Bounds for the Euclidean minima of function fields

Piotr Maciak\textsuperscript{a}, Marina Monsurr\textordmasculine\textsuperscript{b}, Leonardo Zapponi\textsuperscript{c}

\textsuperscript{a}École Polytechnique Fédérale de Lausanne (EPFL), Lausanne (CH)
\textsuperscript{b}Università Europea di Roma (UER), Roma (I)
\textsuperscript{c}Université Pierre et Marie Curie (UPMC), Paris (F)

Abstract

In this paper, we define Euclidean minima for function fields and give some bound for this invariant. We furthermore show that the results are analogous to those obtained in the number field case.

Keywords: Function fields, algebraic curves, Euclidean minima

Contents

1 Introduction 2

2 Geometric approach 4
  2.1 Settings and notation ........................................ 4
  2.2 The index of speciality .................................... 5
  2.3 An upper bound for Euclidean minima .................... 5
  2.4 A special case. Weierstrass gaps ....................... 6

3 The analogy with the number field case 8
  3.1 Upper bounds for the Euclidean minima of number fields ... 8
  3.2 The function fields analogue ............................. 8

4 The case of a general base field 10
  4.1 General base fields ....................................... 10
  4.2 An example: hyperelliptic curves ....................... 10
1. Introduction

The Euclidean minimum is a numerical invariant which measures how elements of a number field can be approximated by algebraic integers. Its study is a classical topic in algebraic number theory, going back to Minkowski and Hurwitz. Many mathematicians have studied its properties; among the others, we can cite Barnes, Swinnerton-Dyer, Cassels, Davenport and Fuchs, but this list is far from being exhaustive. This research area is still very active nowadays, and many problems are still open. We can mention for example the works of Van der Linden, Cerri and Bayer-Fluckiger. One of the central questions is to find upper bounds for Euclidean minima. We refer to [L1995] for a nice survey of the topic.

The Euclidean minima can also be defined in the function field case, replacing the absolute value by the degree. Not much is known in this situation. The existence of Euclidean function fields was studied by Armitage, Markanda, Madam, Queen and Smith but Euclidean minima never explicitly appear in their work. The aim of the present paper is to investigate this question more closely, trying to obtain bounds analogous to the known bounds in the number field case.

The paper is organized as follows: section 2, which is of geometric flavour is mainly inspired from the guiding example of polynomials: it is well-known that, given a field $k$, the ring $k[T]$ is euclidean with respect to the degree. Now, from a geometric point of view, the field $k(T)$ is just the function field of the projective line, and $k[T]$ is the subring consisting of functions which are regular outside the point at infinity. Starting from this observation, we try to generalize the construction: we first of all consider a (smooth, proper) curve $C$ over a field $k$, which is assumed to be algebraically closed. We then consider a finite subset $S$ of $C$ and define a degree function, denoted by $\text{deg}_S$, for rational functions on the curve. The ring $\mathcal{O}_S$ is the subset of the field $K = k(C)$ consisting of rational functions which are regular outside $S$. In other words, the affine curve $C \setminus S$ is just the spectrum of $\mathcal{O}_S$. For $C = \mathbb{P}^1$ and $S = \{\infty\}$, we then find $K = k(T)$ and the ring $\mathcal{O}_S = k[T]$ is an univariate polynomial ring over $k$, the function $\text{deg}_S$ coinciding with the usual degree for polynomials. The (logarithmic) Euclidean minimum of $K$ with respect to $S$, denoted by $\text{M}_S(K)$, is then defined as

$$\text{M}_S(K) = \max_{x \in K} \min_{y \in \mathcal{O}_S} \{\text{deg}_S(x - y)\}.$$  

This integer measures how well a rational function can be approximated by an element of $\mathcal{O}_S$. In particular, the ring $\mathcal{O}_S$ is Euclidean with respect to the function $\text{deg}_S$ if and only if the inequality $\text{M}_S(K) < 0$ holds. The main result of the section relates $\text{M}_S(K)$ to a geometric invariant we introduce here: the degree of speciality $\mu(S)$ of $S$, which, roughly speaking, describes the behaviour of differential forms on $S$ having no poles outside $S$. In Theorem 2, we prove that we have the inequality $\text{M}_S(K) \leq \mu(S)$. The main ingredient of the proof is the Riemann-Roch theorem. It then follows that $\text{M}_S(K)$ is less than or equal to $2g - 1$, where $g$ denotes the genus of $C$ (this bound again follows from Riemann-Roch formula), providing an upper bound which can be considered, as we will
show later, as the precise analogue of the results obtained in the number field case in [BF2006]. The end of the section is devoted to the special case where the set $S$ is a singleton. In this situation, we can prove (cf. Proposition 3) that we have in fact the equality $M_S(K) = \mu(S)$ and, moreover, that $\mu(S)$ is the greatest integer appearing in the Weierstrass gap sequence of $S$. In particular, we obtain the lower bound $M_S(K) \geq g$ and we provide examples where $M_S(K)$ is explicitly computed (hyperelliptic curves, étale covers of the affine line, classical curves).

As stated above, in section 3 we show that Theorem 2 can be considered as a (logarithmic) analogue of the general bounds obtained in the number field case. It is important to notice that there is a crucial difference between number fields and function fields. Indeed, a number field can be obtained in a unique way as an extension of the rationals. In particular, its degree and discriminant are uniquely defined global objects. For a function field $K$, things are quite different, since it can be realized in many (infinite) ways as an extension of the field $k(T)$. Its degree and discriminant are no more intrinsic invariants and strongly depend on this realization. This is the main reason why in section 2 we tried to obtain results avoiding this arbitrary choice. But now, if we want to find a parallel between the present results and the number field counterpart, we have to consider the field $K$ as a finite extension of the field $k(T)$. In this setting, we slightly modify the definition of the Euclidean minimum, now simply denoted by $M(K)$, which turns out to be just a special case of the one defined before (for a particular choice of the set $S$). In theorem 8, we obtain an upper bound for $M(K)$ only depending on the degree and on the discriminant of the extension $\mathcal{O}_K/k[T]$ (here, the ring $\mathcal{O}_K$ is the integral closure of $k[T]$ in $K$, which, once again coincides within the ring $\mathcal{O}_S$ previously defined). In fact, Theorem 8 is just a weaker version (and a direct consequence) of Theorem 2, the main ingredient for its proof being the Hurwitz formula. The main limitation is that we have to suppose that the ramification above the point at infinity is tame. A more general, and sharper result could be obtained by considering the full ramification of the extension $K/k(T)$ (taking account of the behaviour above infinity) but we decided to state it in a form more similar to the number field case.

Until now, we worked in a geometric setting, assuming that the base field $k$ is algebraically closed. In the last section of the paper, we drop this assumption and investigate the more general case of a perfect base field. Most of the constructions and results remain valid in this situation: the Euclidean minimum and the index of speciality are defined in the same way and the inequality of Theorem 2 still holds. However, it is no longer true that $\mu(S)$ is less than or equal to $2g - 1$. Moreover, it actually turns out that the Euclidean minimum depends on the base field. Indeed, we explicitly treat the case of hyperelliptic curves and in Theorem 10 we show that in this case $M(K)$ can actually be equal to $2g$, which is impossible if $k$ is algebraically closed.

We would like to thank Eva Bayer-Fluckiger, who originally motivated and then constantly encouraged this joint work. Her results in the number field case have been the main inspiration of the paper. The second and third authors also
express their thanks for her invitation at the EPFL, where most of the results were obtained.

2. Geometric approach

2.1. Settings and notation

In the following, \( C \) denotes a smooth, projective curve of genus \( g \), defined over an algebraically closed field \( k \). Set \( K = k(C) \) and let \( v_P \) (resp. \( O_P \)) be the valuation of \( K \) (resp. the local ring) associated to a point \( P \) of \( C \). For any finite, nonempty subset \( S \) of \( C \), let \( O_S \) be the subring of \( K \) consisting of rational functions regular outside \( S \). For any rational function \( x \in K \), consider the integer \( \deg_S(x) \) defined by

\[
\deg_S(x) = -\sum_{P \in S} v_P(x).
\]

For simplicity, we furthermore set \( \deg_S(0) = -\infty \). It is easily checked that for any element \( x \neq 0 \) of \( O_S \), we have the inequality \( \deg_S(x) \geq 0 \), which is an equality if and only if \( x \) belongs to \( O_S^\times \). By construction, for any \( x, y \in K \), we have the relations

- \( \deg_S(xy) = \deg_S(x) + \deg_S(y) \).
- \( \deg_S(x + y) \leq \max\{\deg_S(x), \deg_S(y)\} \).

Remark. For \( C = \mathbb{P}^1 \) and \( S = \{\infty\} \), the ring \( O_S \) can be identified with the polynomial ring \( k[T] \) and, for any \( x \in O_S \), the integer \( \deg_S(x) \) is the usual degree of a polynomial.

The Euclidean minimum of \( K \) (with respect to \( S \)) is the integer defined as

\[
M_S(K) = \max_{x \in K} \min_{y \in O_S^\times} \{\deg_S(x - y)\}.
\]

The inequality \( M_S(K) < 0 \) holds if and only if the ring \( O_S \) is Euclidean with respect to the Euclidean function \( \deg_S \).

2.2. The index of speciality

Following the usual notation, for any divisor \( D \) on \( C \), let \( \Omega(D) \) be the \( k \)-vector space of differential forms \( \omega \) on \( C \) satisfying the relations \( v_P(\omega) + v_P(D) \geq 0 \) for any \( P \in C \) (in [S1988], this \( k \)-vector space is denoted by \( \Omega(-D) \), we nevertheless adopt the more recent and usual notation). Denote by \( \mathbb{Z}[S] \) the free abelian group generated by the elements of \( S \), i.e. the subgroup of \( \text{Div}(C) \) consisting of divisors whose support is contained in \( S \). The index of speciality of \( S \) is the integer \( \mu(S) \) defined by

\[
\mu(S) = \min\{\deg(D) \mid D \in \mathbb{Z}[S] \text{ and } \Omega(-D) = 0\}.
\]
Remark. The dimension of the $k$-vector space $\Omega(D)$ only depending on the linear equivalence of the divisor $D$, we may replace $\mathbb{Z}[S]$ by the subgroup of Pic($C$) generated by $S$.

Lemma 1. We have the inequalities

$$g - 1 \leq \mu(S) \leq 2g - 1.$$ 

Proof. Let $D$ be a divisor on $C$ of degree greater than or equal to $2g - 1$ and suppose that there exist an element $\omega \in \Omega(-D)$ different from 0. In this case, we obtain the relations

$$2g - 2 = \text{deg}(\omega) \geq \text{deg}(D) \geq 2g - 1,$$

a contradiction. We therefore have $\Omega(-D) = 0$. Since the field $k$ is algebraically closed, there exists an element $D \in \mathbb{Z}[S]$ of degree $2g - 1$, which implies that $\mu(S) \leq 2g - 1$. Suppose now that $\text{deg}(D) < g - 1$ and denote by $L(D)$ the $k$-vector space of rational functions $x \in K$ for which $v_P(x) + v_P(D) \geq 0$. The Riemann-Roch formula leads to the relations

$$\dim_k \Omega(-D) = \dim_k L(D) - \deg(D) + g - 1 > 0,$$

and the second inequality follows. $\square$

2.3. An upper bound for Euclidean minima

We now prove the main result of the section. We will later see that (and explain why) it is analogous to the bound obtained in the number field case.

Theorem 2. We have the inequality

$$M_S(K) \leq \mu(S).$$

Proof. Let $A_K$ denote the adele ring of $K$, i.e. an element $r \in A_K$ is a collection $r = (r_P)_{P \in C}$ of rational functions such that $r_P \in \mathcal{O}_P$ for almost all $P$ in $C$ (see [S1988], Chapter II, §5 for general definitions and properties of adele rings on curves). For any divisor $D$ on $C$, let $A_K(D)$ denote the $k$-vector space of adeles $r$ such that $v_P(r_P) + v_P(D) \geq 0$ for all $P \in C$. By Serre duality, the quotient $I(D) = A_K/(A_K(D) + K)$ is canonically isomorphic to the dual of the $k$-vector space $\Omega(-D)$. Let now $D \in \mathbb{Z}[S]$ be a divisor such that $\text{deg}(D) = \mu(S)$. Fix a rational function $x \in K^\times$ and consider the adele $r = (r_P)$ defined by

$$r_P = \begin{cases} 
  x & \text{for } P \in S, \\
  0 & \text{otherwise}. 
\end{cases}$$

By construction, we have $\Omega(D) = 0$ and therefore $I(D) = 0$. In particular, there exist $y \in K$ and $r' \in A_K(D)$ such that $r = r' + y$. It then follows that the poles of the rational function $y$ are contained in $S$, and thus we have $y \in \mathcal{O}_S$. Furthermore, from the definition of $r$, we have the inequalities

$$v_P(x - y) + v_P(D) \geq 0$$

and the second inequality follows. $\square$
for any $P \in S$, which finally leads to
$$\deg_S(x - y) \leq \deg(D) = \mu(S).$$
We therefore have the inequality $M_S(K) \leq \mu(S)$. \hfill \Box

2.4. A special case. Weierstrass gaps

Though we are not able to prove it in full generality, it is reasonable to believe that the inequality of Theorem 2 is in fact an equality. We will now see that it is actually true if the set $S = \{P\}$ is reduced to a single point. Until the end of this section, we restrict to this situation. The study of the index of speciality, simply denoted by $\mu(P)$ in this case, is closely related to the Weierstrass gap sequence of $P$. We therefore briefly recall some basic facts of the theory: setting $\ell(nP) = \dim_k L(nP)$ and $i(nP) = \dim_k \Omega(nP)$, we have the relations
$$\ell(0) = 1, \ell(nP) \leq \ell((n + 1)P) \leq \ell(nP) + 1 \text{ and } \ell((2g - 1)P) = g.$$ 
Furthermore, for $n \geq 2g - 1$, we have the identity $\ell(nP) = n - g + 1$. In terms of differential forms, the Riemann-Roch formula leads to the relations
$$i(0) = g, i(-nP) \geq i(-(n + 1)P) \geq i(-nP) - 1 \text{ and } i((1 - 2g)P) = 0.$$ 

A Weierstrass gap of $P$ is an integer $n$ such that $\ell(nP) = \ell((n - 1)P)$, which means that there does not exist a rational function $x \in K$ having a unique pole at $P$ of exact order $n$. Equivalently, we have the identity $i(-nP) = i((1 - n)P) - 1$, which implies that there exists a regular differential form having a zero at $P$ of order $n - 1$. It then follows that there are exactly $g$ gaps $0 < n_1 < n_2 \cdots < n_g < 2g$. The gap sequence is just the collection $(n_1, \ldots, n_g)$. Notice that, by definition, the index of speciality $\mu(P)$ is just the integer $n_g$, the greatest Weierstrass gap. Given the curve $C$, there exist a sequence $N = (n_1, \ldots, n_g)$ such that all but finitely many points of $C$ have $N$ as Weierstrass gap sequence. The points having a Weierstrass gap sequence different from $N$ are called Weierstrass points, while the others are ordinary points. If $N = \{1, 2, \ldots, g\}$, we say that $C$ is a classical curve. In characteristic 0, any curve is classical, but this is false in positive characteristic (though it is the case if the characteristic of the base field is large enough with respect to the genus of the curve).

**Proposition 3.** If $S = \{P\}$ is reduced to a single point, then we have the identity
$$M_S(K) = \mu(S).$$
In particular, we have the inequalities
$$g \leq M_S(K) \leq 2g - 1.$$ 

**Proof.** Given a point $Q \neq P$ of $C$, the Riemann-Roch theorem implies that there exists a rational function $x \in K$ having no poles outside the set $\{P, Q\}$ and such that $v_P(x) = -\mu(P)$, so that $\deg_S(x) = \mu(S)$. Now, the relation
\[ \deg_S(x - y) < \mu(x), \] with \( y \in \mathcal{O}_S \), would imply that the rational function \( y \) has a unique pole at \( P \) of order \( \mu(P) \), which is impossible since \( \mu(P) \) is a Weierstrass gap. The two inequalities again follow from the fact that \( \mu(P) \) is a Weierstrass gap.

**Example.** Once again, taking \( C = \mathbb{P}^1 \) and \( S = \{ \infty \} \), so that \( K = k(T) \) and \( \mathcal{O}_S = k[T] \), we find the inequality \( M_S(K) < -1 \), recovering the well known fact that the ring \( k[T] \) is Euclidean with respect to the degree.

We close this section with three examples where we can actually compute the Euclidean minimum, and show that for fixed \( g \), the bounds of Proposition 3 are attained.

**Corollary 4.** Let \( C \) be an hyperelliptic curve and suppose that \( P \) is a Weierstrass point on it. We then have the identity

\[ M_S(K) = 2g - 1. \]

**Proof.** A well-known result on hyperelliptic curves asserts that \( P \) is a Weierstrass point if and only its gap sequence is \( (1, 3, \ldots, 2g - 1) \) (see for example [F1969, Exercice 8.37], where the characteristic of the base field is assumed to be 0, but everything remains true in full generality), from which we deduce the relation \( \mu(P) = 2g - 1 \). The result is then a direct consequence of Proposition 3.

**Remark.** The above result is actually true for superelliptic curves, i.e. curves \( C \) defined by affine equations \( Y^n = f \), where \( f \in k[X] \) and the characteristic of \( k \) does not divide \( n \). More precisely, if \( r \) denotes the degree of \( f \), then there is a canonical degree \( n \) cover \( C \to \mathbb{P}^1 \) totally ramified at \( r \) or \( r + 1 \) points. If \( P \) is one of them, it is then easily checked that \( 2g - 1 \) belongs to its gap sequence and is therefore the greatest Weierstrass gap. In particular, setting \( S = \{ P \} \), we find \( \mu(S) = 2g - 1 \) and Proposition 3 asserts that we have the identity \( M_S(K) = 2g - 1 \).

**Corollary 5.** Suppose that there exists an étale cover \( \pi : C \setminus S \to \mathbb{A}^1 \). We then have the identity

\[ M_S(K) = 2g - 1. \]

**Proof.** Consider a differential form \( \omega \) on \( \mathbb{P}^1 \) having a double pole at \( \infty \) (it is unique, up to multiplication by an element of \( k^* \)). Since the canonical divisor of \( \mathbb{P}^1 \) has degree \(-2\), it follows that \( \omega \) is regular and non-vanishing outside \( \infty \). In particular, the cover \( \pi \) being étale outside \( \infty \), the pull-back \( \pi^* \omega \) is regular and nowhere vanishing outside \( P = \pi^{-1}(\infty) \), so that \( \omega \) has a unique zero at \( P \) of order \( 2g - 2 \), and thus the integer \( 2g - 1 \) belongs to the gap sequence of \( P \), which concludes the proof.

**Corollary 6.** Suppose that the curve \( C \) is classical and that \( P \) is not a Weierstrass point. We then have the identity

\[ M_S(K) = g. \]

**Proof.** It is again a consequence of Proposition 3, since in this case, the gap sequence of \( P \) is \( (1, 2, \ldots, g) \), leading to \( \mu(P) = g \).
3. The analogy with the number field case

3.1. Upper bounds for the Euclidean minima of number fields

As it is stated in the previous paragraph, Theorem 2 could seem quite far from the kind of results obtained in the number field case. We will now show that it actually leads to an upper bound for the Euclidean minima which is, *mutatis mutandis*, a complete analogy with the known results and conjectures. We first of all briefly summarize the number field case: let $K$ be a number field, i.e. a finite extension of the field $\mathbb{Q}$ of rational numbers, and denote by $\mathcal{O}_K$ its ring of integer (the integral closure of $\mathbb{Z}$ in $K$). The *Euclidean minimum* of $K$ is the real number $M(K)$ defined as

$$M(K) = \sup_{x \in K} \inf_{y \in \mathcal{O}_K} \{|N_{K/\mathbb{Q}}(x-y)|\},$$

where $| \cdot |$ denotes the usual (Archimedean) absolute value. The study of Euclidean minima is a hard and classical topic in algebraic number theory. One of the main results, obtained by E. Bayer-Fluckiger in [BF2006] in 2006, is the following general upper bound for Euclidean minima:

**Theorem 7** (Bayer-Fluckiger, 2006). Let $n$ be the degree of the extension $K/\mathbb{Q}$ and denote by $d_k$ its discriminant. We then have the inequality

$$M(K) \leq 2^{-n} |d_k|.$$

3.2. The function fields analogue

The aim of this section is to give a bound for the Euclidean minima of function fields, analogous to Theorem 7. We first of all fix the notation and settings: the field $\mathbb{Q} = k(T)$ will play the role of the field $\mathbb{Q}$, the ring $\mathbb{Z} = k[T]$ replacing $\mathbb{Z}$. We denote by $K$ a finite, separable extension of $\mathbb{Q}$ of degree $n$ and by $\mathcal{O}_K$ the integral closure of $\mathbb{Z}$ in $K$. The discriminant of the extension $\mathcal{O}_K/\mathbb{Z}$, denoted by $d_K$, considered as an ideal of $\mathbb{Z}$, is generated by a polynomial $f$ and we set $\deg(d_K) = \deg(f)$. The *Euclidean minimum* $M(K)$ is the integer defined as

$$M(K) = \max_{x \in K} \min_{y \in \mathcal{O}_K} \{\deg(N_{K/\mathbb{Q}}(x-y))\},$$

where we have set $\deg = \deg_\infty$ (the extension to $\mathbb{Q}$ of the usual degree of a polynomial, cf. the first remark of §2).

**Remark.** Before continuing, we must stress on two important points:

- The rings $\mathbb{Z}$ and $\mathcal{Z}$ are both Euclidean. In the first case, the associated Euclidean function is the absolute value, which is multiplicative i.e. $|xy| = |x| \cdot |y|$, while in the latter case the Euclidean function is the degree, which is additive i.e. $\deg(xy) = \deg(x) + \deg(y)$. The Euclidean minimum is then defined in a similar way, but because of this difference, the bounds for function fields should be considered as a 'logarithmic' analogue of those obtained in the number field case.
For function fields case, the discriminant $d_K$ does not take account of the ramification above $\infty$ (the valuation associated to the prime element $T^{-1}$); this is the main difference with number fields, where the discriminant completely describes the ramification of the extension.

We can now state and prove the main result of this section, which is a weaker form of Theorem 2 and can be considered as the analogue of Theorem 7.

**Theorem 8.** The assumptions and hypothesis being as above, suppose that the extension $K/\mathbb{Q}$ is tamely ramified above $\infty$. We then have the inequality

$$M(K) \leq \deg(d_K) - n.$$  

**Proof.** From a geometric point of view, the extension $K/\mathbb{Q}$ corresponds to a finite cover $\pi : C \to \mathbb{P}^1$. Setting $S = \pi^{-1}(\infty)$, the ring $\mathcal{O}_K$ then coincides with the ring $\mathcal{O}_S$ defined in the first section and, taking spectra, the extension $\mathcal{O}_K/\mathcal{O}_S$ defines a finite cover $C \setminus S \to \mathbb{A}^1$, which is just the restriction of $\pi$ to the open set $\mathbb{A}^1 \subset \mathbb{P}^1$. For any rational function $x \in K$, a straightforward computation leads to the relation

$$\deg(N_{K/\mathbb{Q}}(x)) = \deg(S(x)).$$

In particular, we find the identity

$$M(K) = M_S(K).$$

Let $R$ be the ramification divisor of $\pi$ and $B = \pi_*(R)$ its branch divisor (see [H1983], §IV.2 for general definitions and properties). We then have the identity $\deg(R) = \deg(B)$ and $d_K$, considered as a divisor, is just the restriction of $B$ to $\mathbb{A}^1$. Moreover, if $g$ denotes the genus of $C$, the Hurwitz formula ([H1983], Corollary 2.4 of Chapter IV) reads

$$2g - 2 = \deg(B) - 2n.$$  

Now, if the ramification above $\infty$ is tame, we then have the inequality

$$\deg(B) \leq \deg(d_K) + n - 1.$$  

In this case, combining Lemma 1 and Theorem 2, we finally obtain the relations

$$M(K) \leq 2g - 1 = \deg(B) - 2n + 1 \leq \deg(d_K) - n,$$

which concludes the proof. \qed

**Theorem 9.** Suppose that the extension $K/\mathbb{Q}$ is totally ramified above $\infty$ and that the characteristic of $k$ does not divide $n$. We then have the inequalities

$$\frac{1}{2} (\deg(d_K) - n - 1) \leq M(K) \leq \deg(d_K) - n.$$
Proof. Following the notation of the proof of Theorem 8, the ramification above \( \infty \) being tame, we have the identity

\[
\deg(B) = \deg(d_K) + n - 1
\]

Now, since the set \( S \) is reduced to a point, Proposition 3 asserts that we have the inequalities

\[
g - 1 \leq M(K) \leq 2g - 1
\]

and the Hurwitz formula finally leads to the relations

\[
\frac{1}{2} (\deg(d_K) - n - 1) \leq M(K) \leq \deg(d_K) - n,
\]

as desired. \( \square \)

4. The case of a general base field

4.1. General base fields

Until now, we assumed that the base field \( k \) is algebraically closed. We now drop this assumption and we only suppose that \( k \) is perfect. Most of the constructions of the previous sections actually apply in this more general situation, with only minor changes: first of all, going back to section 2 and setting \( G_k = \text{Gal}(\bar{k}/k) \), we must assume that the set \( S \subset C(\bar{k}) \) is stable under the action of \( G_k \). The definition of the \( S \)-degree \( \deg_S \) and of the Euclidean minima are exactly the same. Concerning the index of speciality, we just replace the group \( \mathbb{Z}[S] \) by the subgroup \( \mathbb{Z}[S]^{G_k} \) of \( G_k \)-invariants. In particular, it turns out that \( \mu(S) \) can be strictly bigger than in the case of an algebraically closed field \( k \).

Example. Suppose that \( C \) is an elliptic curve and that \( S = \{P, Q\} \) consists of two \( G_k \)-conjugated points. Setting \( D = P + Q \), we then find \( \mathbb{Z}[S]^{G_k} = \mathbb{Z}[D] \) therefore \( \mu(S) = \deg(D) = 2 \). On the other hand, over \( \bar{k} \), setting \( F = P - Q \in \mathbb{Z}[S] \), we find \( \Omega(-F) = 0 \) and it actually turns out that \( \mu(S) = \deg(F) = 0 \).

The result in Theorem 2 still holds. However, in this case we no longer have the inequality \( \mu(S) \leq 2g - 1 \), which was of crucial importance in section 3. Nevertheless, if \( S \) is reduced to a point, then everything works perfectly.

Remark. If the residual degrees (i.e. the degrees of the fields of definition) of the elements of \( S \) are globally coprime, which is the same assumption made in [A1963], then we still have the inequality \( \mu(S) \leq 2g - 1 \) and all the results of the previous sections are true.

4.2. An example: hyperelliptic curves

We close the paper with an example where the Euclidean minimum can be explicitly computed, showing that its behaviour is different than in the case of an algebraically closed field. In the following, we assume that the characteristic of \( k \) is different from 2. Let \( g \) be a positive integer, fix a polynomial \( f \in k[X] \)
of degree $2g + 2$ whose leading coefficient is not a square in $k^\times$ and consider the hyperelliptic curve $C$ defined by the affine equation $Y^2 = f$. By construction, its genus is equal to $g$ and there exist two points $P$ and $Q$ at infinity which are permuted by $G_k$. There is a canonical double cover $C \to \mathbb{P}^1$ and, setting $S = \{P, Q\}$, the ring $\mathcal{O}_S = k[X, Y]$ is an extension of $k[X]$ of degree 2 which coincides with the integral closure of $k[X]$ in $K$. Moreover, as noticed in the proof of Theorem 8, for any rational function $x \in K$, we have the identity

$$\deg_S(f) = \deg(N_{K/\mathbb{Q}}(x)),$$

where we have set $\mathbb{Q} = k(X)$. As in the previous section, we simply write $M(K)$ instead of $M_S(K)$.

**Theorem 10.** The notation and assumptions being as above, we have the identity

$$M(K) = 2g.$$

**Proof.** Any element of $x \in K$ can be uniquely written as a sum $x = a + Yb$, with $a, b \in \mathbb{Q}$, and we have the relation

$$N_{K/\mathbb{Q}}(x) = a^2 - fb^2.$$

We want to minimize the degree (meant as $\deg_\infty$) of the rational function

$$N_{K/\mathbb{Q}}(x - y) = (a - c)^2 - f(b - d)^2 \in \mathbb{Q},$$

where $y = c + dY$ is an element of $\mathcal{O}_S$, with $c, d \in k[X]$. The assumption on the leading coefficient of $f$ leads to the relation

$$\deg \left((a - c)^2 - f(b - d)^2\right) = 2 \max\{\deg(a - c), g + 1 + \deg(b - d)\}.$$

Once again, we have set $\deg = \deg_\infty$ (in particular, the degree of a rational function is not the number of its poles, counted with their multiplicity). Now, as remarked in the first section, the fact that the ring $k[X]$ is Euclidean with respect to the degree implies that there exist two elements $c, d \in k[X]$ (which are in fact unique) such that $\deg(a - c) \leq -1$ and $\deg(b - d) \leq -1$. We therefore find the inequality

$$\min_{y \in k[X]} \{\deg(N_{K/\mathbb{Q}}(x - y))\} \leq 2g$$

and thus $M(K) \leq 2g$. Finally, it is easily checked that for the rational function $x = YX^{-1} \in K$ we have the identity

$$\min_{y \in k[X]} \{\deg(N_{K/\mathbb{Q}}(x - y))\} = 2g,$$

so that $M(K) = 2g$, which concludes the proof.
References

[A1963] Armitage, J. Vernon. Euclid’s algorithm in algebraic function fields. J. London Math. Soc. 38 (1963).

[BF2006] Bayer-Fluckiger, Eva. Upper bounds for Euclidean minima of algebraic number fields. J. Number Theory 121, no. 2 (2006).

[F1969] Fulton, William. Algebraic curves. Mathematics Lecture Notes Series (1969).

[H1983] Hartshorne, Robin. Algebraic geometry. GTM 52 (1983).

[L1995] Lemmermeyer, Franz. The Euclidean algorithm in algebraic number fields. Exposition. Math. 13 (1995), no. 5.

[S1988] Serre, Jean-Pierre. Algebraic groups and class fields. GTM 117 (1988).