

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/36589> holds various files of this Leiden University dissertation.

Author: Zhuang, Weidong

Title: Symmetric diophantine approximation over function fields

Issue Date: 2015-12-03

Chapter 1

Preliminaries

In this chapter we collect some results related to discriminants, resultants, valuations, heights and twisted heights.

Unless otherwise stated, throughout this dissertation, k will be an algebraically closed field of characteristic 0 and $K = k(t)$ the rational function field in the variable t . By a function field, we always mean a finite extension of K .

1.1 Discriminants and resultants

Let L be an arbitrary field. Let

$$F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in L[X, Y]$$

be a binary form of degree $n \geq 2$.

We have a factorization $F(X, Y) = \prod_{i=1}^n (\alpha_i X + \beta_i Y)$ over an algebraic closure \bar{L} of L . As usual, we define the discriminant of F to be

$$D(F) := \prod_{i < j} (\alpha_i \beta_j - \alpha_j \beta_i)^2.$$

This is a homogeneous polynomial of degree $2n - 2$ in $\mathbb{Z}[a_0, \dots, a_n]$. In particular, for a linear form, we define its discriminant to be 1.

$$R(G, F) = (-1)^{mn} R(F, G),$$

$$R(F, G + HF) = R(F, G),$$

where $\lambda, \mu \in L$, F, G, F_1, F_2 are binary forms and H is a binary form of degree $n - m$ if $n \geq m$.

For an invertible matrix $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, define

$$F_U(X, Y) := F(aX + bY, cX + dY).$$

Then $R(F_U, G_U) = (\det U)^{mn} R(F, G)$.

1.2 Valuations on function fields

Recall $K = k(t)$. Denote by M_K the collection of normalized discrete valuations on K that are trivial on k . This set is described as follows. For $f \in k[t] \setminus \{0\}$, define $\nu_p(f)$ ($p \in k \cup \{\infty\}$) by $f = (t - p)^{\nu_p(f)} g$ where $g \in k[t]$ and $g(p) \neq 0$ if $p \in k$; further, define $\nu_\infty(f) = -\deg f$. We extend this to $k(t)$ by setting $\nu_p(0) := \infty$ and $\nu_p(\frac{f}{g}) = \nu_p(f) - \nu_p(g)$ for $f, g \in k[t], g \neq 0$. Then $M_K = \{\nu_p : p \in k \cup \{\infty\}\}$. In this thesis we often work with absolute values. We define the absolute value $|\cdot|_\nu$ by $e^{-\nu(\cdot)}$ for $\nu \in M_K$. These absolute values satisfy the product formula

$$\prod_{\nu \in M_K} |x|_\nu = 1$$

for every $x \in K^*$. All valuations of K are non-archimedean, so for a binary form $F \in K[X, Y]$ we have

$$|D(F)|_\nu \leq \max_{0 \leq j \leq n} (|a_j|_\nu^{2n-2}) \quad (1.2.1)$$

for every $\nu \in M_K$. Let S be a finite set of valuations of K , containing the 'infinite valuation' ν_∞ . Define the ring of S -integers and group of S -units by

$$\begin{aligned} \mathcal{O}_S &= \{x \in K : |x|_\nu \leq 1 \text{ for } \nu \notin S\}, \\ \mathcal{O}_S^\times &= \{x \in K : |x|_\nu = 1 \text{ for } \nu \notin S\}. \end{aligned}$$

We define the S -norm of $x \in K$ by

$$|x|_S = \prod_{\nu \in S} |x|_\nu.$$

It is clear that $|x|_S \geq 1$ for $x \in \mathcal{O}_S \setminus \{0\}$ and $|x|_S = 1$ for $x \in \mathcal{O}_S^\times$.

Remark 1.2.1. *Let K be a purely transcendental extension of k of transcendence degree 1. Choose t such that $K = k(t)$. The 'infinite valuation' ν_∞ is the one with $\nu_\infty(t) < 0$. The choice of the infinite valuation depends on the choice of a transcendental element t generating K . In what follows, we make a distinction between the infinite valuation ν_∞ and the other valuations on K . But we should mention that in our arguments we could as well have chosen any other valuation to play the role of the infinite valuation.*

Recall that k is an algebraically closed field of characteristic 0, and $K = k(t)$. Let L be a finite extension of K . We say a valuation ω is normalized if $\omega(L^*) = \mathbb{Z}$. Denote by M_L the normalized valuations on L that are trivial on k . For valuations $\nu \in M_K$, $\omega \in M_L$, we say that ω lies above ν , and denote it by $\omega|\nu$, if the restriction of ω to K is a positive multiple of ν . Then for every $\nu \in M_K$, we have finitely many valuations $\omega \in M_L$ above ν . For every $\omega \in M_L$, we define the corresponding absolute value $|x|_\omega := e^{-\omega(x)}$. Then we have $\omega(x) = e(\omega|\nu)\nu(x)$ for $\omega|\nu, x \in K$, where $e(\omega|\nu)$ is called the ramification index. Let L_ω denote the completion of L at ω . In our case, k is algebraically closed with $\text{char } k = 0$ and the residue field of ν is k , hence the residue degree is 1, implying that $e(\omega|\nu) = [L_\omega : K_\nu]$. Thus our chosen absolute value is a prolongation of $|\cdot|_\nu^{[L_\omega : K_\nu]}$, rather than $|\cdot|_\nu$, to L , hence by Proposition 1.2.7 of [4], we have the relation $|x|_\omega = |N_{L_\omega/K_\nu}(x)|_\nu$ for every $x \in L$. By assumption, K has characteristic 0, so the extension L/K is separable. Hence

$$N_{L/K}(x) = \prod_{\omega|\nu} N_{L_\omega/K_\nu}(x) \text{ for } x \in L,$$

so we have

$$\prod_{\omega|\nu} |x|_{\omega} = |N_{L/K}(x)|_{\nu} \text{ for } x \in L, \nu \in M_K$$

and

$$\prod_{\omega \in M_L} |x|_{\omega} = 1 \text{ for } x \in L^*.$$

Similarly, we define the T -norm of $x \in L$ by

$$|x|_T = \prod_{\omega \in L} |x|_{\omega}.$$

We recall some facts about Dedekind domains. For a non-zero fractional ideal \mathfrak{a} of a Dedekind domain A and a prime ideal \wp of A , we denote by $v_{\wp}(\mathfrak{a})$ the exponent of \wp in the prime ideal factorization of \mathfrak{a} .

Lemma 1.2.2. *There is a bijection between the non-zero prime ideals of A and the discrete valuations of F that are non-negative on A , given by $\mathfrak{p} \mapsto \nu_{\mathfrak{p}}$ such that $\nu_{\mathfrak{p}}(a)$ is the exponent of \mathfrak{p} in the unique prime ideal factorization of the ideal generated by a .*

Proof. See [1]. □

Lemma 1.2.3. *Let A be a Dedekind domain with fraction field K_1 . Let L be a finite separable extension of K_1 , and B the integral closure of A in L . Assume that L/K_1 is tamely ramified. Denote by $D_{B/A}$ the discriminant ideal and $\mathfrak{D}_{B/A}$ the different ideal of B over A . Let \mathfrak{p} be a prime ideal of A , let \wp_1, \dots, \wp_r be the prime ideals of B above \mathfrak{p} , and ν the valuation corresponding to \mathfrak{p} , and ω_i corresponding to \wp_i for $i = 1, \dots, r$. Then*

$$N_{L/K_1}(\mathfrak{D}_{B/A}) = D_{B/A}.$$

Further

$$\nu(D_{B/A}) = \sum_{i=1}^r (e(\omega_i|\nu) - 1).$$

Proof. For the first part, see Proposition 6, §3, Chapter III of [22].

Since the extension L/K_1 is tamely ramified with residue degree $f(\omega_i|\nu) = 1$, we get by Proposition 13, §6, Chapter III of [22],

$$\omega_i(\mathfrak{D}_{B/A}) = e(\omega_i|\nu) - 1 \text{ for } i = 1, \dots, r,$$

hence

$$\nu(D_{B/A}) = \nu\left(N_{L/K_1}(\mathfrak{D}_{B/A})\right) = \sum_{i=1}^r \left(e(\omega_i|\nu) - 1\right),$$

which gives the claim. \square

Later we will apply this lemma frequently to the case $K_1 = k(t)$, $A = k[t]$ and $K_1 = K_\nu$, the completion of K at ν and $A = R_\nu := \{x \in K_\nu : \nu(x) \geq 0\}$ for $\nu \in M_K$.

1.3 Polynomials and heights

Recall $K = k(t)$. For $\nu \in M_K$, denote by K_ν the completion of K at the valuation ν . Then ν has a unique extension to K_ν . Define

$$R_\nu = \{x \in K_\nu : \nu(x) \geq 0\}$$

to be the local ring of K_ν . Then its group of units is

$$R_\nu^\times = \{x \in K_\nu : \nu(x) = 0\}.$$

For $\mathbf{x} = (x_1, x_2, \dots, x_n) \in K_\nu^n$, define

$$\begin{aligned} \nu(\mathbf{x}) &= \min_{1 \leq i \leq n} \nu(x_i), \\ \|\mathbf{x}\|_\nu &= e^{-\nu(\mathbf{x})} = \max_{1 \leq i \leq n} |x_i|_\nu, \end{aligned}$$

and for $\mathbf{x} \in K^n$, define the homogeneous height and S -height

$$H_K(\mathbf{x}) = \prod_{\nu \in M_K} \|\mathbf{x}\|_\nu,$$

$$H_S(\mathbf{x}) = \prod_{\nu \in S} \|\mathbf{x}\|_{\nu}.$$

Clearly, the product is well-defined and $H_K(\mathbf{x}) \geq 1$ for every $\mathbf{x} \neq \mathbf{0}$ because of the product formula. Also, $H_K(\lambda\mathbf{x}) = H_K(\mathbf{x})$.

For a polynomial $P \in K[X_1, \dots, X_n]$ or $P \in K_{\nu}[X_1, \dots, X_n]$ we define $|P|_{\nu}$ to be the maximum of the $|\cdot|_{\nu}$ -values of its coefficients.

Lemma 1.3.1 (Gauss' lemma). *Let K be a field, $|\cdot|_{\nu}$ a non-archimedean absolute value on K , and $P = \prod_{i=1}^t P_i$ with $P_i \in K[X_1, \dots, X_n]$ for $i = 1, \dots, t$. Then*

$$|P|_{\nu} = \prod_{i=1}^t |P_i|_{\nu}.$$

Proof. See [14]. □

As a direct consequence, we have

Corollary 1.3.2. *Let $F = \prod_{i=1}^n (\alpha_i X + \beta_i Y)$ with $\alpha_i, \beta_i \in K$ for $i = 1, \dots, n$. Then $|F|_{\nu} = \prod_{i=1}^n \max(|\alpha_i|_{\nu}, |\beta_i|_{\nu})$ for every $\nu \in M_K$.*

For L a finite extension of K and a polynomial $P \in L[X_1, \dots, X_m]$, we define

$$N_{L/K}(P) = \prod_{i=1}^{[L:K]} \sigma_i(P),$$

where $\sigma_1, \dots, \sigma_{[L:K]}$ are the K -embeddings of L into \overline{K} , and $\sigma_i(P)$ is obtained by the action of σ_i on the coefficients of P .

1.4 Galois theory of valuations

In this section, we give a brief sketch of some aspects of Galois theory of valuations that will be needed later.

Lemma 1.4.1. *Let K be a field with a non-trivial absolute value $|\cdot|_\nu$, and L a finite Galois extension of K with Galois group $G = \text{Gal}(L/K)$. Then for every two absolute values $|\cdot|_\omega, |\cdot|_{\omega'}$ on L prolonging $|\cdot|_\nu$, there is $\sigma \in G$ such that $|x|_\omega = |\sigma(x)|_{\omega'}$ for $x \in L$.*

Proof. See Corollary 1.3.5 of [4]. \square

For $\nu \in M_K$ and L a Galois extension of K , denote by $\mathcal{A}(\nu)$ the set of normalized valuations of L above ν . Fix $\omega_1 \in \mathcal{A}(\nu)$. The completion L_{ω_1} of L at ω_1 is a Galois extension of K_ν . We may view L as a subfield of L_{ω_1} . As mentioned before, the absolute values on L defined above satisfy the relation $|x|_{\omega_1} = |N_{L_{\omega_1}/K_\nu}(x)|_\nu$ for $x \in L_{\omega_1}$. Without loss of generality, we may assume $K \subset K_\nu \subset L_{\omega_1} \subset \overline{K_\nu}$ and $K \subset L \subset L_{\omega_1} \subset \overline{K_\nu}$. Let $\mathcal{E}(\omega_1|\nu)$ be the set $\{\sigma \in G : \omega_1 \circ \sigma = \omega_1\}$ equipped with composition. This is by definition the decomposition group of ω_1 over ν . By, for instance, §9, Chapter II of [18], we have an isomorphism

$$\begin{aligned} \text{Gal}(L_{\omega_1}/K_\nu) &\xrightarrow{\sim} \mathcal{E}(\omega_1|\nu), \\ \sigma &\longmapsto \sigma|_L. \end{aligned}$$

Thus we may view $\text{Gal}(L_{\omega_1}/K_\nu)$ as a subgroup of G . Further, let

$$\mathcal{E}(\omega|\nu) = \{\sigma \in G : \omega = \omega_1 \circ \sigma\} \text{ for } \omega \in \mathcal{A}(\nu). \quad (1.4.1)$$

Since G acts transitively on $\mathcal{A}(\nu)$ (see §9, Chapter II, [18]), the sets $\mathcal{E}(\omega|\nu)$ form a partition of G , and in fact they are the right cosets of $\text{Gal}(L_{\omega_1}/K_\nu)$ in G , so have the same cardinality:

$$[L_\omega : K_\nu] = [L_{\omega'} : K_\nu] \text{ for } \omega, \omega' \text{ above } \nu. \quad (1.4.2)$$

It is now reasonable to put $g_\nu := \#\mathcal{E}(\omega|\nu) = [L_{\omega_1} : K_\nu]$. If we still denote by $|\cdot|_\nu$ the prolongation of $|\cdot|_\nu$ from K to $\overline{K_\nu}$, and hence on L_{ω_1} , then $|x|_\nu = |N_{L_{\omega_1}/K_\nu}(x)|_\nu^{1/[L_{\omega_1}:K_\nu]}$ for $x \in L_{\omega_1}$. It follows that for $x \in L, \omega \in \mathcal{A}(\nu), \sigma \in \mathcal{E}(\omega|\nu)$, we have

$$|x|_\omega = |\sigma(x)|_{\omega_1} = |\sigma(x)|_\nu^{g_\nu}. \quad (1.4.3)$$

Notice that $\sigma \in \text{Gal}(L/K)$, hence we may extend $\sigma \in \mathcal{E}(\omega|\nu)$ to a K_ν -isomorphism from L_ω to L_{ω_1} , by sending $\alpha = \lim_{n \rightarrow \infty} \alpha_n$ to $\sigma(\alpha) = \lim_{n \rightarrow \infty} \sigma(\alpha_n)$ where $\alpha \in L_\omega$ and $\alpha_n \in L$. Moreover, for every $x \in L_\omega$, we also have $|x|_\omega = |\sigma(x)|_{\omega_1} = |\sigma(x)|_\nu^{g_\nu}$.

1.5 Twisted heights

Let S be a finite set of valuations of K . We define the ring of S -adeles

$$\mathbb{A}_S := \prod_{\nu \in S} K_\nu = \{(x_\nu) | x_\nu \in K_\nu \text{ for every } \nu \in S\}$$

with componentwise addition and multiplication.

Further, let

$$\text{GL}_n(\mathbb{A}_S) = \{(A_\nu) | A_\nu \in \text{GL}_n(K_\nu) \text{ for every } \nu \in S\},$$

where $\text{GL}_n(R_\nu)$ is the subgroup of $\text{GL}_n(K_\nu)$ of $n \times n$ matrices whose entries are in R_ν and whose determinant is in R_ν^\times .

For $A = (A_\nu) \in \text{GL}_n(\mathbb{A}_S)$, define

$$|\det(A)|_S := \prod_{\nu \in S} |\det(A_\nu)|_\nu.$$

Also, we define the ν -norm of A_ν as follows: if $A_\nu = (a_{ij})_{1 \leq i, j \leq n}$, then $\|A_\nu\|_\nu = \max_{i, j} |a_{ij}|_\nu$. Given a ring R we denote by R^n the module of n -dimensional column vectors with entries in R .

Lemma 1.5.1. *Let $\nu \in M_K$. For $A_\nu \in \text{GL}_n(R_\nu)$ and $\mathbf{x} \in K_\nu^n$, we have $\nu(A_\nu \mathbf{x}) = \nu(\mathbf{x})$.*

Proof. Let $A_\nu = (a_{ij})$, $\mathbf{x} = (x_1, \dots, x_n) \in K_\nu^n$.

As $\min_{i,j} \nu(a_{ij}) \geq 0$, we have

$$\begin{aligned} \nu(A_\nu \mathbf{x}) &\geq \min_{1 \leq i \leq n} \nu(a_{i1}x_1 + \cdots + a_{in}x_n) \\ &\geq \min_{1 \leq i,j \leq n} \nu(a_{ij}x_j) \\ &\geq \min_{1 \leq j \leq n} \nu(x_j) + \min_{i,j} \nu(a_{ij}) \\ &\geq \nu(\mathbf{x}). \end{aligned}$$

Since $A_\nu^{-1} \in \mathrm{GL}_n(R_\nu)$, we have similarly for $A_\nu \in \mathrm{GL}_n(R_\nu)$, $\mathbf{x} \in K^n$ that $\nu(\mathbf{x}) = \nu(A_\nu^{-1}A_\nu \mathbf{x}) \geq \nu(A_\nu \mathbf{x})$. This completes the proof. \square

For $A \in \mathrm{GL}_n(\mathbb{A}_S)$, $\mathbf{x} \in K^n$ define the divisor

$$\mathrm{div}_A(\mathbf{x}) := \sum_{\nu \in S} \nu(A_\nu \mathbf{x}) + \sum_{\nu \notin S} \nu(\mathbf{x})$$

and its degree

$$\mathrm{deg}(\mathrm{div}_A(\mathbf{x})) = \sum_{\nu \in S} \nu(A_\nu \mathbf{x}) + \sum_{\nu \notin S} \nu(\mathbf{x}).$$

Also define the corresponding twisted additive height

$$h_A(\mathbf{x}) := -\mathrm{deg}(\mathrm{div}_A(\mathbf{x})) = -\sum_{\nu \in S} \nu(A_\nu \mathbf{x}) - \sum_{\nu \notin S} \nu(\mathbf{x}).$$

The sum is well-defined by the fact that for every $\mathbf{x} \in K^*$, we have $\nu(\mathbf{x}) = 0$ for almost all $\nu \in M_K$. Define the twisted multiplicative height for $\mathbf{x} \in K^n$ by:

$$H_A(\mathbf{x}) := \exp(h_A(\mathbf{x})) = \prod_{\nu \in S} \|A_\nu \mathbf{x}\|_\nu \prod_{\nu \notin S} \|\mathbf{x}\|_\nu.$$

It is projective in the sense that, by the product formula, $H_A(\lambda \mathbf{x}) = H_A(\mathbf{x})$ for $\mathbf{x} \in K^n$, $\lambda \in K^\times$.

Lastly, we define for $A \in \mathrm{GL}_n(\mathbb{A}_S)$

$$\mathrm{div}(A) := \mathrm{div}_A(K^n) := \sum_{\nu \in S} \nu(\det(A_\nu)),$$

and

$$\begin{aligned} h_A(K^n) &:= -\mathrm{deg}(\mathrm{div}(A)), \\ H_A(K^n) &:= \exp(h_A(K^n)) = \prod_{\nu \in S} |\det A_\nu|_\nu = |\det(A)|. \end{aligned}$$

Lemma 1.5.2. *Let $A \in GL_n(\mathbb{A}_S)$. Then there exist positive constants c_1, c_2 depending on A such that $c_2 H_K(\mathbf{x}) \leq H_A(\mathbf{x}) \leq c_1 H_K(\mathbf{x})$ for all $\mathbf{x} \in K^n$. In particular, for $\mathbf{x} \neq \mathbf{0}$, we have $H_A(\mathbf{x}) \geq c_2$.*

Proof. Let $c_1 = \prod_{\nu \in S} \|A_\nu\|_\nu$ and $c_2 = \prod_{\nu \in S} \|A_\nu^{-1}\|_\nu^{-1}$.

Clearly, we have $\|A_\nu \mathbf{x}\|_\nu \leq \|A_\nu\|_\nu \|\mathbf{x}\|_\nu$ because for all $\nu \in S$, the valuation is non-archimedean. Similarly we have $\|\mathbf{x}\|_\nu = \|A_\nu^{-1} A_\nu \mathbf{x}\|_\nu \leq \|A_\nu^{-1}\|_\nu \|A_\nu \mathbf{x}\|_\nu$, hence $\|A_\nu^{-1}\|_\nu^{-1} \|\mathbf{x}\|_\nu \leq \|A_\nu \mathbf{x}\|_\nu \leq \|A_\nu\|_\nu \|\mathbf{x}\|_\nu$ for $\nu \in S$. By taking the product over all $\nu \in M_K$ we get $c_2 H_K(\mathbf{x}) \leq H_A(\mathbf{x}) \leq c_1 H_K(\mathbf{x})$. \square

Consider a finite extension L of K . Let S be a finite subset of M_K and let $T \subset M_L$ be the set of valuations of L lying above those of S . For $x \in L$ put $|x|_T := \prod_{\omega \in T} |x|_\omega$. Define the ring of T -integers and T -units

$$\mathcal{O}_T := \{x \in L : |x|_\omega \leq 1 \text{ for } \omega \notin T\},$$

$$\mathcal{O}_T^\times := \{x \in L : |x|_\omega = 1 \text{ for } \omega \notin T\}.$$

Then \mathcal{O}_T is the integral closure of \mathcal{O}_S in L . We have

$$|x|_T = |N_{L/K}(x)|_S \text{ for } x \in L, \quad (1.5.1)$$

and in particular,

$$|x|_T = |x|_S^{[L:K]} \text{ for } x \in K. \quad (1.5.2)$$

For $\omega \in M_L$, denote by L_ω the completion of L at ω . Then there is a unique extension of ω to L_ω . For $\mathbf{x} = (x_1, \dots, x_n)^T \in L_\omega^n$, we define

$$\begin{aligned} \omega(\mathbf{x}) &= \min_{1 \leq i \leq n} \omega(x_i), \\ \|\mathbf{x}\|_\omega &= \max_{1 \leq i \leq n} |x_i|_\omega = \max_{1 \leq i \leq n} e^{-\omega(x_i)}. \end{aligned}$$

Similarly as before, we define $\text{div}_A(\mathbf{x}), \text{div}(A)$ for $\mathbf{x} \in L^n, A \in GL_n(\mathbb{A}_T)$ by replacing K, S with L, T respectively. That is,

$$\text{div}_A(\mathbf{x}) := \sum_{\omega \in M_L} \omega(A_\omega \mathbf{x}) \omega,$$

$$\operatorname{div}(A) := \sum_{\omega \in M_L} \omega(\det(A_\omega))\omega.$$

Define

$$\begin{aligned} h_A(\mathbf{x}) &:= -\deg(\operatorname{div}_A(\mathbf{x}))/[L : K], \\ h_A(L^n) &:= -\deg(\operatorname{div}(A))/[L : K], \end{aligned}$$

and

$$\begin{aligned} H_A(\mathbf{x}) &:= \exp(h_A(\mathbf{x})) = \left(\prod_{\omega \in M_L} \|A_\omega \mathbf{x}\|_\omega \right)^{\frac{1}{[L:K]}}, \\ H_A(L^n) &:= \exp(h_A(K^n)) = \left(\prod_{\omega \in M_L} |\det A_\omega|_\omega \right)^{\frac{1}{[L:K]}} = |\det(A)|_L^{\frac{1}{[L:K]}}. \end{aligned}$$

The height H_A on L^n is compatible with the one on K^n : $H_A(L^n) = H_A(K^n)$.

We recall Thunder's analogue of Minkowski's convex body theorem for function fields.

Lemma 1.5.3. *Let L be a finite extension of K of degree m , and H_A be the twisted height on L^n corresponding to $A \in GL_n(\mathbb{A}_S)$. Then there is a basis $\mathbf{a}_1, \dots, \mathbf{a}_n$ of L^n satisfying*

$$\prod_{i=1}^n H_A(\mathbf{a}_i) \leq H_A(L^n) e^{n(g_L+m-1)/m}.$$

where g_L is the genus of L .

Proof. See Theorem 1 of [24]. □

Lemma 1.5.4. *For every basis $\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ of L^n , we have*

$$\prod_{i=1}^n H_A(\mathbf{x}_i) \geq H_A(L^n).$$

In particular, there is a basis $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ of K^n such that

$$\prod_{i=1}^n H_A(\mathbf{a}_i) = H_A(K^n).$$

Proof. See Lemma 5 of [24] for the inequality. The equality is a combination with Lemma 1.5.3. □