c_{d_0,\dots,d_n}^i|_v |a_0|_v^{d_0} \cdots |a_n|_v^{d_n} \right) \\ &\leq \log k_v + d \log \left(\max_{0 \leq i \leq n} \{|a_i|_v\} \right) + \log \binom{n+d}{d} \end{aligned}$$

Here $k_v = \max |c_{d_0,\dots,d_n}^i|_v$. It is clear that, for all but finitely many v , $\log k_v = 0$. As before, the combinatorial term is not necessary in the non-archimedean case. The result follows by summing over v . ■

Remark: If $(\phi_0, \dots, \phi_r) = (x_0, \dots, x_n)^k$, then $h(\Phi(a)) = dh(a) + O(1)$.