Introduction to the Weil height

1041, November 23, 2019

Philosophy: let X be a set of interesting algebraic objects. By a height function we understand a map

$$h : X \to [0, \infty)$$

such that:

(i) for x in X, the value of $h(x)$ measures how complicated x is,

(ii) we have $h(x) = 0$ if and only if x is a trivial element of X,

(iii) for nice subsets $Y \subseteq X$ and positive numbers T, the subset

$$\{y \in Y : h(y) \leq T\}$$

is a finite set.

The Weil height: the Weil height on $\overline{\mathbb{Q}}$ can be defined in two different ways.

(1.) Let $\alpha \neq 0$ be an algebraic number and

$$m_\alpha(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_{d-1} x + a_d$$

its minimal polynomial in $\mathbb{Z}[x]$. The Weil height of α is given by

$$h(\alpha) = d^{-1} \int_0^1 \log\left| m_\alpha\left(e^{2\pi i t}\right)\right| \, \mathrm{d}t.$$

(2.) Let k be an algebraic number field that contains $\alpha \neq 0$, and let

$$\left\{ |\ |_v : v \text{ a place of } k \right\}$$

be the collection of all normalized absolute values on k. The Weil height of α is also

$$h(\alpha) = \sum_v \log^+ |\alpha|_v.$$

Note: if $\alpha \neq 0$ then by the product formula

$$\sum_v \log |\alpha|_v = 0.$$

An *absolute value* on a field K is a map

$$| \; | : K \to [0, \infty)$$

that satisfies:

(i) $|x| = 0$ if and only if $x = 0$,

(ii) $|xy| = |x||y|$ for all x and y in K,

(iii) $|x + y| \leq |x| + |y|$ for all x and y in K.

For some absolute values it may happen that

(iv) $|x + y| \leq \max\{|x|, |y|\}$ for all x and y in K.

The inequality (iv) is called the *strong triangle inequality*. If $| \; |$ satisfies (i), (ii), and (iii), but not (iv), then $| \; |$ is *archimedean*. If $| \; |$ satisfies (i), (ii), and (iv), then $| \; |$ is *non-archimedean*.

If $|\ |$ is an absolute value on K then

$$(x, y) \mapsto |x - y|$$

is a metric that induces a metric topology in K. Two absolute values are *equivalent* if they induce the same metric topology. An equivalence class determined by a nontrivial absolute value is called a *place* of K. Equivalent absolute values on K can be characterized in a simple way.

Lemma 1. *Let $|\ |_1$ and $|\ |_2$ be two absolute values on K. Then the following are equivalent:*

(i) $|\ |_1$ and $|\ |_2$ induce the same metric topology in K,

(ii) $\{x \in K : |x|_1 < 1\} = \{x \in K : |x|_2 < 1\}$,

(iii) there exists a positive number θ such that $|x|_1^\theta = |x|_2$ for all x in K.

We write $\| \ \|_\infty$ for the "usual" archimedean absolute value on $\mathbb{Q}$. For each prime number p we write $\| \ \|_p$ for the "usual" p-adic absolute value on $\mathbb{Q}$.

If $\beta \neq 0$ is a rational number then

$$\beta = \pm 2^{w_2(\beta)} 3^{w_3(\beta)} 5^{w_5(\beta)} 7^{w_7(\beta)} \ldots,$$

where $\{w_q(\beta)\}$ is an integer indexed by the set of prime numbers q. The usual p-adic absolute value of β is

$$\|\beta\|_p = p^{-w_p(\beta)}.$$

Then $\| \ \|_p$ is a non-archimedean absolute value on $\mathbb{Q}$. Note that

$$\{\beta \in \mathbb{Q} : \|\beta\|_p \leq 1\} = \{a/b \in \mathbb{Q} : p \nmid b\}$$

is an integral domain, and

$$\{\beta \in \mathbb{Q} : \|\beta\|_p < 1\} = \{a/b \in \mathbb{Q} : p|a, \text{ and } p \nmid b\}$$

is its unique maximal ideal.

Using Lemma 1 we get:

Theorem 1. [Ostrowski] *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to exactly one of the absolute values in the set*

$$\Big\{\|\ \|_\infty,\ \|\ \|_2,\ \|\ \|_3,\ \|\ \|_5,\ \|\ \|_7,\ \dots\Big\}$$

Hence the collection of all places of $\mathbb{Q}$ is indexed by the set

$$\Big\{\infty, 2, 3, 5, 7, \dots\Big\}.$$

The collection of nontrivial absolute values on $\mathbb{Q}$ satisfies:

Theorem 2. (The Product Formula in $\mathbb{Q}$) *If $\beta \neq 0$ is a rational number then*

$$\|\beta\|_\infty \prod_p \|\beta\|_p = 1.$$

Alternatively, we have

$$\log\|\beta\|_\infty + \sum_p \log\|\beta\|_p = 0.$$

Proof. Assume that $\beta \neq 0$ has the factorization

$$\beta = \pm 2^{w_2(\beta)} 3^{w_3(\beta)} 5^{w_5(\beta)} 7^{w_7(\beta)} \cdots.$$

Then

$$\prod_p \|\beta\|_p = \prod_p p^{-w_p(\beta)} = \|\beta\|_\infty^{-1},$$

which proves the product formula for $\mathbb{Q}$. $\square$

The Weil height of the rational number $\beta \neq 0$ is the positive number

$$H(\beta) = \max\{1, \|\beta\|_\infty\} \prod_p \max\{1, \|\beta\|_p\},$$

and the (logarithmic) Weil height of $\beta \neq 0$ is the nonnegative real number

$$h(\beta) = \log H(\beta) = \log^+ \|\beta\|_\infty + \sum_p \log^+ \|\beta\|_p.$$

If $\beta = r/s \neq 0$ and $\gcd(r, s) = 1$, then

$$h(r/s) = \max\{\log \|r\|_\infty, \log \|s\|_\infty\},$$

At each place u of $\mathbb{Q}$ the field $\mathbb{Q}$ is a metric space with metric defined by

$$(\alpha, \beta) \mapsto \|\alpha - \beta\|_u,$$

Here we can use $u = \infty$ or $u = p$, where p is a prime number. We write $\mathbb{Q}_u$ for the *completion* of $\mathbb{Q}$ with respect to the metric induced by $\| \|_u$. Then $\mathbb{Q}_\infty = \mathbb{R}$ is the field of real numbers, and for each prime p the completion $\mathbb{Q}_p$ is the field of p-adic numbers. In both cases $\mathbb{Q}$ is a dense subfield of $\mathbb{Q}_u$.

Let $\overline{\mathbb{Q}_u}$ be an algebraic closure of the complete field $\mathbb{Q}_u$. For example, $\overline{\mathbb{Q}_\infty} = \mathbb{C}$. It turns out that the absolute value $\| \|_u$ on $\mathbb{Q}_u$ has a *unique* extension to an absolute value on $\overline{\mathbb{Q}_u}$. This allows us to determine all the absolute values (and so all the places) of an algebraic number field k.

Let $k/\mathbb{Q}$ be a number field with global degree

$$d = [k : \mathbb{Q}],$$

and v a *place* of k. Each absolute value from v determines the same metric topology in k. We write k_v for the *completion* of k with respect to the metric topology. It follows that k is a dense subfield of the complete field k_v. For example, $\mathbb{Q}_\infty = \mathbb{R}$, and for each prime number p, $\mathbb{Q}_p$ is the field of p-*adic numbers*.

If $\| \ \|_v$ is an absolute value in the place v of k, then $\| \ \|_v$ restricted to $\mathbb{Q}$ must equal $\| \ \|_u$ for a unique place

$$u \in \{\infty, 2, 3, 5, 7, \dots\},$$

such that $\| \ \|_v$ restricted to $\mathbb{Q}$ is an absolute value in u. In this case we write

$$v|u, \quad \text{or "}v\text{ lies over }u\text{"}.$$

We also find that the completion k_v is a *finite* extension of the field $\mathbb{Q}_u$, and we write

$$d_v = [k_v : \mathbb{Q}_u].$$

for the local degree.

Let α be an algebraic number, $k = \mathbb{Q}(\alpha)$, and $d = [k : \mathbb{Q}]$. Let u be a place of $\mathbb{Q}$. We wish to determine $\|\alpha\|_v$ at places v of k such that $v|u$.

(i) Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ be the conjugates of α in $\overline{\mathbb{Q}_u}$, and write

$$m_\alpha(x) = \prod_{j=1}^{d} (x - \alpha_j)$$

for the minimal polynomial in $\mathbb{Q}[x]$.

(ii) Factor $m_\alpha(x)$ into irreducible polynomials in $\mathbb{Q}_u[x]$:

$$m_\alpha(x) = g_1(x) g_2(x) \cdots g_J(x).$$

At this point we know there will be exactly J places $v_1, v_2, \ldots, v_J$, of k such that $v_j|u$.

(iii) To determine v_1, factor $g_1(x)$ in $\overline{\mathbb{Q}_u}[x]$:

$$g_1(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{I_1}).$$

(iv) Recall that

$$\text{Norm} : \mathbb{Q}_u(\alpha_1)^\times \to \mathbb{Q}_u^\times$$

is a homomorphism such that

$$\begin{aligned} \text{Norm}(\alpha_1) = \text{Norm}(\alpha_2) &= \cdots \\ &= \alpha_1\alpha_2\cdots\alpha_{I_1} \\ &= (-1)^{I_1} g_1(0). \end{aligned}$$

(v) Now define $\|\alpha\|_{v_1}$ by

$$\|\alpha\|_{v_1}^{I_1} = \|\,\text{Norm}(\alpha_1)\|_u = \|g_1(0)\|_u.$$

(vi) Some useful identities:

$$k_{v_1} = \mathbb{Q}_u(\alpha_1) \quad \text{and} \quad [k_{v_1} : \mathbb{Q}_u] = d_{v_1} = I_1.$$

and

$$\sum_{j=1}^{J} [k_{v_j} : \mathbb{Q}_u] = \sum_{v|u} d_v = \sum_{j=1}^{J} I_j = [k : \mathbb{Q}] = d.$$

Let u be a place of $\mathbb{Q}$ and v a place of k such that $v|u$. Then $\| \ \|_v$ is an absolute value in v which extends the "usual" absolute value $\| \ \|_u$ in u. We now define a second absolute value $| \ |_v$ in the place v by

$$| \ |_v = \| \ \|_v^{d_v/d}, \quad \text{or} \quad \log | \ |_v = \frac{d_v}{d} \log \| \ \|_u,$$

where

$$d_v = [k_v : \mathbb{Q}_u] \quad \text{and} \quad d = [k : \mathbb{Q}].$$

The absolute values $| \ |_v$ are *normailzed*.

Theorem 3. (The Product Formula) *Let $\alpha \neq 0$ be an algebraic number contained in k, then*

$$\prod_v |\alpha|_v = 1.$$

Alternatively, we have

$$\sum_v \log |\alpha|_v = 0.$$

Proof: Using the previous notation, at each place u of $\mathbb{Q}$ we have

$$\begin{aligned}\sum_{v|u} d_v \log \|\alpha\|_v &= \sum_{j=1}^{J} I_j \log \|\alpha\|_{v_j} \\ &= \sum_{j=1}^{J} \log \|g_j(0)\|_u \\ &= \log \|m_\alpha(0)\|_u.\end{aligned}$$

Now $m_\alpha(0)$ is a nonzero point in $\mathbb{Q}$. Therefore by the product formula in $\mathbb{Q}$:

$$\begin{aligned}\sum_{v} \log |\alpha|_v &= \sum_{u} \left(\sum_{v|u} \log |\alpha|_v \right) \\ &= d^{-1} \sum_{u} \left(\sum_{v|u} d_v \log \|\alpha\|_v \right) \\ &= d^{-1} \sum_{u} \log \|m_\alpha(0)\|_u \\ &= 0.\end{aligned}$$

This proves the product formula for each point $\alpha \neq 0$ in k.

Again let $\alpha \neq 0$ be an algebraic number contained in k. We define the multiplicative Weil height of α by

$$H(\alpha) = \prod_v \max\{1, |\alpha|_v\},$$

and the logarithmic Weil height of α by

$$h(\alpha) = \sum_v \log^+ |\alpha|_v.$$

Here the product and sum are over the set of all places v of a number field k that contains α. It can be shown that H and h are well defined because there value does not depend on the choice of number field k that contains α. Therefore we have both

$$H : \overline{\mathbb{Q}}^\times \to [1, \infty), \quad \text{and} \quad h : \overline{\mathbb{Q}}^\times \to [0, \infty).$$

Some authors call these *absolute* heights.

Properties of the Weil height: Let r/s be a rational number, ζ a root of unity, and let $\alpha \neq 0$ and $\beta \neq 0$ be elements of $\overline{\mathbb{Q}}^{\times}$. Then

(i) $h(\alpha \pm \beta) \leq \log 2 + h(\alpha) + h(\beta)$,

(ii) $h(\alpha\beta) \leq h(\alpha) + h(\beta)$,

(iii) $h(\zeta\alpha) = h(\alpha)$,

(iv) $h\Big(\alpha^{r/s}\Big) = |r/s|_\infty h(\alpha)$,

(v) $h(r/s) = \max\{\log |r|_\infty, \log |s|_\infty\}$,

(vi) $h(\alpha) = 0$ if and only if α is a root of unity.

Theorem 4. *Let $\alpha \neq 0$ and $\beta \neq 0$ distinct elements of a number field k, and let S be a nonempty subset of places of k. Then we have*

$$\Big(2H(\alpha)H(\beta)\Big)^{-1} \leq \prod_{v \in S} |\alpha - \beta|_v \leq 2H(\alpha)H(\beta).$$

Proof: If v is an archimedean place of k then

$$\begin{aligned} \|\alpha - \beta\|_v &\leq \|\alpha\|_v + \|\beta\|_v \\ &\leq 2\max\{\|\alpha\|_v, \|\beta\|_v\} \\ &\leq 2\max\{1, \|\alpha\|_v\}\max\{1, \|\beta\|_v\} \end{aligned}$$

and

$$|\alpha - \beta|_v \leq 2^{d_v/d}\max\{1, |\alpha|_v\}\max\{1, |\beta|_v\}.$$

If v is non-archimedean we use the strong triangle inequality and get

$$|\alpha - \beta|_v \leq \max\{1, |\alpha|_v\}\max\{1, |\beta|_v\}.$$

Recall that

$$\sum_{v|\infty} (d_v/d) = 1.$$

It follows that

$$\prod_{v\in S} |\alpha-\beta|_v \le 2 \prod_{v\in S} \max\{1,|\alpha|_v\} \max\{1,|\beta|_v\}$$
$$\le 2H(\alpha)H(\beta).$$

This proves the upper bound.

Let T be the complement of S in the set of all places of k. If T is empty the theorem is trivial. If T is not empty

$$\prod_{v\in S} |\alpha-\beta|_v \prod_{v\in T} |\alpha-\beta|_v = 1$$

by the product formula. Therefore

$$\prod_{v\in S} |\alpha-\beta|_v^{-1} = \prod_{v\in T} |\alpha-\beta|_v$$
$$\le 2H(\alpha)H(\beta)$$

by what we have already proved. This verifies the lower bound.

Let $\gamma \neq 0$ be contained in a number field k. Assume that

$$0 < |\gamma|_v < 1$$

for some place v of k. Then

$$\alpha = \sum_{n=1}^{\infty} \gamma^{n!}$$

is an element of the completion k_v. Let

$$\beta_N = \sum_{n=1}^{N} \gamma^{n!}$$

be a partial sum, which is obviously an algebraic number in k. Evidently

$$|\alpha - \beta_N|_v \leq \left| \sum_{n=N+1}^{\infty} \gamma^{n!} \right|_v$$

tends rapidly to 0 as $N \to \infty$. If α is algebraic it can be shown that the lower bound in the previous inequality is false for large N. It follows that α is transcendental.

Some useful references:

E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge U. Press, 2006

W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* 3rd ed. Springer-Verlag, 2010

A. Weil, Arithmetic on algebraic varieties, *Annals of Math.* 53, 412-444, (1951)

A. Weil, *Basic Number Theory*, Springer-Verlag, 1973