UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

CONTRIBUCIONES A LA TEORIA DE LOS POLINOMIOS RALOS

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Martín Avendaño

Director de tesis: Dra. Teresa Krick.

Buenos Aires, 21 de Diciembre de 2007

CONTRIBUCIONES A LA TEORIA DE LOS POLINOMIOS RALOS

Se presentan contribuciones al estudio de los polinomios ralos en tres diferentes aspectos. El primer resultado es un algoritmo que permite encontrar todos los factores irreducibles, de grado acotado por una constante prefijada, de un polinomio ralo multivariado con coeficientes algebraicos. El costo del algoritmo es polinomial en la longitud bit de su codificación rala y en la constante prefijada, y exponencial en el número de variables (esta dependencia exponencial siendo inevitable). El segundo es un algoritmo que permite interpolar un polinomio ralo univariado con coeficientes enteros, con t términos no nulos, a partir de $2t$ puntos enteros conocidos de altura chica. El último es una cota sobre la cantidad de soluciones reales que puede tener un sistema de ecuaciones ralas que consiste de un polinomio bivariado y una recta. A partir de esta se deriva un algoritmo sencillo para verificar si un polinomio lineal divide o no un polinomio ralo con coeficientes reales.

Palabras Clave: Polinomios Ralos, Factorización, Interpolación.

CONTRIBUTIONS TO THE THEORY OF LACUNARY POLYNOMIALS

We present contributions to the study of lacunary polynomials in three different aspects. The first result is an algorithm which finds all the factors, of degree bounded by a fixed constant, of a multivariate lacunary polynomial with algebraic coefficients. The cost of the algorithm is polynomial in the bit length of the lacunary encoding of the polynomial and in the fixed constant, and exponential in the number of variables (this last dependence being unavoidable). The second result is an algorithm which interpolates an univariate lacunary polynomial with integer coefficients and t non-zero terms from $2t$ known integer points of small height. The last result is a bound on the number of real roots of a system of lacunary polynomials consisting on a bivariate polynomial and a line. From this result, we derive a simple algorithm which decides whether a linear polynomial divides a bivariate lacunary polynomial with real coefficients or not.

Keywords: Lacunary Polynomials, Factorization, Interpolation.

Contents

Chapter 3

Preliminaries

3.1 Absolute values

Definition 3.1.1. *Let K be a field. An absolute value v on K is a map $v : K \to \mathbb{R}_{\geq 0}$ satisfying the following three properties:*

- $v(x) = 0 \quad \Leftrightarrow \quad x = 0$,
- $v(xy) = v(x)\, v(y) \quad \forall\, x, y \in K$,
- $v(x + y) \leq v(x) + v(y) \quad \forall\, x, y \in K$ *(triangle inequality).*

We also use $|x|_v$ to denote $v(x)$. If the absolute value satisfies, in addition to the triangle inequality, the stronger condition:

- $v(x + y) \leq \max\{v(x), v(y)\} \quad \forall\, x, y \in K$ *(ultrametric inequality),*

then we say that it is non-Archimedean.

It is clear, from the definition, that every absolute value v on a field K satisfies $v(1) = v(-1) = 1$ and $v(x) = v(-x)$ for all $x \in K$.

Example. *1. On an arbitrary field K, the trivial absolute value:*

$$v(x) = \begin{cases} 0 & \text{if} \quad x = 0 \\ 1 & \text{if} \quad x \neq 0. \end{cases}$$

2. On $\mathbb{R}$ or $\mathbb{C}$, the standard absolute value $|x|$.

3. On $\mathbb{Q}$, for every integer prime number $p \in \mathbb{N}$, the p-adic absolute value v_p given by:

$$v_p\left(p^r \frac{a}{b}\right) = p^{-r},$$

where $a, b, r \in \mathbb{Z}$, $b > 0$, $p \nmid a$ and $p \nmid b$.

4. *On $K(T)$, the absolute value $v_\infty(F/G) = 2^{\deg(F)-\deg(G)}$, where F, G are non-zero polynomials in $K[T]$.*

5. *On $K(T)$, for every $P \in K[T]$ irreducible, the absolute value v_P given by:*

$$v_P\left(P^r \frac{F}{G}\right) = 2^{-r},$$

where $r \in \mathbb{Z}$, $F, G \in K[T] - \{0\}$, $P \nmid F$ and $P \nmid G$.

The absolute values given in items (1) to (5), except (2), are non-Archimedean. The standard absolute value on $\mathbb{C}$ is written v_∞, $|\cdot|$, $|\cdot|_\infty$ or $|\cdot|_{v_\infty}$ indistinctly, and the p-adic absolute value v_p on $\mathbb{Q}$ is also $|\cdot|_p$ or $|\cdot|_{v_p}$.

Lemma 3.1.2. *Let v be an absolute value on a field K. Then v is non-Archimedean if and only if $v(\mathbb{N})$ is bounded.*

Proof. If v is non-Archimedean, then for every natural number $n \in \mathbb{N}$ we have:

$$v(n) = v(1 + \cdots + 1) \leq \max\{v(1), \ldots, v(1)\} = 1,$$

and therefore $v(\mathbb{N})$ is bounded. Now suppose that $v(n) \leq C$ for all $n \in \mathbb{N}$. Then, for every $x, y \in K$,

$$v(x+y)^n \leq \sum_{i=0}^{n} \left|\binom{n}{i}\right|_v v(x)^i v(y)^{n-i} \leq nC \max\{v(x), v(y)\}^n,$$

and taking its n-th root,

$$v(x+y) \leq (nC)^{1/n} \max\{v(x), v(y)\}.$$

The ultrametric inequality follows taking limits in the previous expression. □

Lemma 3.1.3. *Let v be a non-Archimedean absolute value on a field K. Let $a_1, \ldots, a_n \in K$ be such that $v(a_1) > v(a_i)$ for all $i \neq 1$. Then $v(a_1 + \cdots + a_n) = v(a_1)$.*

Proof. It is enough to prove the case $n = 2$. Suppose $v(a_1) > v(a_2)$. The inequalities:

$$v(a_1) = v(a_1 + a_2 - a_2) \leq \max\{v(a_1 + a_2), v(a_2)\} \leq \max\{v(a_1), v(a_2), v(a_2)\} = v(a_1)$$

imply that $v(a_1) = \max\{v(a_1 + a_2), v(a_2)\}$. This maximum is not $v(a_2)$ because $v(a_1) > v(a_2)$. Then $v(a_1) = v(a_1 + a_2)$. □

An absolute value v on a field K, induces on it the metric $d(x, y) = v(x - y)$. The arithmetic operations (addition, additive inverse, multiplication and multiplicative inverse) are continuous with respect to this metric.

Lemma 3.1.4. *Let v_1 and v_2 be non-trivial absolute values on a field K. Then, the following statements are all equivalent:*

1. *v_1 and v_2 induce the same topology.*

2. *for all $x \in K$, if $v_1(x) < 1$ then $v_2(x) < 1$.*

3. *$\exists \lambda > 0$ such that $v_1(x) = v_2(x)^\lambda$ for every $x \in K$.*

Proof. $(1 \Rightarrow 2)$: Let $x \in K$ be such that $v_1(x) < 1$. Then $x^n \to 0$ with respect to the topology induced by v_1. Since both absolute values induce the same topology, we also have $x^n \to 0$ with respect to v_2, i.e. $v_2(x)^n \to 0$. This implies that $v_2(x) < 1$.
$(2 \Rightarrow 3)$: We know that $v_1(x) < 1$ implies $v_2(x) < 1$, and using this fact for x^{-1}, we have that $v_1(x) > 1$ implies $v_2(x) > 1$. Since v_1 is non-trivial, there exists $z \in K$ such that $v_1(z) > 1$. Let $a = v_1(z)$, $b = v_2(z)$ and $\lambda = \log(a)/\log(b)$. Note that $v_1(z) = v_2(z)^\lambda$. Now take any non-zero $x \in K$. Then $v_1(x) = v_1(z)^\alpha$ for some $\alpha \in \mathbb{R}$. It is enough to prove that $v_2(x) = v_2(z)^\alpha$, because in this case we have $v_1(x) = v_1(z)^\alpha = v_2(z)^{\alpha\lambda} = v_2(x)^\lambda$. If $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ satisfy $\alpha < m/n$, then $v_1(x) < v_1(z)^{m/n}$. This implies that $v_1(x^n/z^m) < 1$ and then $v_2(x^n/z^m) < 1$, i.e. $v_2(x) < v_2(z)^{m/n}$. Therefore $v_2(x) \leq v_2(z)^\alpha$ because we can freely choose m/n as close to α as we want. The other inequality follows using the same idea, but taking $\alpha > m/n$.
$(3 \Rightarrow 1)$: Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in K. Then: $x_n \to x$ with respect to the topology induced by $v_1 \Leftrightarrow v_1(x_n - x) = v_2(x_n - x)^\lambda \to 0 \Leftrightarrow v_2(x_n - x) \to 0 \Leftrightarrow x_n \to x$ with respect to v_2. □

Theorem 3.1.5. [Ostrowski] *Let v be a non-trivial absolute value on $\mathbb{Q}$. Then either v is Archimedean and there exists $0 < \lambda \leq 1$ such that $v(x) = |x|^\lambda$, or v is non-Archimedean and there exists a prime number $p \in \mathbb{N}$ and $\lambda > 0$ such that $v(x) = v_p(x)^\lambda$.*

Proof. For every integer $k \in \mathbb{Z}$ we have $v(k) = v(|k|) = v(1 + \cdots + 1) \leq v(1) + \cdots + v(1) = |k|$. Let $a, b, m \in \mathbb{Z}$ with $a > 1$, $b > 1$ and $m \geq 0$. Suppose that $b^m = c_0 + c_1 a + \cdots + c_n a^n$ is the a-adic representation of b^m, i.e. $0 \leq c_i < a$ for all i and $c_n \neq 0$. In particular, we have $a^n \leq b^m$ and then $n \leq m \log(b)/\log(a)$. Define $M = \max\{1, v(a)\}$.

$$\begin{aligned} v(b^m) &\leq v(c_0) + \cdots + v(c_n)v(a)^n \leq a(1 + \cdots + v(a)^n) \\ &\leq a(1 + \cdots + M^n) \leq a(n+1)M^n \end{aligned}$$

$$\begin{aligned} &\Rightarrow \quad v(b)^m \leq a(n+1)M^n \leq a\left(1 + m\frac{\log(b)}{\log(a)}\right) M^{m\frac{\log(b)}{\log(a)}} \\ &\Rightarrow \quad \left(\frac{v(b)}{M^{\frac{\log(b)}{\log(a)}}}\right)^m \leq a\left(1 + m\frac{\log(b)}{\log(a)}\right) \\ &\Rightarrow \quad \frac{v(b)}{M^{\frac{\log(b)}{\log(a)}}} \leq \left(a\left(1 + m\frac{\log(b)}{\log(a)}\right)\right)^{1/m} \to 1 \\ &\Rightarrow \quad v(b) \leq M^{\frac{\log(b)}{\log(a)}} = \max\{1, v(a)^{\frac{\log(b)}{\log(a)}}\}. \qquad (*) \end{aligned}$$

Case v Archimedean: By Lemma 3.1.3, there exists $b \in \mathbb{N}$ such that $v(b) > 1$. If we had $v(a) \leq 1$ for some integer $a > 1$, then $(*)$ would imply the contradiction $v(b) \leq 1$. Therefore $v(a) > 1$ for every integer $a > 1$. Then, for every $a, b \in \mathbb{N}$ with $a > 1$ and $b > 1$, the inequality $(*)$ is

$$v(b) \leq v(a)^{\frac{\log(b)}{\log(a)}}$$

or more simply $v(b)^{1/\log(b)} \leq v(a)^{1/\log(a)}$. By the symmetry of this expression, swapping a and b, we get the identity:

$$v(b)^{1/\log(b)} = v(a)^{1/\log(a)} \quad \forall\, a, b \in \mathbb{N},\ a > 1,\ b > 1.$$

Now take $b \in \mathbb{N}$, $b > 1$ and let $0 < \lambda \leq 1$ be such that $v(b) = b^{\lambda}$. For any $a \in \mathbb{N}$, $a > 1$ we have:

$$v(a) = v(b)^{\frac{\log(a)}{\log(b)}} = b^{\lambda \frac{\log(a)}{\log(b)}} = 2^{\log(b)\lambda \frac{\log(a)}{\log(b)}} = 2^{\lambda \log(a)} = a^{\lambda}.$$

This means that for all $k \in \mathbb{Z}$, $v(k) = v(|k|) = |k|^{\lambda}$ holds. We conclude taking $x = p/q \in \mathbb{Q}$ with $p \in \mathbb{N}$ and $q \in \mathbb{Z}$, and then

$$v(x) = v\left(\frac{p}{q}\right) = \frac{v(p)}{v(q)} = \frac{|p|^{\lambda}}{|q|^{\lambda}} = |x|^{\lambda}.$$

Case v non-Archimedean: Here we have $v(x) \leq 1$ for all $x \in \mathbb{Z}$. Define

$$I = \{x \in \mathbb{Z} \ :\ v(x) < 1\}.$$

By the multiplicativity of v and the ultrametric inequality, the set I is an ideal of Z. Moreover, if $x, y \in \mathbb{Z}$ and $xy \in I$, then $v(x) \leq 1$, $v(y) \leq 1$ and $v(xy) < 1$. This is only possible if $v(x) < 1$ or $v(y) < 1$, i.e. $x \in I$ or $y \in I$. Therefore I is a non-trivial prime ideal of $\mathbb{Z}$. Let $p \in \mathbb{N}$ be the prime number such that $I = p\mathbb{Z}$. For any $x = p^r \frac{a}{b} \in \mathbb{Q} - \{0\}$ with $a, b, r \in \mathbb{Z}$, $b > 0$, $p \nmid a$ and $p \nmid b$, we have that $a \notin I$ and $b \notin I$. Then $v(a) = 1$, $v(b) = 1$ and

$$v(x) = v(p)^r \frac{v(a)}{v(b)} = v(p)^r = p^{\frac{\log(p)}{\log(v(p))}\, r} = v_p(x)^{-\frac{\log(p)}{\log(v(p))}}.$$

Note that $\lambda = -\log(p)/\log(v(p)) > 0$, because $p \in I$ implies $v(p) < 1$. □

Theorem 3.1.6. *Let v be an absolute value on a field K. Then, there exists an extension K_v/K and an absolute value $\overline{v}$ on K_v extending v, such that K_v is complete and $K \subseteq K_v$ is dense. Moreover, if E/K is an extension with an absolute value w extending v, such that E is complete and $K \subseteq E$ is dense, then there exists a K-isomorphism of fields $\sigma : E \to K_v$ with $w = \overline{v} \circ \sigma$.*

Proof. See [Lan93, Ch. 12, Prop. 2.1]. □

The field K_v together with the absolute value $\overline{v}$ of Theorem 3.1.6 is called the completion of K with respect to v. For instance, the completion of $\mathbb{Q}$ with respect to $|\cdot|$ is $\mathbb{R}$, and the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is the field of p-adic numbers $\mathbb{Q}_p$.

Theorem 3.1.7. *Let K be a complete field with respect to a non-trivial absolute value v and let E/K be an algebraic extension. Then, there exists a unique absolute value w on E extending v. Moreover, if E/K is finite, then E is complete with respect to w.*

Proof. See [Lan93, Ch. 12, Prop. 2.5]. □

Let K be a complete field with respect to a non-trivial absolute value v and let E/K be a Galois extension. If w is an absolute value on E extending v and $\sigma \in \mathrm{Gal}(E/K)$, then $w \circ \sigma$ is also an absolute value on E extending v. By Theorem 3.1.7 (uniqueness), we have $w = w \circ \sigma$. Taking the product over all $\sigma \in \mathrm{Gal}(E/K)$, we get:

$$w(x)^{[E:K]} = \prod_{\sigma \in \mathrm{Gal}(E/K)} w(\sigma(x)) = w\left(N_K^E(x)\right) = v\left(N_K^E(x)\right),$$

i.e.,

$$w(x) = v\left(N_K^E(x)\right)^{1/[E:K]}. \tag{3.1}$$

For instance, if $(K, v) = (\mathbb{R}, |\cdot|)$, Theorem 3.1.7 and Formula (3.1) prove that the only extension of $|\cdot|$ to $\mathbb{C}$ is given by $|a + bi| = (a^2 + b^2)^{1/2}$.

Let v be a non-trivial absolute value on a field K, let K_v be the completion of K with respect to v and let $\overline{K_v}$ be the algebraic closure of K_v. The absolute value $\overline{v}$ on K_v, and the only absolute value on $\overline{K_v}$ extending $\overline{v}$ will all be written v for simplicity of notation.

Every finite extension E/K can be embedded in $\overline{K_v}$, and for every embedding $\sigma : E \to \overline{K_v}$, we get an absolute value $w = v \circ \sigma$ extending v. The converse is given by the following theorem.

Theorem 3.1.8. *Let v be a non-trivial absolute value on a field K and let E/K be a finite extension with an absolute value w extending v. Then, there exists an embedding $\sigma \in \mathrm{Hom}_K(E, \overline{K_v})$ such that $w = v \circ \sigma$.*

Proof. Let E_w be the completion of E with respect to w, let $\overline{E_w}$ be the algebraic closure of E_w and let K_w be the (topologic) closure of K in E_w. The composite EK_w is contained in E_w because $E \subseteq E_w$ and $K_w \subseteq E_w$. Besides, EK_w/K_w is finite (because E/K is finite) and K_w is complete (because it is a closed subset in the complete field E_w), thus EK_w is also complete (by Theorem 3.1.7). Since $E \subseteq EK_w$, we also have $E_w \subseteq EK_w$. Therefore $E_w = EK_w$ and E_w/K_w is a finite extension with $[E_w : K_w] = [EK_w : K_w] \leq [E : K]$. In particular, $\overline{E_w}$ is an algebraic closure of K_w.
The field K_w with the absolute value w satisfies the hypothesis of Theorem 3.1.6, i.e. K_w is complete, K is dense in K_w and $w|_K = v$. Then, there exists a K-isomorphism $\sigma : K_w \to K_v$ such that $w = v \circ \sigma$. We can extend σ to a K-isomorphism $\tilde{\sigma} : \overline{E_w} \to \overline{K_v}$, and by Formula (3.1), we still have $w = v \circ \tilde{\sigma}$ in $\overline{E_w}$. We conclude by restricting $\tilde{\sigma}$ to E. □

Definition 3.1.9. *Let v be a non-trivial absolute value on a field K and let E/K be a finite extension with an absolute value w extending v. The local degree of the extension is defined as $N_w = [E_w : K_w]$, where K_w is the topologic closure of K in E_w.*

For instance, suppose that $(K, v) = (\mathbb{Q}, |\cdot|)$ and $E = \mathbb{Q}(\xi_5)$ where $\xi_5 = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$ is a 5-th root of the unity. In this case we have $K_v = \mathbb{R}$ and $\overline{K_v} = \mathbb{C}$. According to Theorem 3.1.8, every absolute value w on $\mathbb{Q}(\xi_5)$ extending $|\cdot|$ is given by embedding $\mathbb{Q}(\xi_5)$ in $\mathbb{C}$ with the standard absolute value, i.e. $w(x) = |\sigma(x)|$ where $\sigma : \mathbb{Q}(\xi_5) \to \mathbb{C}$ is a $\mathbb{Q}$-embedding. Therefore there

are only 4 possible absolute values $w_1, \dots, w_4$ on $\mathbb{Q}(\xi_5)$ extending $|\cdot|$, given by the embeddings $\sigma_i(\xi_5) = \xi_5^i$ with $i = 1, \dots, 4$. It is clear that σ_1 is the identity and σ_4 is the complex conjugation, thus they induce the standard absolute value $w_1 = |\cdot|$ on $\mathbb{Q}(\xi_5)$. On the other hand, σ_2 and σ_3 induce a different absolute value w_2 on $\mathbb{Q}(\xi_5)$ because $w_2(1+\xi_5) = |1+\xi_5^2| = |1+\xi_5^3| < 1$ and $w_1(1+\xi_5) = |1+\xi_5| > 1$. As we will see in next theorem, this example generalizes to the general case.

Definition 3.1.10. *Two embeddings $\sigma, \tau : E \to \overline{K_v}$ are conjugated if there exists a K_v-isomorphism $\lambda : \overline{K_v} \to \overline{K_v}$ such that $\sigma = \lambda \circ \tau$.*

Theorem 3.1.11. *Let v be a non-trivial absolute value on a field K and let E/K be a finite extension. Two embeddings $\sigma, \tau : E \to \overline{K_v}$ induce the same absolute value on E if and only if they are conjugated.*

Proof. Suppose that σ and τ are conjugated, i.e. $\sigma = \lambda \circ \tau$ where $\lambda : \overline{K_v} \to \overline{K_v}$ is a K_v-isomorphism. They induce on E the absolute values $w_\sigma = v \circ \sigma$ and $w_\tau = v \circ \tau$ respectively. The absolute values v and $v \circ \lambda$ on $\overline{K_v}$ coincide on K_v. Therefore we have $v = v \circ \lambda$ by Theorem 3.1.7, and then $w_\sigma = v \circ \sigma = v \circ \lambda \circ \tau = v \circ \tau = w_\tau$.
Now suppose that σ and τ induce the same absolute value on E. We extend the K-isomorphism $\lambda = \sigma \circ \tau^{-1} : \tau E \to \sigma E$ to a K_v-isomorphism $\overline{\lambda} : \tau E \cdot K_v \to \sigma E \cdot K_v$ via sequences: since τE is dense in $\tau E \cdot K_v$, every $x \in \tau E \cdot K_v$ is a limit $x = \lim \tau(x_n)$ for some sequence $x_n \in E$, then we can define $\overline{\lambda}(x) = \lim \sigma(x_n)$ that converges because τ and σ induce the same absolute value and $\sigma E \cdot K_v$ is complete. It is clear that $\overline{\lambda}$ is well defined, i.e. it does not depend on the sequence, and $\sigma = \overline{\lambda} \circ \tau$. Besides, $\overline{\lambda} : \tau E \cdot K_v \to \sigma E \cdot K_v$ is an isomorphism because we can define an inverse $\gamma : \sigma E \cdot K_v \to \tau E \cdot K_v$ by extending $\lambda^{-1} : \sigma E \to \tau E$ using the same construction. Moreover, $\overline{\lambda}$ fixes K_v because for every $x \in K_v$ we have a sequence $x_n \in K$ such that $x = \lim x_n = \lim \tau(x_n) = \lim \sigma(x_n) = \overline{\lambda}(x)$. We conclude by extending $\overline{\lambda}$ to the algebraic closure $\overline{K_v}$. □

We write $w|v$ to indicate that w is an absolute value extending v.

Proposition 3.1.12. *Let v be an absolute value on a field K and let E/K be a separable finite extension. Then, for every absolute value w on E extending v, we have*

- $N_w = \#\{\sigma : E \to \overline{K_v},\ K\text{-embedding},\quad s.t.\ w = v \circ \sigma\}$
- $[E : K] = \sum_{w|v} N_w$.

Proof. Let $\alpha \in E$ such that $E = K(\alpha)$ and let $f \in K[X]$ be the minimal polynomial of α over K. Suppose that $f = f_1 \dots f_r$ is the factorization into irreducibles of f in $K_v[X]$, where because α is separable, $f_i \neq f_j$ for $i \neq j$. The embeddings of E in $\overline{K_v}$ are the K-morphisms that map α to a root of f, and two such embeddings are conjugated if and only if they map α to a root of the same factor f_i. This implies that there are exactly r absolute values $w_1, \dots, w_r$ on E extending v. Also, $E_{w_i} = EK_{w_i} = K_{w_i}(\alpha)$, and since K_v and K_{w_i} are isomorphic, f_i (up to this isomorphism) is also the minimal polynomial of α in $K_{w_i}[X]$. This means that $N_{w_i} = [E_{w_i} : K_{w_i}] = [K_{w_i}[\alpha] : K_{w_i}] = \deg(f_i)$ equals the number of embeddings that induce w_i. Moreover $\sum_{i=1}^r N_{w_i} = \sum_{i=1}^r \deg(f_i) = \deg(f) = [E : K]$. □

Corollary 3.1.13. *Let v be an absolute value on a field K and let E/K be a separable finite extension. Then, for every $x \in E$ we have*

$$\prod_{w|v} |x|_w^{N_w} = |N_K^E(x)|_v.$$

Proof. Let $\sigma_1, \dots, \sigma_n$ be all the embeddings of E in $\overline{K_v}$, then

$$v(N_K^E(x)) = \prod_{i=1}^{n} v(\sigma_i(x)) = \prod_{w|v} \prod_{\substack{i: \\ w=v\circ\sigma_i}} w(x) = \prod_{w|v} w(x)^{N_w}.$$

□

Notation. *We write $M_{\mathbb{Q}} = \{v_p \ : \ p \text{ prime or } p = \infty\}$ for the set of standard and p-adic absolute values on $\mathbb{Q}$. Moreover, if $K/\mathbb{Q}$ is a finite extension, we write M_K for the set of all the extension to K of the absolute values in $M_{\mathbb{Q}}$ and M_K^∞ for the subset of Archimedean absolute values in M_K.*

$$M_K = \{w \ : \ w|v \text{ for some } v \in M_{\mathbb{Q}}\} \qquad M_K^\infty = \{w \ : \ w|v_\infty\}.$$

A remarkable property of the absolute values in $M_{\mathbb{Q}}$ is that $\prod_{v\in M_{\mathbb{Q}}} |x|_v = 1$ for all $x \in \mathbb{Q}^\times$. This holds because if $x = \pm p_1^{n_1} \cdots p_r^{n_r} \in \mathbb{Q}^\times$ where $p_i \in \mathbb{N}$ are (distinct) primes and $n_i \in \mathbb{Z}$, then $v_{p_i}(x) = p_i^{-n_1}$ for $1 \le i \le r$ and $v_p(x) = 1$ for all $p \neq p_i$ for some i, and $v_\infty(x) = p_1^{n_1} \dots p_r^{n_r}$.
Moreover, this property holds over every finite extension $K/\mathbb{Q}$ if we take into account the local degrees N_w. More precisely, for every $x \in K^\times$ we have:

$$\prod_{w\in M_K} |x|_w^{N_w} = \prod_{v\in M_{\mathbb{Q}}} \prod_{w|v} |x|_w^{N_w} = \prod_{v\in M_{\mathbb{Q}}} |N_{\mathbb{Q}}^K(x)|_v = 1. \tag{3.2}$$

This identity is known as the "product formula".

Definition 3.1.14. *Let v be an absolute value on a field K and let $a = (a_1, \dots, a_d) \in K^d$ be a vector. We define the 1-norm, 2-norm and ∞-norm by:*

- $\|a\|_{1,v} = \sum_{i=1}^d |a_i|_v$,
- $\|a\|_{2,v} = \left(\sum_{i=1}^d |a_i|_v^2\right)^{1/2}$,
- $\|a\|_v = \|a\|_{\infty,v} = \max\{|a_i| \ : \ 1 \le i \le d\}$.

When $K \subseteq \mathbb{C}$ and v is not explicitly written, we assume $v = v_\infty$. These norms are also defined for polynomials $f = \sum_{i=0}^d a_i x^i \in K[X_1, \dots, X_n]$, using the vector of coefficients of f, i.e. as $\|f\|_{\cdot,v} = \|(a_0, \dots, a_d)\|_{\cdot,v}$.

Remark. *For every $a \in K^d$ we have:*

$$\|a\|_{\infty,v} \le \|a\|_{2,v} \le \|a\|_{1,v} \le d\,\|a\|_{\infty,v}.$$

3.2 Height of algebraic numbers

Definition 3.2.1. *Let $K/\mathbb{Q}$ be a finite extension. The* relative height *(with respect to K) is the map $H_K : K \to \mathbb{R}_{\geq 1}$ given by:*

$$H_K(r) = \prod_{v \in M_K} \max\{1, |r|_v\}^{N_v},$$

where $N_v = [K_v : \mathbb{Q}_v]$.

Proposition 3.2.2. *Let $L/K/\mathbb{Q}$ be a tower of finite extensions. Then*

$$H_L(r) = H_K(r)^{[L:K]}$$

for every $r \in K$.

Proof. Let $v \in M_K$ and $w \in M_L$ such that $w|v$. Since $r \in K$ and $N_w = [L_w : \mathbb{Q}_w] = [L_w : K_w]\,[K_v : \mathbb{Q}_v] = N_v\,[L_w : K_w]$, we have:

$$\max\{1, |r|_w\}^{N_w} = \max\{1, |r|_v\}^{N_v[L_w:K_w]}.$$

Besides, by proposition 3.1.12, we have $\sum_{w|v}[L_w : K_w] = [L : K]$. This implies that:

$$\prod_{\substack{w \in M_L \\ w|v}} \max\{1, |r|_w\}^{N_w} = \prod_{\substack{w \in M_L \\ w|v}} \max\{1, |r|_v\}^{N_v[L_w:K_w]} = \max\{1, |r|_v\}^{N_v \sum_{w|v}[L_w:K_w]} = \max\{1, |r|_v\}^{N_v[L:K]}.$$

We conclude by multiplying over all $v \in M_K$,

$$H_L(r) = \prod_{w \in M_L} \max\{1, |r|_w\}^{N_w} = \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max\{1, |r|_w\}^{N_w} = \prod_{v \in M_K} \max\{1, |r|_v\}^{N_v[L:K]} = H_K(r)^{[L:K]}.$$

□

Definition 3.2.3. *The* absolute height *is the map $H : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 1}$, given by:*

$$H(r) = H_K(r)^{1/[K:\mathbb{Q}]},$$

where K is a finite extension of $\mathbb{Q}$ such that $r \in K$. The (logarithmic) height *is the map $h : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$, defined by $h(r) = \log H(r)$.*

Proposition 3.2.2 guarantees that $H(r)$ is well defined, i.e. it does not depend on the field K.

Definition 3.2.4. *Let $f = a_d \prod_{i=1}^{d}(X - r_i) \in \mathbb{C}[X]$. The* Mahler measure *of f is:*

$$M(f) = |a_d| \prod_{i=1}^{d} \max\{1, |r_i|\}.$$

The logarithmic Mahler measure *of f is $m(f) = \log M(f)$.*

The Mahler measure is multiplicative, i.e. if $f, g \in \mathbb{C}[X]$ then $M(fg) = M(f)M(g)$ and $m(fg) = m(f) + m(g)$.

Lemma 3.2.5. *Let $f = a_d X^d + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ be a primitive polynomial of degree d and let $p \in \mathbb{N}$ be a prime. Suppose that $r_1, \ldots, r_d \in \overline{\mathbb{Q}_p}$ are all the roots of f. Then:*

$$|a_d|_p \prod_{i=1}^{d} \max\{1, |r_i|_p\} = 1.$$

Proof. Suppose that $|r_1|_p \leq 1, \ldots, |r_k|_p \leq 1$ y $|r_{k+1}|_p > 1, \ldots, |r_d|_p > 1$. The coefficient a_k can be written as $a_k = a_d(r_1 \cdots r_{d-k} + \cdots + r_{k+1} \cdots r_d)$, where the sum ranges over all possible products of $d-k$ roots of f. Among all these terms, the product $r_{k+1} \cdots r_d$ has (strictly) maximal absolute value. Then, by Lemma 3.1.3 we have:

$$|a_k|_p = |a_d|_p \prod_{i=k+1}^{d} |r_i|_p = |a_d|_p \prod_{i=1}^{d} \max\{1, |r_i|_p\}.$$

On the other hand, every coefficient $a_j = a_d(r_1 \cdots r_{d-j} + \cdots + r_{j+1} \cdots r_d)$ has a similar formula, but all these terms have absolute value less or equal than $|r_{k+1} \cdots r_d|_p$. Therefore $|a_j|_p \leq |a_k|_p$ for every j, i.e. a_k is a coefficient with maximal absolute value. Since $f \in \mathbb{Z}[X]$ is primitive, we have $|a_j|_p \leq 1$ for every j, but we cannot have $|a_j|_p < 1$ for every j because p does not divides all the coefficients of f. Thus, there is at least one coefficient which absolute value equals exactly 1. Hence, the maximum of the absolute values of the coefficients of f is 1, and then $|a_k|_p = 1$. □

Proposition 3.2.6. *Let $r \in \overline{\mathbb{Q}}$, let $K = \mathbb{Q}[r]$ and let $f \in \mathbb{Z}[X]$ be the primitive minimal polynomial of r. Then $M(f) = H_K(r)$.*

Proof. Let $p \in \mathbb{N}$ be a prime number and let $r_1, \ldots, r_d \in \overline{\mathbb{Q}_p}$ be the roots of f. By Proposition 3.1.12, the sequence $|r_1|_p, \ldots, |r_d|_p$ contains $|r|_w$ for every absolute value w on K extending v_p with multiplicity N_w. By Lemma 3.2.5, we have:

$$\prod_{w|v_p} \max\{1, |r|_w\}^{N_w} = \prod_{i=1}^{d} \max\{1, |r_i|_p\} = |a_d|_p^{-1}. \tag{3.3}$$

On the other hand, for the Archimedean absolute values, we have:

$$\prod_{w|v_\infty} \max\{1, |r|_w\}^{N_w} = \prod_{i=1}^{d} \max\{1, |r_i|\}. \tag{3.4}$$

Multiplying (3.3) for all prime $p \in \mathbb{N}$ and (3.4), we conclude:

$$\begin{aligned} H_K(r) &= \prod_{w \in M_K} \max\{1, |r|_w\}^{N_w} = \prod_{v \in M_\mathbb{Q}} \prod_{w|v} \max\{1, |r|_w\}^{N_w} \\ &= \prod_{p} |a_d|_p^{-1} \prod_{i=1}^{d} \max\{1, |r_i|\} = |a_d| \prod_{i=1}^{d} \max\{1, |r_i|\} = M(f). \end{aligned}$$

□

For instance, if $r = a/b \in \mathbb{Q} - \{0\}$ where $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and $\gcd(a,b) = 1$, then the primitive minimal polynomial of r is $f = bX - a \in \mathbb{Z}[X]$. Therefore $H(r) = H_{\mathbb{Q}}(r) = M(f) = |b| \max\{1, |a/b|\} = \max\{|a|, |b|\}$.

Lemma 3.2.7. *Let $r, s \in \overline{\mathbb{Q}}$ and let $n \in \mathbb{Z}$. Then:*

1. $h(r^n) = |n| h(r)$.
2. $h(rs) \leq h(r) + h(s)$.
3. $h(r+s) \leq h(r) + h(s) + \log 2$.

Proof. Let $K = \mathbb{Q}[r,s]$.
(1) For every $x \geq 0$ and $n \in \mathbb{N}_0$, $\max\{1, x^n\} = \max\{1,x\}^n$ holds. If $n \in \mathbb{N}_0$, then:

$$H_K(r^n) = \prod_{v \in M_K} \max\{1, |r^n|_v\}^{N_v} = \prod_{v \in M_K} \max\{1, |r|_v^n\}^{N_v} = \prod_{v \in M_K} \max\{1, |r|_v\}^{nN_v} = H_K(r)^n.$$

On the other hand, if $r \neq 0$, then the relative height of r^{-1} is:

$$H_K(r^{-1}) = \prod_{v \in M_K} \max\{1, |r|_v^{-1}\}^{N_v} = \underbrace{\prod_{v \in M_K} |r^{-1}|_v^{N_v}}_{=1} \prod_{v \in M_K} \max\{1, |r|_v\}^{N_v} = H_K(r).$$

Using both identities we get $H_K(r^n) = H_K(r)^{|n|}$ for every $n \in \mathbb{Z}$.
(2) For every $x, y \geq 0$ we have $\max\{1, xy\} \leq \max\{1,x\}\max\{1,y\}$. Then:

$$H_K(rs) = \prod_{v \in M_K} \max\{1, |rs|_v\}^{N_v} \leq \prod_{v \in M_K} \max\{1, |r|_v\}^{N_v} \max\{1, |s|_v\}^{N_v} = H_K(r) H_K(s).$$

(3) For every $x, y \geq 0$ we have $\max\{1, x+y\} \leq 2\max\{1,x\}\max\{1,y\}$ and $\max\{1,x,y\} \leq \max\{1,x\}\max\{1,y\}$. Then:

$$\begin{aligned} H_K(r+s) &= \prod_{v \in M_K} \max\{1, |r+s|_v\}^{N_v} \leq \prod_{v \in M_K^\infty} \max\{1, |r|_v + |s|_v\}^{N_v} \prod_{v \notin M_K^\infty} \max\{1, |r|_v, |s|_v\}^{N_v} \leq \\ &\leq \prod_{v \in M_K^\infty} 2\max\{1, |r|_v\}^{N_v} \max\{1, |s|_v\}^{N_v} \prod_{v \notin M_K^\infty} \max\{1, |r|_v\}^{N_v} \max\{1, |s|_v\}^{N_v} \leq \\ &\leq 2^{|M_K^\infty|} H_K(r) H_K(s). \end{aligned}$$

We conclude by using that the number $|M_K^\infty|$ of Archimedean absolute values on K is bounded by the number $[K : \mathbb{Q}]$ of $\mathbb{Q}$-embeddings of K in $\mathbb{C}$. □

Theorem 3.2.8. [Jensen's Formula] *Let $f \in \mathbb{C}[X]$ be a non-zero polynomial. Then:*

$$m(f) = \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})| d\theta.$$

Proof. Due to the additivity of both sides of the formula, it is enough to prove it for polynomials $f = X - \alpha$ where $\alpha \in \mathbb{C}$, and up to a linear change of variables, this is equivalent to:

$$\int_0^1 \log|\alpha - e^{2\pi it}|dt = \max\{0, \log|\alpha|\}.$$

The map $\log|z|$ is harmonic in $\mathbb{C} - \{0\}$. Then $\log|z - \alpha|$ is harmonic in $\mathbb{C} - \{\alpha\}$. In particular, if $|\alpha| > 1$, then the map $\log|z - \alpha|$ is harmonic in the disc of radius 1 centered in the origin. Using the mean-value identity for harmonic maps, we get:

$$\log|\alpha| = \int_0^1 \log|\alpha - e^{2\pi it}|dt.$$

Now suppose that $|\alpha| < 1$. The map $\log|1 - \overline{\alpha}z|$ is harmonic in $\mathbb{C} - \{\beta\}$, where $\beta = 1/\overline{\alpha} = \alpha/|\alpha|^2$. Since $|\beta| > 1$, then this map is harmonic in the disc of radius 1 centered in the origin. On the other hand, for every $z \in \mathbb{C}$ such that $|z| = 1$ we have $|1 - \overline{\alpha}z| = |\alpha - z|$. Therefore, using again the mean-value identity, we get:

$$0 = \int_0^1 \log|1 - \overline{\alpha}e^{2\pi it}|dt = \int_0^1 \log|\alpha - e^{2\pi it}|dt.$$

It only remains to consider the case $|\alpha| = 1$. By rotational symmetry, we can further reduce to the case $\alpha = 1$, i.e. we have to prove that

$$\int_0^1 \log|1 - e^{2\pi it}|dt$$

converges and is equal to zero. Since $|1 - e^{2\pi it}| = 2\sin(\pi t)$ for every $0 \leq t \leq 1$, then we have to prove that

$$\int_0^1 \log\sin(\pi t)dt = -\log 2.$$

The convergence of the integral follows from

$$\int_0^1 \log\sin(\pi t)dt = 2\int_0^{1/2} \log\sin(\pi t)dt,$$

and the facts that $\sin(\pi t)$ behaves like πt for every t near zero and that $\int_0^{1/2} \log(\pi t)dt$ converges. To compute the value of the integral, note that:

$$\begin{aligned} I &= \int_0^{1/2} \log\sin(\pi t)dt \\ &= \int_0^{1/2} \log(2\sin(\pi t/2)\cos(\pi t/2))dt \\ &= \tfrac{1}{2}\log(2) + \int_0^{1/2} \log\sin(\pi t/2)dt + \int_0^{1/2} \log\cos(\pi t/2)dt. \end{aligned}$$

Making the changes of variables $t = 2u$ and $t = 1 - 2u$, we get $I = \frac{1}{2}\log(2) + 2I$. Therefore $I = -\frac{1}{2}\log(2)$. □

Proposition 3.2.9. *Let $f \in \mathbb{C}[X]$ be a non-zero polynomial of degree d. Then:*

$$2^{-d}\|f\|_1 \leq M(f) \leq \|f\|_1.$$

Proof. Let $f = \sum_{i=0}^{d} a_i X^i = a_d \prod_{i=1}^{d}(X - r_i)$. Then:

$$\|f\|_1 = \sum_{i=0}^{d} |a_i| \leq |a_d| \prod_{i=1}^{d}(1 + |r_i|) \leq 2^d |a_d| \prod_{i=1}^{d} \max\{1, |r_i|\} = 2^d M(f).$$

To prove the other inequality, we use Theorem 3.2.8 and the bound $|f(e^{2\pi i t})| \leq \|f\|_1$ and we get:

$$m(f) = \int_0^1 \log |f(e^{2\pi i t})| dt \leq \int_0^1 \log \|f\|_1 dt = \log \|f\|_1.$$

□

Theorem 3.2.10. [Kronecker] *Let $r \in \overline{\mathbb{Q}}^{\times}$ be such that $h(r) = 0$. Then $r \in \mu_\infty$.*

Proof. Let $f \in \mathbb{Z}[X]$ be the minimal primitive polynomial of r. By Proposition 3.2.6, we have that $M(f) = 1$. Let $r = r_1, r_2, \ldots, r_d \in \overline{\mathbb{Q}}$ be all the roots of f. Since $M(f) = 1$, then f is a monic polynomial and $|r_i| \leq 1 \; \forall i$. The polynomials $f_n = \prod_{i=1}^{d}(X - r_i^n)$ are all in $\mathbb{Z}[X]$ because the r_i's are algebraic integers and the coefficients of f_n are symmetric polynomials in $r_1, \ldots, r_d$. Since $M(f_n) \leq 1$ and $\deg(f_n) = d$, we have that $\|f_n\|_1 \leq 2^d$ for all $n \in \mathbb{N}$, by Proposition 3.2.9. Therefore, there are two polynomials $f_n = f_m$ with $n \neq m$. Then the sets $\{r_1^n, \ldots, r_d^n\}$ and $\{r_1^m, \ldots, r_d^m\}$ coincide. After a suitable permutation of the roots r_i's, we get a cycle $r_1^n = r_2^m$, $r_2^n = r_3^m$, …, $r_k^n = r_1^m$. This implies that $r_1^{n^k} = r_1^{m^k}$, and therefore $r = r_1$ is a root of the unity, because we are assuming $r \neq 0$. □

Theorem 3.2.11. *Let $r \in \overline{\mathbb{Q}}^{\times} \setminus \mu_\infty$ be an algebraic number of degree d over $\mathbb{Q}$, then*

$$h(r) \geq \frac{2}{d \, \log^3(3d)}.$$

Proof. See [Vou96, Corollary 2]. □

Now we extend the notion of height and Mahler measure to the multivariate setting.

Definition 3.2.12. *Let $\xi \in \overline{\mathbb{Q}}^t$. The* (logarithmic) height of ξ *is*

$$h(\xi) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} N_v \log \max\{1, \|\xi\|_v\},$$

where K is an (arbitrary) field containing ξ. We also define the (logarithmic) 1-height of ξ *as*

$$h_1(\xi) = \frac{1}{[K : \mathbb{Q}]} \left(\sum_{v \in M_K^\infty} N_v \log \max\{1, \|\xi\|_{1,v}\} + \sum_{v \notin M_K^\infty} N_v \log \max\{1, \|\xi\|_v\} \right).$$

We also define $H(\xi) = \exp h(\xi)$ *and* $H_1(\xi) = \exp h_1(\xi)$. *If* $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ *then we define* $h(f)$, $H(f)$, $h_1(f)$ *and* $H_1(f)$ *as the height and* 1*-height of the vector of coefficients of* f *respectively.*

Lemma 3.2.7 (items 2 and 3) extends to the multivariate setting with the same proofs. Item 1 only extends when $n \geq 0$ (also with the same proof). It cannot be extended for $n < 0$ because for $\xi \in (\overline{\mathbb{Q}}^\times)^t$, the heights $H(\xi)$ and $H(\xi^{-1})$ are not equal in general. For instance, if $\xi = (2, 3)$, then $H(\xi) = 3$ but $H(\xi^{-1}) = 6$.

Lemma 3.2.13. *Let* $\xi \in \overline{\mathbb{Q}}^t$. *Then* $h(\xi) \leq h_1(\xi) \leq h(\xi) + \log t$.

Proof. The first inequality is clear from the definition because $\|\xi\|_v \leq \|\xi\|_{1,v}$ for all $v \in M_K^\infty$. For the second inequality, we use the estimation $\|\xi\|_{1,v} \leq t \, \|\xi\|_v$, that implies $\max\{1, \|\xi\|_{1,v}\} \leq t \max\{1, \|\xi\|_v\}$ for all $v \in M_K^\infty$ and we get

$$h_1(\xi) \leq h(\xi) + \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K^\infty} N_v \log t.$$

We conclude by using that $\sum_{v \in M_K^\infty} N_v \leq \sum_{v \in M_K} N_v = [K : \mathbb{Q}]$. □

Lemma 3.2.14. *Let* $\xi \in \overline{\mathbb{Q}}^t$ *and* $\eta \in \overline{\mathbb{Q}}^u$. *Let us write* $(\xi, \eta) \in \overline{\mathbb{Q}}^{t+e}$ *to the concatenation of* ξ *and* η. *Then* $\max\{h(\xi), h(\eta)\} \leq h((\xi, \eta)) \leq h(\xi) + h(\eta)$.

Proof. Let $K/\mathbb{Q}$ be a finite extension containing both ξ and η. The first inequality follows directly from the definition and from the fact that $\|\xi\|_v$ and $\|\eta\|_v$ are both bounded above by $\|(\xi, \eta)\|_v$ for all $v \in M_K$. More precisely, we have that $\|(\xi, \eta)\|_v = \max\{\|\xi\|_v, \|\eta\|_v\}$, which implies $\max\{1, \|(\xi, \eta)\|_v\} \leq \max\{1, \|\xi\|_v\} \max\{1, \|\eta\|_v\}$ for all $v \in M_K$, and then $h((\xi, \eta)) \leq h(\xi) + h(\eta)$. □

Suppose that $\xi = (\xi_1, \ldots, \xi_t) \in (\overline{\mathbb{Q}}^\times)^t$. We have that $h(\xi_i^{-1}) = h(\xi_i)$ for all $1 \leq i \leq t$. By applying Lemma 3.2.14 we get the inequality

$$h(\xi^{-1}) \leq h(\xi_1^{-1}) + \cdots + h(\xi_t^{-1}) = h(\xi_1) + \cdots + h(\xi_t) \leq t \, h(\xi)$$

that controls the height of ξ^{-1} in terms of the height of ξ. This gives a generalization of item 1 of Lemma 3.2.7 (with $n < 0$) for the multivariate case.

Lemma 3.2.15. *Let* $f \in \overline{\mathbb{Q}}[X]$ *be an univariate polynomial and let* $r \in \overline{\mathbb{Q}}$ *be a root of* f. *Then* $h(r) \leq h_1(f)$.

Proof. Suppose that $f = \sum_{i=0}^d a_i X^i$ with $a_d \neq 0$. Let $K = \mathbb{Q}[a_0, \ldots, a_d, r]$. Let $v \in M_K$. If v is Archimedean, i.e. $v \in M_K^\infty$, we have

$$|a_d|_v |r|_v^d = |a_{d-1} r^{d-1} + \cdots + a_0|_v \leq (|a_{d-1}|_v + \cdots + |a_0|_v) \max\{1, |r|_v\}^{d-1}.$$

This implies that

$$|a_d|_v \max\{1,|r|_v\}^d \leq (|a_d|_v + \cdots + |a_0|_v)\max\{1,|r|_v\}^{d-1} = \|f\|_{1,v}\max\{1,|r|_v\}^{d-1}$$

$$|a_d|_v \max\{1,|r|_v\} \leq \|f\|_{1,v} \leq \max\{1,\|f\|_{1,v}\}. \tag{3.5}$$

On the other hand, if v is non-Archimedean, we have

$$|a_d|_v|r|_v^d = |a_{d-1}r^{d-1} + \cdots + a_0|_v \leq \max\{|a_{d-1}|_v,\ldots,|a_0|_v\}\max\{1,|r|_v\}^{d-1}.$$

This implies that

$$|a_d|_v \max\{1,|r|_v\}^d \leq \max\{|a_d|_v,\ldots,|a_0|_v\}\max\{1,|r|_v\}^{d-1} = \|f\|_v\max\{1,|r|_v\}^{d-1}$$

$$|a_d|_v \max\{1,|r|_v\} \leq \|f\|_v \leq \max\{1,\|f\|_v\}. \tag{3.6}$$

Raising equations 3.5 and 3.6 to the $N_v/[K:\mathbb{Q}]$ and multiplying over all $v \in M_K$, we get $H(r) \leq H_1(f)$ as desired. The terms $|a_d|_v$ cancel out when multiplying because of the product formula 3.2. □

Lemma 3.2.16. *Let $f \in \overline{\mathbb{Q}}[X_1,\ldots,X_n]$ and let $\xi \in \overline{\mathbb{Q}}^n$. Then*

$$h(f(\xi)) \leq h_1(f) + \deg(f)h(\xi).$$

Proof. Suppose that $f = \sum_{|\alpha|\leq d} a_\alpha X^\alpha$ where $d = \deg(f)$. Let $K = \mathbb{Q}[a_\alpha,\xi]$ be the extension of $\mathbb{Q}$ generated by the coefficients of f and the coordinates of ξ. Let $v \in M_K$. If v is Archimedean,

$$|f(\xi)|_v \leq \sum_{|\alpha|\leq d} |a_\alpha|_v|\xi_1|_v^{\alpha_1}\cdots|\xi_n|_v^{\alpha_n} \leq \left(\sum_{|\alpha|\leq d}|a_\alpha|_v\right)\max\{|\xi_1|_v,\ldots,|\xi_n|_n\}^d = \|f\|_{1,v}\|\xi\|_v^d,$$

and then $\max\{1,|f(\xi)|_v\} \leq \max\{1,\|f\|_{1,v}\}\max\{1,\|\xi\|_v\}^d$. Similarly, if v is non-Archimedean, the ultrametric inequality gives $\max\{1,|f(\xi)|_v\} \leq \max\{1,\|f\|_v\}\max\{1,\|\xi\|_v\}^d$. Raising these inequalities to the $N_v/[K:\mathbb{Q}]$ and multiplying over all $v \in M_K$, we obtain $H(f(\xi)) \leq H_1(f)H(\xi)^d$. □

Definition 3.2.17. *Let $f \in \mathbb{C}[X_1,\ldots,X_n]$. The* (logarithmic) Mahler measure of f *is*

$$m(f) = \frac{1}{(2\pi)^n}\int_0^{2\pi}\cdots\int_0^{2\pi}\log|f(e^{it_1},\ldots,e^{it_n})|dt_1\cdots dt_n.$$

We also define $M(f) = \exp m(f)$.

As in the univariate case, the Mahler measure is multiplicative, i.e. $M(fg) = M(f)M(g)$ and $m(fg) = m(f) + m(g)$ for all $f,g \in \mathbb{C}[X_1,\ldots,X_n]$. Moreover, the inequality $M(f) \leq \|f\|_1$ of Proposition 3.2.9 also holds in the multivariate case with the same proof.

Definition 3.2.18. *Let $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$. The* global Mahler measure of f *is*

$$m_{\overline{\mathbb{Q}}}(f) = \frac{1}{[K : \mathbb{Q}]} \left(\sum_{v|v_\infty} N_v m_v(f) + \sum_{v \nmid v_\infty} N_v \log \max |\mathrm{coeff}(f)|_v \right),$$

where K is a number field containing all the coefficients of f and $m_v(f) = m(\sigma(f))$ for the corresponding embedding $\sigma : K \to \mathbb{C}$.

If $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is a primitive polynomial then $m_{\overline{\mathbb{Q}}}(f) = m(f)$. The global Mahler measure is also multiplicative, i.e. $m_{\overline{\mathbb{Q}}}(fg) = m_{\overline{\mathbb{Q}}}(f) + m_{\overline{\mathbb{Q}}}(g)$ for all $f, g \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$. We also have the inequality $m_{\overline{\mathbb{Q}}}(f) \leq h_1(f)$ for all $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$.

Definition 3.2.19. *Let V be a hypersurface of $\overline{\mathbb{Q}}^n$ given by $f \in K[X_1, \ldots, X_n]$, where $K/\mathbb{Q}$ is a finite extension. The* normalized height of V *is $\widehat{h}(V) = m_{\overline{\mathbb{Q}}}(f)$.*

In the case of a hypersurface V given by a primitive polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$, then the normalized height reduces to $\widehat{h}(V) = m(f)$.

Bibliography

[Ave07] M. Avendaño, *The number of roots of a bivariate polynomial on a line.* MEGA'07, Effective Methods in Algebraic Geometry Digital Proceedings (2007).

[AKP06] M. Avendaño, T. Krick, A. Pacetti, *Newton-Hensel interpolation lifting.* Found. Comp. Math. **6(1)** Special Vol. dedicated to Steve Smale on his 75th birthday (2006), 81–120.

[AKS07] M. Avendaño, T. Krick, M. Sombra, *Factoring bivariate sparse (lacunary) polynomials.* Journal of Complexity **23** (2007), 193–216.

[AD00] F. Amoroso, S. David, *Minoration de la hauteur normalisée des hypersurfaces.* Acta Arith. **92** (2000), 339–366.

[BBS07] D.J. Bates, F. Bihan, F. Sottile, *Bounds on the number of real solutions to polynomial equations.* IMRN, to appear.

[BeTi88] M. Ben-Or, P. Tiwari, *A deterministic algorithm for sparse multivariate polynomial interpolation. Extended abstract.* STOC (1988) 301–309.

[Ber70] E.R. Berlekamp, *Factoring polynomials over large finite fields.* Math. Comp. **24** (1970), 713–735.

[BHKS05] K. Belabas, M. van Hoeij, J. Klüners, A. Steel, *Factoring polynomials over global fields.* Preprint (2005).

[BiSo06] F. Bihan, F. Sottile, *New fewnomial upper bounds from Gale dual polynomial systems.* Moscow Mathematics Journal **7(3)** (2007), 387–407.

[BoTi91] A. Borodin, P. Tiwari, *On the decidability of sparse univariate polynomial interpolation.* Comput. Complexity **1** (1991) 67–90. STOC (1988), 301–309.

[Chi84] A. Chistov, *Factoring polynomials over a finite field and solution of systems of algebraic equations.* (Russian. English summary.) Theory of the complexity of computations, II. Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984) 124–188.

[ChGr82] A. Chistov, D. Grigoriev, *Polynomial time factoring of the multivariate polynomials over a global field.* Preprint LOMI E-5-82 (1982) 39 p.

[CDGK91] M. Clausen, A. Dress, J. Grabmeier, M. Karpinski, *On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields.* Theoretical Computer Science **84** (1991), 151–164.

[CKS99] F. Cucker, P. Koiran, S. Smale, *A polynomial time algorithm for Diophantine equations in one variable.* J. Symbolic Comput. **27** (1999), 21–29.

[Dob79] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial.* Acta Arith. **34** (1979), 391–401.

[DrGr91] A. Dress, J. Grabmeier, *The interpolation problem for k-sparse polynomials and character sums.* Adv. in Appl. Math. **12** (1991), 57–75.

[GaKa85] J. von Zur Gathen, E. Kaltofen, *Factoring sparse multivariate polynomials.* Journal of Computer and System Sciences **31(2)** (1985), 265–287

[Gri84] D. Grigoriev, *Factoring polynomials over a finite field and solution of systems of algebraic equations.* (Russian. English summary.) Theory of the complexity of computations, II. Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984) 20–79.

[GKS90] D. Grigoriev, M. Karpinski, M. Singer, *Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields.* Siam J. Comput. Vol. **19(6)** (1990), 1059–1063.

[GKS91] D. Grigoriev, M. Karpinski, M. Singer, *The interpolation problem for k-sparse sums of eigenfunctions of operators.* Adv. in Appl. Math. **12** (1991), 76–81.

[GKS94] D. Grigoriev, M. Karpinski, M. Singer, *Computational complexity of sparse rational function interpolation.* SIAM J. Comput. **23** (1995), 1–11.

[Haas02] B. Haas, *A simple counter-example to Koushnirenko's conjecture.* Beiträge zur Algebra und Geometrie **43(1)** (2002), 1–8.

[vHoeij02] M. van Hoeij, *Factoring polynomials and the knapsack problem.* Journal of Number Theory **95** (2002), 167–189.

[Kal85] E. Kaltofen, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization.* SIAM J. Comput. **14** (1985), 469–489.

[KK05] E. Kaltofen, P. Koiran, *On the complexity of factoring bivariate supersparse (lacunary) polynomials.* ISSAC'05, Proc. 2005 Internat. Symp. Symbolic Algebraic Comput. (2005), 208–215.

[KK06] E. Kaltofen, P. Koiran, *Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields.* ISSAC'06, Proc. 2006 Internat. Symp. Symbolic Algebraic Comput. (2006), 162–168.

[KaLa88] E. Kaltofen, Y.N. Lakshman *Improved sparse multivariate polynomial interpolation algorithms.* ISSAC'88, Proc. 1988 Internat. Symp. Symbolic Algebraic Comput., Lecture Notes in Comput. Sci **358**, Springer-Verlag, New York (1988), 467–474.

[KLW90] E. Kaltofen, Y.N. Lakshman, J.-M. Wiley, *Modular rational sparse multivariate polynomial interpolation.* ISSAC'90, Proc. 1990 Internat. Symp. Symbolic Algebraic Comput. (S. Watanabe and M. Nagata, eds.), ACM Press, New York (1990), 135–139.

[KaLe03] E. Kaltofen, W.-s Lee, *Early termination in sparse interpolation algorithms.* J. Symbolic Computation **36(3-4)** (2003), 365–400.

[KLL00] E. Kaltofen, A. Lobo, W.-s Lee, *Early termination in Ben-Or/Tiwari sparse interpolation and a hybrid of Zippel's algorithm.* ISSAC'00, Proc. 2000 Internat. Symp. Symbolic Algebraic Comput. (C. Travero, ed.), ACM Press, New York (2000), 192–201.

[Kho91] A. Khovanskii, *Fewnomials.* AMS press, Providence, Rhode Island (1991).

[Lan85] S. Landau, *Factoring polynomials over algebraic number fields.* SIAM J. Comput. **14** (1985), 184–195.

[Lan93] S. Lang, *Algebra.* Addison Wesley (1993).

[Lec05] G. Lecerf, *Improved dense multivariate polynomial factorization algorithms.* To appear in J. Symb. Comput.

[Lee01] W.-s. Lee, *Early Termination Strategies in Sparse Interpolation Algorithms.* Ph.D. Dissertation, North Carolina State University (2001).

[Len84] A.K. Lenstra, *Factoring multivariate integral polynomials.* Theoret. Comput. Sci. **34** (1984), 207–213.

[Len87] A.K. Lenstra, *Factoring multivariate polynomials over algebraic number fields.* SIAM J. Comput. **16** (1987), 591–598.

[Len99a] H.W. Lenstra Jr., *On the factorization of lacunary polynomials.* Number theory in progress **1** (1999), 277–291.

[Len99b] H.W. Lenstra Jr., *Finding small degree factors of lacunary polynomials.* Number theory in progress **1** (1999), 267–276.

[LLL82] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, *Factoring polynomials with rational coefficients.* Math. Ann. **261** (1982), 515–534.

[LRW03] T.Y. Li, J.M. Rojas, X. Wang, *Counting real connected components of trinomial curves intersections and m-nomial hypersurfaces.* Discrete and computational geometry **30(3)** (2003), 379–414.

[Per05] D. Perruci, *Some bounds for the number of connected components of real zero sets of sparse polynomials.* Discrete and computational geometry **34(3)** (2005), 475–495.

[Pon05] M. Corentin Pontreau, *Minoration de la hauteur normalisée en petite codimension.* Université de Caen, Doctoral Thesis (2005).

[Vou96] P. Voutier, *An effective lower bound for the height of algebraic numbers.* Acta Arith. **74** (1996), 81–95.

[Zas69] H.Zassenhaus, *On Hensel Factorization I.* J. Number Theory **1** (1969), 291–311.

[Zha95a] S. Zhang, *Positive line bundles on arithmetic varieties.* J. Amer. Math. Soc. **8** (1995), 187–221.

[Zha95b] S. Zhang, *Small points and adelic metrics.* J. Algebraic Geom. **4** (1995), 281–300.

[Zip90] R. Zippel, *Interpolating polynomials from their values.* J. Symbolic Computation **9** (1990), 375–403.