Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

Small generators of function fields

par Martin Widmer

Résumé. Soit K/k une extension finie d'un corps global, donc K contient un élément primitif α, c'est à dire $K = k(\alpha)$. Dans cet article, nous démontrons l'existence d'un élément primitif de petite hauteur en cas d'un corps de fonctions. Notre résultat répond à une quéstion de Ruppert en cas d'un corps de fonctions.

Abstract. Let K/k be a finite extension of a global field. Such an extension can be generated over k by a single element. The aim of this article is to prove the existence of a "small" generator in the function field case. This answers the function field version of a question of Ruppert on small generators of number fields.

1. Introduction

Let K be a finite extension of a global field k where global field means finite extension of either $\mathbb{Q}$ or of a rational function field of transcendence degree one over a finite field. Such an extension is generated by a single element and there exists a natural concept of size on K given by the height. The well-known Theorem of Northcott (originally proved for algebraic numbers but easily seen to hold also in positive characteristic) implies that for each real T there are only finitely many $\alpha \in K$ whose height does not exceed T. In particular there exists a smallest generator. It is therefore natural to ask for lower and upper bounds for the height of a smallest generator. We emphasize the situation where d is fixed and K runs over all extensions of k of degree d.

Several people proved lower bounds for generators; first Mahler [5] for the ground field $k = \mathbb{Q}$ and then Silverman [8] for arbitrary ground fields (and also higher dimensions), but see also [7], [6] and [4] for simpler results. For an extension K/k of number fields Silverman's inequality implies

(1.1)
$$h(1,\alpha) \geq \log|\Delta_K|/(2d(d-1)) - \log|\Delta_k|/(2(d-1)) - [k:\mathbb{Q}]\log d/(2(d-1))$$

for any generator α of K/k. As shown by examples of Masser (Proposition 1 [6]) and Ruppert [7], this bound is sharp, at least up to an additive constant depending only on k and d. A version of Silverman's bound in the function field case follows quickly from Castelnuovo's inequality. For simplicity let us temporarily assume K and k are finite separable extensions of the rational function field $\mathbb{F}_q(t)$ both with field of constants $\mathbb{F}_q$. We apply Castelnuovo's inequality as in [9] III.10.3.Theorem with $F = K = k(\alpha)$, $F_1 = k$ and $F_2 = \mathbb{F}_q(\alpha)$. Writing g_k and g_K for the genus of k and K we conclude $[K : \mathbb{F}_q(\alpha)] \geq g_K/(d-1) - dg_k/(d-1) + 1$. From (2.1), (2.2) and the definition of the height in (2.3) we easily deduce $h(1,\alpha) \geq [K : \mathbb{F}_q(\alpha)]/d$ and thus

$$h(1,\alpha) \geq g_K/(d(d-1)) - g_k/(d-1) + 1/d. \tag{1.2}$$

The discriminant $\Delta_K = q^{\deg Diff(K/\mathbb{F}_q(t))}$ of $K/\mathbb{F}_q(t)$ is related with the genus by the Riemann-Hurwitz formula, more precisely $\Delta_K = q^{2g_K+2([K:\mathbb{F}_q(t)]-1)}$. Thus (1.2) matches with (1.1), at least up to an additive constant depending only on the degrees of k and K. A similar inequality as in (1.2) was given by Thunder ([10] Lemma 6). Opposed to Silverman Thunder does not assume separability for the extension K/k.

What about upper bounds for the smallest generator? It seems that this problem has not been studied much yet. However, at least for number fields the problem has been proposed explicitly by Ruppert. More precisely Ruppert ([7] Question 2) addressed the following question.

Question 1 (Ruppert, 1998). *Does there exist a constant $C = C(d)$ such that for each number field K of degree d there exists a generator α of the extension $K/\mathbb{Q}$ with $h(1,\alpha) \leq \log|\Delta_K|/(2d) + C$?*

Ruppert used the non-logarithmic naive height whereas we use the logarithmic projective absolute Weil height as defined in [2]. However, it is easily seen that the question formulated here is equivalent to Ruppert's Question 2 in [7]. One can show that there exists always an integral generator α of $K/\mathbb{Q}$ with $h(1,\alpha) \leq \log|\Delta_K|/d$, for a proof of this simple fact see [11]. On the other hand, if α is an integral generator of an imaginary quadratic field K with minimal polynomial $x^2+bx+c = (x-\alpha)(x-\overline{\alpha})$ then $h(1,\alpha) = \log\sqrt{\alpha\overline{\alpha}} = \log\sqrt{c} \geq \log\sqrt{4c-b^2} - \log 2 \geq \log|\Delta_K|/d - \log 2$. Nevertheless, Ruppert showed that Question 1 has an affirmative answer for $k = \mathbb{Q}$ and K either quadratic or a totally real field of prime degree. In fact, using Minkowski's convex body Theorem to construct a Pisot-number generator, it suffices to assume K has a real embedding and one can drop the prime degree condition. For more details we refer to [11]. Ruppert's result for $d = 2$ relies heavily on a distribution result of Duke [3] that does not appear to have an analogue for higher degrees and is ineffective. As a consequence Ruppert's constant C for $d = 2$ is ineffective.

In this note we introduce a completely different strategy which applies in the function field case and the number field case. However, it relies on the existence of a certain divisor which is guaranteed under GRH but might be rather troublesome to establish unconditionally. The aim of this short note is to answer positively Ruppert's question in the function field case. So let k be an algebraic function field with finite constant field k_0 and transcendence degree one over k_0. We have the following result.

Theorem 1.1. *Let K be a finite field extension of k. There exists an element α in K with $K = k(\alpha)$ and a constant $C = C(k, [K : k])$ depending solely on $k, [K : k]$ such that*

$$h(1, \alpha) \leq \frac{g_K}{d(K/k)} + C$$

where g_K denotes the genus of the function field K with field of constants K_0 and $d(K/k) = [K : k]/[K_0 : k_0]$.

2. Notation and definitions

Throughout this note we fix an algebraic closure $\overline{k}$ of k. All fields are considered to be subfields of $\overline{k}$. For any finite extension F of k we write F_0 for the field of constants in F; in other words F_0 is the algebraic closure of k_0 in F. When we talk of the field F we implicitly mean the field F with field of constants F_0. We define the geometric degree $d(F/k)$ of the extension F over k as

$$d(F/k) = \frac{[F : k]}{[F_0 : k_0]}.$$

Let $M(F)$ be the set of all places in F. For a place $\wp$ in $M(F)$ let $\mathcal{O}_\wp$ be the valuation ring of F at $\wp$; we can identify $\wp$ with the unique maximal ideal in $\mathcal{O}_\wp$. We write $F_\wp = \mathcal{O}_\wp/\wp$ for the residue class field and $\hat{F}_\wp$ for the topological completion of F at the place $\wp$. Write $\mathrm{ord}_\wp$ for the order function on $\hat{F}_\wp$ normalized to have image in $\mathbb{Z} \cup \infty$. We extend $\mathrm{ord}_\wp$ to ${\hat{F}_\wp}^n$ by defining

$$\mathrm{ord}_\wp(x_1, ..., x_n) = \min_{1 \leq i \leq n} \mathrm{ord}_\wp x_i$$

with the usual convention $\mathrm{ord}_\wp 0 = \infty > 0$. Each non-zero element $\boldsymbol{x}$ of F^n gives rise to a divisor $(\boldsymbol{x})$ over F

$$(\boldsymbol{x}) = \sum_{\wp \in M(F)} \mathrm{ord}_\wp(\boldsymbol{x}) \cdot \wp.$$

For a divisor A over F we define the Riemann-Roch space in F^n

$$L_n(A) = \{\boldsymbol{x} \in F^n \backslash 0; (\boldsymbol{x}) + A \geq 0\} \cup \{0\}.$$

This is a F_0 vector space of finite dimension. Denote its dimension over F_0 by $l_n(A)$.

The degree of a place $\wp$ in $M(F)$ is defined by $\deg_F \wp = [F_\wp : F_0]$. Let K be a finite extension of F and let $\mathfrak{B}$ be a place in $M(K)$ above $\wp$. We write $f(\mathfrak{B}/\wp) = [K_\mathfrak{B} : F_\wp]$ for the residue degree of $\mathfrak{B}$ over $\wp$. Then we have

$$\begin{aligned}\deg_K \mathfrak{B} = [K_\mathfrak{B} : K_0] = \frac{[K_\mathfrak{B} : F_0]}{[K_0 : F_0]} &= \frac{[K_\mathfrak{B} : F_\wp]}{[K_0 : F_0]}[F_\wp : F_0] \\ &= \frac{f(\mathfrak{B}/\wp)}{[K_0 : F_0]} \deg_F \wp. \qquad (2.1)\end{aligned}$$

Writing $e(\mathfrak{B}/\wp)$ for the ramification index we also have

$$\sum_{\mathfrak{B}|\wp} e(\mathfrak{B}/\wp) f(\mathfrak{B}/\wp) = [K : F], \qquad (2.2)$$

see for example III.1.11.Theorem in [9].

Each divisor $A = \sum_\wp a_\wp \wp$ over the smaller field F naturally defines a divisor

$$A^{(K)} = \sum_\wp \sum_{\mathfrak{B}|\wp} a_\wp e(\mathfrak{B}/\wp)\mathfrak{B}$$

over the large field K.

As in [10] we define the height h on non-zero $\boldsymbol{x}$ in K^n by

$$h(\boldsymbol{x}) = -\frac{\deg_K(\boldsymbol{x})}{d(K/k)}. \qquad (2.3)$$

Note that the degree of a principal divisor is zero so that the height defines a function on projective space $\mathbb{P}^{n-1}(K)$ over K of dimension $n-1$. This shows also that the height is nonnegative since to evaluate the height of $\boldsymbol{x}$ we can assume that one coordinate is 1. Moreover it is absolute in the following sense. Suppose $\boldsymbol{x} \in K^n$ and let D be the divisor given by $D = (\boldsymbol{x})$. Let R be a finite extension of K and view $\boldsymbol{x} \in R^n$. Let $D^{(R)}$ be the divisor over R given by $D^{(R)} = (\boldsymbol{x})$. By [1] Chap.15, Thm.9 we have $\deg_R(D^{(R)}) = d(R/K) \deg_K(D)$ and by [1] Chap.15, Thm.2 we have $d(R/k) = d(R/K)d(K/k)$. Thus $h(\boldsymbol{x})$ remains unchanged if one views $\boldsymbol{x}$ in R^n. Therefore the height extends to a projective height on $\overline{k}^n$. Suppose $\boldsymbol{x} \in L_n(\mathfrak{A}) \subseteq K^n$ then directly from the definition we see that

$$h(\boldsymbol{x}) \leq \frac{\deg_K \mathfrak{A}}{d(K/k)}. \qquad (2.4)$$

3. The strategy

Let S be a finite set of places in $M(K)$ such that the following two properties hold:
(i) for each place p in $M(k)$ there is at most one place in S that lies above p,
(ii)$f(\mathfrak{B}/p) = 1$ for all $\mathfrak{B} \in S$ and $p \in M(k)$ with $\mathfrak{B} \mid p$.

A set S with these two properties will be called admissible. Note that for each field F with $k \subseteq F \subseteq K$ and for all places $\mathfrak{B}, \mathfrak{B}' \in S$, $\wp, \wp' \in M(F)$ with $\mathfrak{B} \mid \wp$ and $\mathfrak{B}' \mid \wp'$ we have

$$\mathfrak{B} \neq \mathfrak{B}' \Rightarrow \wp \neq \wp', \tag{3.1}$$

$$f(\mathfrak{B}'/\wp') = 1. \tag{3.2}$$

We say the divisor $\mathfrak{A}$ is admissible if it can be written in the form

$$\mathfrak{A} = \sum_{\mathfrak{B} \in S} 1 \cdot \mathfrak{B}. \tag{3.3}$$

with an admissible set S.

Lemma 3.1. *Suppose $\mathfrak{A}$ is an admissible divisor and suppose $\boldsymbol{x} = (1, x)$ with $x \notin K_0$ and $\boldsymbol{x} \in L_2(\mathfrak{A})$. Then $k(x) = K$ and $h(\boldsymbol{x}) \leq \deg_K \mathfrak{A}/d(K/k)$.*

Proof. Suppose $k(x) = F \subsetneq K$ and write $(\boldsymbol{x}) = \sum_{\wp} a_{\wp}\wp$ for the divisor over F. When we consider $(\boldsymbol{x})$ as a divisor over K we have $(\boldsymbol{x}) = \sum_{\mathfrak{B}} a_{\mathfrak{B}}\mathfrak{B}$ with $a_{\mathfrak{B}} = a_{\wp}e(\mathfrak{B}/\wp)$. Note that none of the coefficients $a_{\wp}$ is positive and since $x \notin K_0$ at least one is negative, say $a_{\wp'}$. Since $(\boldsymbol{x})$ lies in $L_2(\mathfrak{A})$ and $\mathfrak{A}$ is an admissible divisor we conclude by (3.1) that there is exactly one place $\mathfrak{B}'$ in $M(K)$ with $\mathfrak{B}' \mid \wp'$ and by (3.2) that $f(\mathfrak{B}'/\wp') = 1$. Together with (2.2) we deduce that $1 < [K : F] = \sum_{\mathfrak{B}' \mid \wp'} e(\mathfrak{B}'/\wp')f(\mathfrak{B}'/\wp') = e(\mathfrak{B}'/\wp')$. This means that $a_{\mathfrak{B}'} = a_{\wp'}e(\mathfrak{B}'/\wp') < a_{\wp'} \leq -1$, contradicting the fact $\mathfrak{A} + (\boldsymbol{x}) \geq 0$. Thus $k(x) = K$. The remaining statement comes from (2.4). □

Lemma 3.2. *Suppose $\mathfrak{A}$ is an admissible divisor with $\deg_K \mathfrak{A} > g_K$. Then there exists α in K with $k(\alpha) = K$ and*

$$h(1, \alpha) \leq \frac{\deg_K \mathfrak{A}}{d(K/k)}.$$

Proof. We apply the Theorem of Riemann-Roch to the space $L_1(\mathfrak{A}) = \{x \in K\backslash 0; (x) + \mathfrak{A} \geq 0\} \cup \{0\}$ to conclude $l_1(\mathfrak{A}) > 1$. Therefore we find a α in $L_1(\mathfrak{A})\backslash K_0$. Now $(\boldsymbol{x}) = (1, \alpha)$ and (α) have the same pole-divisors and since $\mathfrak{A} \geq 0$ we see that $(\boldsymbol{x})$ lies in $L_2(\mathfrak{A})$. Applying Lemma 3.1 proves the lemma. □

4. Constructing a suitable divisor

In this section we will prove that K admits an admissible divisor of degree g_K+1 provided g_K is large enough.

Lemma 4.1. *Let l be a positive integer. The number of places $\mathfrak{B} \in M(K)$ with*

$$\begin{aligned}&\deg_K \mathfrak{B} = l \text{ and}\\ &f(\mathfrak{B}/p) = 1 \text{ for } p \in M(k) \text{ with } \mathfrak{B} \mid p\end{aligned}$$

is

$$\geq \frac{|K_0|^l}{l} - (2+7g_K)\frac{|K_0|^{l/2}}{l} - l[K_0:k_0][K:k](|K_0|^{l/2} + (2+7g_k)|K_0|^{l/4}).$$

Proof. Using Riemann's hypothesis one can obtain a good lower bound for the number of places $\mathfrak{B}$ of fixed degree. For instance V.2.10 Corollary (a) in [9] tells us that the total number of places $\mathfrak{B} \in M(K)$ with $\deg_K \mathfrak{B} = l$ is

$$\geq \frac{|K_0|^l}{l} - (2+7g_K)\frac{|K_0|^{l/2}}{l}.$$

From (2.1) we get $\deg_k p = l[K_0:k_0]/f(\mathfrak{B}/p)$ for $p \in M(k)$, $\mathfrak{B} \mid p$. Suppose $f = f(\mathfrak{B}/p) > 1$. Applying V.2.10 Corollary (a) again we get the following upper bound for the number of places $p \in M(k)$ with $\deg_k p = l[K_0:k_0]/f$

$$\begin{aligned}&\frac{f|k_0|^{l[K_0:k_0]/f}}{l[K_0:k_0]} + (2+7g_k)\frac{f|k_0|^{l[K_0:k_0]/(2f)}}{l[K_0:k_0]}\\ =&\frac{f|K_0|^{l/f}}{l[K_0:k_0]} + (2+7g_k)\frac{f|K_0|^{l/(2f)}}{l[K_0:k_0]}\\ \leq&|K_0|^{l/2} + (2+7g_k)|K_0|^{l/4}.\end{aligned}$$

Above each place p in $M(k)$ there lie at most $[K:k]$ places $\mathfrak{B} \in M(K)$. Therefore the number of places $\mathfrak{B} \in M(K)$ satisfying $\deg_K \mathfrak{B} = l$ and $f(\mathfrak{B}/p) = f > 1$ is

$$\leq [K:k](|K_0|^{l/2} + (2+7g_k)|K_0|^{l/4}).$$

Summing over all divisors f of $l[K_0:k_0]$ we find that the number of places $\mathfrak{B} \in M(K)$ satisfying $\deg_K \mathfrak{B} = l$ and $f(\mathfrak{B}/p) > 1$ is

$$\leq l[K_0:k_0][K:k](|K_0|^{l/2} + (2+7g_k)|K_0|^{l/4}).$$

This in turn implies that the number of places $\mathfrak{B} \in M(K)$ satisfying $\deg_K \mathfrak{B} = l$ and $f(\mathfrak{B}/p) = 1$ is

$$\geq \frac{|K_0|^l}{l} - (2+7g_K)\frac{|K_0|^{l/2}}{l} - l[K_0:k_0][K:k](|K_0|^{l/2} + (2+7g_k)|K_0|^{l/4})$$

and this proves the lemma. □

5. Proof of Theorem 1.1

Let d be a positive integer. We can find a constant $C_1 = C_1(k,d)$ such that with $l = g_K + 1$

$$\frac{|K_0|^l}{l} - (2+7g_K)\frac{|K_0|^{l/2}}{l} - l[K_0:k_0][K:k](|K_0|^{l/2} + (2+7g_k)|K_0|^{l/4}) > 0$$

for all extensions K of k satisfying $g_K > C_1$ and $[K:k] = d$. By virtue of Lemma 4.1 we conclude that for each such K there exists a place $\mathfrak{B} \in M(K)$ with $\deg_K \mathfrak{B} = g_K + 1$ and $f(\mathfrak{B}/p) = 1$ for $p \in M(k)$ with $\mathfrak{B} \mid p$. In particular there exists an admissible divisor, namely $\mathfrak{B}$, with $\deg_K \mathfrak{B} = g_K + 1$. From Lemma 3.2 we conclude that if $g_K > C_1$ and $[K:k] = d$ then there exists $\alpha \in K$ with $K = k(\alpha)$ and $h(1,\alpha) \leq (g_K+1)/d(K/k)$. There are only finitely many field extensions K of k of degree d with $g_K \leq C_1$. Hence there exists a constant C as in Theorem 1.1 depending solely on C_1, k, d and thus depending solely on k, d such that the statement of Theorem 1.1 holds for all extensions K of k of degree d.

Acknowledgements

I would like to thank Felipe Voloch for giving me the idea of the proof of Lemma 4.1 and pointing out the connection with Castelnuovo's bound mentioned in the Introduction. Moreover I am grateful to David Masser, Jeff Thunder and Jeff Vaaler for many delightful discussions.

References

1. E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach, New York, 1967.
2. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
3. W. Duke, *Hyperbolic distribution problems and half-integral weight Masss forms*, Invent. Math. **92** (1988), 73–90.
4. J. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **no.1, Art. ID rnm002** (2007).
5. K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.
6. D. Roy and J. L. Thunder, *A note on Siegel's lemma over number fields*, Monatsh. Math. **120** (1995), 307–318.
7. W. Ruppert, *Small generators of number fields*, Manuscripta math. **96** (1998), 17–22.
8. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
9. H. Stichtenoth, *Algebraic function fields and codes*, Springer, 1993.
10. J. L. Thunder, *Siegel's lemma for function fields*, Michigan Math. J. **42** (1995), 147–162.
11. J. D. Vaaler and M. Widmer, *On small generators of number fields*, in preparation (2009).

Martin Widmer
Institut für Mathematik A
Technische Universität Graz
Steyrergasse 30/II
8010 Graz
Austria
E-mail : widmer@tugraz.at