Heights, Integral Models and Arakelov Theory IMJ-PRG

B. Wagener

November 26th, 2015

The basics

Polynomial equations were for long studied in two different ways, either by the algebra of the underlying numbers or by the geometric form that they define.
There were many developments between XIX^{th} century and the XX^{th} century that made many mathematicians dream about a unification of Algebra and Geometry into a unified field:

- The discovery of algebraic numbers and the corresponding development of Algebraic Number Theory
- The developments of Geometry
- The revolution in Algebraic Geometry

The new conceptions in Algebraic Geometry that somehow unified algebraic and geometric questions made now possible to ask for the very old Diophantine questions in geometric terms: it was the birth of Diophantine Geometry

Example of Diophantine Equation

A Diophantine equation is essentially a polynomial equation with integer coefficients,

$$P(X_0, X_1, \ldots, X_n) = 0,$$

for which we ask for solutions in integers.
Perhaps one of the most famous Diophantine equation is Fermat's equation which ask for integer solutions to

$$x^n + y^n = z^n.$$

As the field of Algebra and Geometry were unified it had become something of special interest to study such problems geometrically, this is the field of Diophantine Geometry.

Polynomial equations are the oldest mathematical equations but what makes them so exceptional is that somehow they are universal:

- Polynomial equations are the most general equations one can form with the two elementary laws of addition and multiplication.

It was already a revolution during Antiquity to discover that $\sqrt{2}$ (i.e. the root of $X^2 - 2 = 0$) is not a rational number.
Then with the discovery of imaginary numbers it was realized that it is possible to define a whole new class of numbers that with their underlying structure behave mainly has the field $\mathbb{Q}$ with underlying integral structure $\mathbb{Z}$.
A number field looks mainly as $\mathbb{Q}[\alpha]$ where α is the root of some polynomial with coefficient in $\mathbb{Q}$, with an underlying integral structure of the form $\mathbb{Z}[\beta]$.

Example

We know that imaginary numbers may be described abstractly as the quotient

$$\mathbb{C} = \mathbb{R}[X]/(X^2 + 1),$$

which can be seen simply as considering all polynomials with real coefficient while setting abstractly the algebraic relation $X^2 + 1 = 0$ in.
A basic example of number field is $\mathbb{Q}[i] = \mathbb{Q}[X]/(X^2 + 1)$ of which ring of integers is simply in this case $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2 + 1)$.

Algebraic Numbers field of the form $\mathbb{Q}[\alpha]$ have the first property that they form a field which is perhaps not obvious at first sight.
The integers of an algebraic number field are the element of the field that are roots of a monic (leading coefficient 1) polynomial with coefficient in $\mathbb{Z}$.
The integers form a Dedekind ring (unique factorization).
Therefore we have the equivalent of prime numbers which then become prime ideals.
For the remaining of this exposition we fix a number field K and we denote by $\mathcal{O}_K$ its ring of integers.

Absolute Values

Definition: *An absolute value on a field K is a real-valued function*

$$|\cdot| : K \to [0, +\infty[$$

such that:

1. $|x| = 0$ iff $x = 0$ (Nondegenretate)
2. $|x \cdot y| = |x||y|$ (Multiplicative)
3. $|x + y| \leq |x| + |y|$ (Triangle Inequality)

Moreover an absolute value is said to be finite or nonarchimedean or ultrametric if it satisfies

- $|x + y| \leq \max\{|x|, |y|\}$

Theorem (Ostrowski) *Any absolute value over $\mathbb{Q}$ is topologically equivalent either to the usual absolute value or to a p-adic absolute value, one for each prime p as defined below.*

This gives rise to completions of $\mathbb{Q}$, known as the usual real numbers $\mathbb{R}$ or the $p-$adic numbers, $\mathbb{Q}_p$.

Absolute Values II

On $\mathbb{Q}$ the absolute values are $|x|_\infty = \max\{x, -x\}$ and the nonarchimedean absolute values given, for each prime number p, by the following:
If one write $x = p^{\mathrm{ord}_p(x)} \cdot \frac{a}{b}$ where a and b are prime to p,

$$|x|_p = p^{-\mathrm{ord}_p(x)}.$$

This generalizes to any number field K, where now we have a nonarchimedean absolute value for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and we have a finite set of archimdean absolute values according to embeddings $K \hookrightarrow \mathbb{C}$.
As one can easily see from the case of $\mathbb{Q}$, if one denotes by M_K the set of absolute values over a number field K, once suitably normalized they satisfy the product rule:

$$\prod_{\mathfrak{p} \in M_K} |x|_\mathfrak{p} = 1.$$

Heights in Projective Space I

For $P \in \mathbb{P}^n(K)$ with in projective coordinates $P = (x_0 : x_1 : \cdots : x_n)$ we define the logarithmic normalized height of P as:

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \log \left(\prod_{\mathfrak{p} \in M_K} \max\{|x_0|_{\mathfrak{p}}, |x_1|_{\mathfrak{p}}, \ldots, |x_n|_{\mathfrak{p}}\} \right)$$

- The product rule guarantee that it is independent of the choice of coordinates.
- It is nonnegative
- As normalized it is not only defined for points in $\mathbb{P}^n(K)$ but for points in $\mathbb{P}^n(\bar{\mathbb{Q}})$
- And the most important for us is certainly that as such it represents harmoniously the arithmetic complexity of the point P once taken into account the balance between finite and infinite places.

Heights in Projective Space II

The heights has the following properties:

- **Theorem**(Northcott) The number of points of both bounded degree and bounded height is finite.
- **Theorem**(Kronecker) With the preceding notations, a $h(P) = 0$ if and only if for any $0 \leq i, j \leq n$, $\frac{x_i}{x_j}$ is either a root of unity or zero.
  We will see later that those important theorems generalizes very well to the geometric settings, the theorem of Northcott is even very often taken has a essential definition of what is called an height in Arithmetic Geometry.

Example

If one consider $(a : b) \in \mathbb{P}^1(\mathbb{Q})$ with a and b relatively prime, we have simply

$$h((a : b)) = \log \max\{|a|, |b|\}.$$

As an example for Kronecker theorem, a root of unity in K is an element $\zeta \in K$ such that $\zeta^n = 1$ for some integer n. The simplest example is certainly "1" itself.
And can easilly see that

$$h((1 : 1 : \ldots : 1 : 0 : 0 : \ldots : 0 : 1 : 1 : \ldots)) = log(1) = 0.$$

From Projective Space to Projective Varieties

There is a basic way to generalize this definition to a variety in $\mathbb{P}^n$. Essentially, if $\phi : V \to \mathbb{P}^n$ is a morphism it seems reasonable to define the height on V relative to ϕ as

$$h_\phi : V(\bar{\mathbb{Q}}) \to [0, +\infty[; \quad h_\phi(P) = h(\phi(P))$$

What is remarkable is that this definition suits almost perfectly the geometry of projective varieties as we will see.

Reminder of Algebraic Geometry I

A projective variety may essentially be seen has the set of common zeros of homogeneous polynomial with coefficient in K:

$$\begin{cases} P_1(X_0, X_1, \ldots, X_n) = 0 \\ P_2(X_0, X_1, \ldots, X_n) = 0 \\ \qquad\qquad \ldots \\ P_M(X_0, X_1, \ldots, X_n) = 0 \end{cases}$$

What is especially important in the study of such varieties is the group of divisors. Here we consider only smooth variety and for such a divisor is either a subvariety locally defined by only one equations or equivalently with respect to the zeros and poles of those equation by a finite sum

$$D = \sum n_W [W]$$

where W is a subvariety of codimension 1 and $n_W \in \mathbb{Z}$.

Reminder of Algebraic Geometry II

As we can easily see, those divisors form a group that we denote $\mathrm{Div}(V)$ and what is perhaps not so obvious is that the study of such divisors and of the corresponding group is an essential tool for understanding the geometric structure of such varieties.
Locally defined by only one equation means that they are defined by a cocycle in the same way that line bundles are.
Therefore, in the smooth case, there is an equivalence between considering a divisor or a line bundles.
To a divisor D is associated a line bundle that we denote $\mathcal{O}(D)$.

Example

A basic example of a divisor is an hyperplane in $\mathbb{P}^n$, it is simply defined by an equation of the form:

$$a_0X_0 + a_1X_1 + \cdots + a_nX_nn = 0,$$

and as it relates the $(n+1)$ projective coordinates together one can easily see that it defines an object of dimension $(n-1)$. Locally defined by one equations means that on each open subset of some covering of $\mathbb{P}^n$ by open set, let say for example U_i it is defined by an equation of the form f_i and in such a way that those objects glue together on the covering to form a well defined object. There is an equivalence relation on divisors that says that two divisors are equivalent when they differ by one global equation.

Weil's Height Machine I

Let K be a number field, for any smooth projective variety V/K there exists a map:

$$h_V : \mathrm{Div}(V) \to \{\text{function } V(\bar{K}) \to \mathbb{R}\}$$

with the following properties:

(1) (Normalization)Let $H \subset \mathbb{P}^n$ be a hyperplane, and let $h(P)$ be the normalized logarithmic height, then

$$h_{\mathbb{P}^n,H}(P) = h(P) + O(1),$$

(2) (Functoriality) Let $\phi : V \to W$ be a morphism and let $D \in \mathrm{Div}(W)$ then,

$$h_{V,\phi^* D}(P) = h_{W,D}(\phi(D)) + O(1),$$

(3) (Additivity) Let $D, E \in \mathrm{Div}(V)$, then:

$$h_{V,D+E}(P) = h_{V,D}(P) + h_{V,E}(P) + O(1),$$

Weil's Height Machine II

(4) (Linear equivalence)Let $D, V \in \mathrm{Div}(V)$ be linearly equivalent, then

$$h_{V,D}(P) = h_{V,E}(P) + O(1),$$

(5) (Positivity) $h_{V,D}$ is bounded from below,

(6) (Finitness, Northcott) If D is ample, then for any finite extension K'/K,

$$\{P \in V(K') | h_{V,D}(P) \leq Cte\}$$

is finite.

The bounded quantities $O(1)$ are dependent on the data but are independent of the points.

The Case of Abelian Varieties I

An abelian variety is a projective variety whose rational points form a group group. A very special property is that being both projective and a group variety it forces it to be an abelian group.

- Let A/K be an abelian variety and let $D \in \mathrm{Div}(A)$ then for any integer m and for any point $P \in A(\bar{K})$:

$$h_{A,D}([m]P) = \frac{m^2+m}{2} h_{A,D}(P) + \frac{m^2-m}{2} h_{A,D}(-P) + O(1).$$

In particular if $[-1]^* D \cong D$,

$$h_{A,D}([m]P) = m^2 h_{A,D}(P) + O(1),$$

and if $[-1]^* D \cong -D$,

$$h_{A,D}([m]P) = m h_{A,D}(P) + O(1)$$

The Case of Abelian Varieties II

When the divisor is symmetric, $h_{A,D}$ is almost a quadratic form and indeed we are going to make it a quadratic form:

$$h_{A,D}(P+Q)+h_{A,D}(P-Q)=2h_{A,D}(P)+2h_{A,D}(Q)+O(1)$$

Therefore we can set (D symmetric)

$$\hat{h}_{A,D}(P)=\lim_{m\to+\infty}\frac{h_{A,D}([m]P)}{m^2},$$

and defined this way it kills the constant $O(1)$ and therefore defines properly a quadratic form $\hat{h}_{A,D}$ on the rational points of $A(\bar{K})$. As such, $\hat{h}_{A,D}([m]P)=m^2\hat{h}_{A,D}(P)$ and $\hat{h}_{A,D}(P+Q)+\hat{h}_{A,D}(P-Q)=2\hat{h}_{A,D}(P)+2\hat{h}_{A,D}(Q)$ which is absolutely remarkable, it defines an arithmetic norm on rational points.

What to do with Heights?

- Prove theorems!! (Mordell-Weil, Siegel, Faltings)
- Do Euclidean Geometry on $A(\bar{K}) \otimes \mathbb{R}$ (Vojta, Bombieri...). With the remarkable property that points with $\hat{h}(P) = 0$ are precisely the torsion points.
- Study arithmetic dynamic by iteration of maps.
- Count point of bounded heights and degree (concrete arithmetic information)

Local Heights

What is especially remarkable with absolute values is that for each place $\mathfrak{p} \in M_K$ we have a corresponding complete local field $K_{\mathfrak{p}}$. There is quite a close connection between the study of rational points in $V(K)$ and the points in the (simpler) local field $V(K_{\mathfrak{p}})$ given for every v.(Local-Global Principle)
Especially we have the

- (Local Height Machine) This says that each height on a projective varieties split, up to a constant, as a sum of local height each defined on the corresponding local field and such that the local heights satisfies the needed properties (Normalization, Additivity, Functoriality, Positivity)
- The Theorem of Néron which says that the canonical heights on abelian varities split, up to a constant, as a sum of canonical local heights with suitable properties

Integral Models

As $\mathcal{O}_K$ is a Dedekind domain of fraction field K one can get from any variety defined over K a variety defined over $\mathcal{O}_K$ by killing denominators. We assume it to be smooth.

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & \mathcal{V} \\ \uparrow & & \uparrow \\ K & \longrightarrow & V \end{array}$$

With the valuation criterion of properness, then any point P of V extends to an integral section of $\mathcal{V}$.
What is especially interesting and absolutely remarkable is that any abelian variey defined over a number field admits an integral model which is also a group variety, it is called a Néron Model.

Arakelov Divisors I

What was noticed and mainly solved by Arakelov is that in standard Algebraic Geometry when you have a variety over $\mathcal{O}_K$ you can not do intersection theory because the moving lemma doesn't hold still, divisors move "to infinity" when moving them. The idea of Arakelov has been (amongst other things) to had the archimedean places to the usual shceme theory over $\mathcal{O}_K$.

Definition (Arakelov Divisor) Over $\mathcal{O}_K$, it is a formal sum

$$\bar{E} = \sum_{\mathfrak{p} \in M_K} m_{\mathfrak{p}}[\mathfrak{p}] \text{ with } m_{\mathfrak{p}} \in \begin{cases} \mathbb{Z} \text{ for } v \text{ finite} \\ \mathbb{R} \text{ for } v \text{ infinite} \end{cases}$$

Arakelov Divisors II

Definition The degree of an Arakelov divisor over $\mathcal{O}_K$ is defined by

$$\widehat{\deg}(\bar{E}) = \sum_{\mathfrak{p} \text{ finite}} m_v \log \operatorname{Norm}([\mathfrak{p}]) - \sum_{\sigma \text{ infinite}} m_\sigma [K_\sigma : \mathbb{R}]$$

In usual Algebraic Geometry there is just the left hand side. What is of special interest to us is when $\mathcal{P}$ is some integral section associated to a rational point P. We can then consider the pullback $\mathcal{P}^*\mathcal{D}$ of the Zariski closure $\mathcal{D}$ of some divisor $D \in \operatorname{Div}(V)$. Then $\mathcal{P}^*\mathcal{D}$ is a divisor over $\mathcal{O}_K$, the question that remains and that was also answered by Arakelov is: what to do of the places at infinity?

Arakelov Diviors III

In the case of divisors the preceding coefficients m_σ at places at infinity are defined by by a Green function. This was an other great insight of Arakelov. It is a functions with a logartihmic pole along D. It means that locally, if $f = 0$ is a functions that defines D in $K_\sigma = \mathbb{C}$ or $\mathbb{R}$, the coefficient m_σ is given by some function $G(D, \cdot) : V(K_\sigma) \setminus \mathrm{supp}(D) \to \mathbb{R}$ such that

$$G(D, P) + \log |f(P)|$$

extends to a continuous function on $V(K_\sigma)$.
Defined this way we have the following theorem:
Theorem(Arakelov) Once $\mathcal{D}$ has been compactified with the preceeding green function, the function defined by

$$h_{Ar}(P) = \frac{1}{[K : \mathbb{Q}]} \widehat{\deg} \mathcal{P}^* \mathcal{D},$$

is a Weil height function;

- Such kind of compactifications at infinity has been widely generalized and is know known as Arakelov Theory. In spite of points one can makes sense of the heights of higher dimensional objects and in spite of divisors (codim 1) one can do Arakelov theory with higher dimensional cycles
- An important aspect of Arakelov Theory is that it also generalizes the correspondence between line bundles and divisors. In spite of compactified divisors we use metrized line bundles.
- In this generalization one can define the height of a variety with respect to some cycle but also in the example of abelian varieties, Gerd Faltings had had the insight to define

$$h_{\mathrm{Falt}}(A) = \frac{1}{[K:\mathbb{Q}]}\widehat{\deg} e_0^* \omega_{\mathcal{N}/\mathcal{O}_K}.$$