Troisième Rencontre Internationale sur les Polynômes à Valeurs Entières

Rencontre organisée par :
Sabine Evrard

29 novembre-3 décembre 2010

David Adam and Paul-Jean Cahen

Newton and Schinzel sequences in quadratic fields

Vol. 2, n° 2 (2010), p. 15-20.

<http://acirm.cedram.org/item?id=ACIRM_2010__2_2_15_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

Actes des rencontres du C.I.R.M.
Vol. **2** n° 2 (2010) 15-20

Newton and Schinzel sequences in quadratic fields

David Adam and Paul-Jean Cahen

Abstract

We give the maximal length of a Newton or a Schinzel sequence in a quadratic extension of a global field. In the case of a number field, the maximal length of a Schinzel sequence is 1, except in seven particular cases, and the Newton sequences are also finite, except for at most finitely many cases, all real. We give the maximal length of these sequences in the special cases. We have similar results in the case of a quadratic extension of a function field $\mathbb{F}_q(T)$, taking in account that the ring of integers may be isomorphic to $\mathbb{F}_q[T]$, in which case there are obviously infinite Newton and Schinzel sequences.

1. Introduction

This talk[1] gives an account of a paper with the same title and by the same authors, in *Journal of Pure and Applied Algebra*, **215** (2011) 1902–1918.

For a domain D with quotient field K, we let, as usual, $\mathrm{Int}(D)$ be the *ring of integer-valued polynomials on* D, that is

$$\mathrm{Int}(D) = \{f \in K[X] \mid f(D) \subseteq D\}.$$

We are interested in *Newton* and *Schinzel sequences.* Let us start with the first ones: they are the test sequences for integer-valued polynomials, that is,

Definition 1. Let D be a domain, with quotient field K and $\{u_n\}_{n\geq 0}$ be a sequence in D. We say that $\{u_n\}_{n\geq 0}$ is a *Newton sequence* if, for each $n \geq 0$ and each polynomial $f \in K[X]$ of degree $d \leq n$,

$$f \in \mathrm{Int}(D) \Longleftrightarrow \forall j \leq n, f(u_j) \in D.$$

If D is endowed with an infinite Newton sequence we say that D is a *Newtonian domain.*

It is easy to see that the sequence $\{n\}_{n\geq 0}$ of natural integers is a Newton sequence of $\mathbb{Z}$, and hence, that $\mathbb{Z}$ is a Newtonian domain. Yet no number field K (other than $\mathbb{Q}$) is known to be such that the the ring of integers $\mathcal{O}_K$ of K is Newtonian. Another approach is the following.

Recall, following M. Bhargava [4, 5], that for a maximal ideal $\mathfrak{P}$ of a Dedekind domain D, a $\mathfrak{P}$-ordering of D is a sequence $\{u_n\}_{n\geq 0}$ in D such that, u_0 being arbitrarily chosen, u_n is inductively defined by the condition

$$v_{\mathfrak{P}}\left(\prod_{k=0}^{n-1}(u_n - u_k)\right) = \inf_{x\in D} v_{\mathfrak{P}}\left(\prod_{k=0}^{n-1}(x - u_k)\right), \tag{1.1}$$

where $v_{\mathfrak{P}}$ is the valuation associated to $\mathfrak{P}$. For a valuation domain with maximal ideal $\mathfrak{P}$, it is immediate that a $\mathfrak{P}$-ordering is nothing else than a Newton sequence.

In a Dedekind domain D, a Newton sequence is then a *simultaneous ordering*, that is, a $\mathfrak{P}$-ordering for every maximal ideal of D [8]. M. Wood actually proved, in particular, that the ring of integers of an imaginary quadratic field is never endowed with a simultaneous ordering [16, Theorem 5.2].

Text presented during the meeting “Third International Meeting on Integer-Valued Polynomials” organized by Sabine Evrard. 29 novembre-3 décembre 2010, C.I.R.M. (Luminy).
2000 *Mathematics Subject Classification.* 13F20,11R58.

[1]This paper was presented by Paul-Jean Cahen.

As noted by J. Yeramian [17], a $\mathfrak{P}$-ordering $\{u_n\}_{n\geq 0}$ is nothing else than a *very well ordered sequences* of Y. Amice [3]: letting q be the norm of $\mathfrak{P}$ then, for each s, and each k, the q^k consecutive elements $\{u_{sq^k}, u_{sq^k+1}, \ldots, u_{(s+1)q^k-1}\}$ form a complete system of representatives of $\mathcal{O}_K$ modulo $\mathfrak{P}^k$ [8, Proposition 3.9].

This question is then related to Schinzel's problem [13, Problem 8]: given a number field K, is there a sequence $\{u_n\}_{n\geq 0}$ in the ring of integers $\mathcal{O}_K$ such that, for each ideal I with norm $N = N(I)$, the first N terms of the sequence $\{u_n\}_{n\geq 0}$ represent all residue classes modulo I? We shall call such a sequence $\{u_n\}_{n\geq 0}$ a *Schinzel sequence*.

As for Newton sequences, the sequence of natural integers clearly gives a positive answer for $\mathbb{Z}$ but no number field K is known to have this property (in fact, the question was first raised by J. Browkin in 1965 for $\mathbb{Q}[i]$ with already a negative answer provided by E.G. Strauss in 1966). In the same direction, B. Wantula [14] showed the answer again to be negative for all quadratic number fields with seven possible exceptions, J. Latham [11] proved the same for cubic fields with a negative discriminant, again with at most finitely many exceptions, and so did R. Wasen [15] for pure extensions of prime degree. But also, Wasen characterized the Schinzel sequences $\{u_n\}_{n\geq 0}$ by a condition on the norm of the difference of two terms of the sequence. We shall take this condition as the general definition of Schinzel sequences, for a domain D, letting the *norm* $N(I)$ of an ideal I of D, possibly infinite, to be the cardinality of the quotient D/I and the *norm* $N(a)$ of an element $a \in D$ to be the norm of the principal ideal aD.

Definition 2. Let D be a domain, with quotient field K and $\{u_n\}_{n\geq 0}$ be a sequence of D. We say that $\{u_n\}_{n\geq 0}$ is a *Schinzel sequence* if,

$$\text{for } i \neq j,\ N(u_i - u_j) \leq \max(i, j).$$

If D is endowed with an infinite Schinzel sequence we say that D is a *Schinzel domain*.

(But as Wasen indexed a sequence from u_1, he wrote $N(u_i - u_j) < \max(i, j)$).

In this talk we investigate Newton and Schinzel sequences in the ring of integers of a global field K, that is, either a number field or an algebraic extension of a function field $\mathbb{F}_q(T)$. We say that a K is a *Newtonian* or a *Schinzel field* if the corresponding ring of integers $\mathcal{O}_K$ is a Newtonian or a Schinzel domain (for a function field, $\mathcal{O}_K$ is the integral closure of $\mathbb{F}_q[T]$).

In the case of a function field, $\mathbb{F}_q[T]$ is endowed, similarly to $\mathbb{Z}$, with a sequence $\{a_n\}$, the *Car sequence* [9], that is both a Newtonian and Schinzel ordering: letting $a_0 = 0, a_1 = 1, \ldots, a_{q-1}$ be the elements of $\mathbb{F}_q$, and $n = n_0 + n_1 q + \ldots + n_s q^s$ be the q-adic expansion of n, $a_n = a_{n_0} + a_{n_1}T + \ldots + a_{n_s}T^s$. Unlike the case of number fields, there are obvious cases where an algebraic extension K of $\mathbb{F}_q(T)$ is both a Newtonian and a Schinzel field: for instance, if $K = \mathbb{F}_q(\sqrt{T})$ then $\mathcal{O}_K = \mathbb{F}_q[\sqrt{T}]$ is clearly isomorphic to $\mathbb{F}_q[T]$, and the same holds for $K = \mathbb{F}_{q^2}(T)$, with $\mathcal{O}_K = \mathbb{F}_{q^2}[T]$. Yet, we conjecture there are no Newtonian or Schinzel function field other than these trivial cases.

As there are likely no infinite Schinzel or Newton sequence, we investigate the maximal length of such sequences with the following natural definition for sequences of finite length.

Definition 3. Let $\{u_0, \ldots, u_L\}$ be a sequence of length L in the domain D.

(1) We say that $\{u_n\}_{n\geq 0}$ is a *Newton sequence* if, for each polynomial $f \in K[X]$ of degree $n \leq L$,

$$f \in \mathrm{Int}(D) \iff \forall j \leq n, f(u_j) \in D.$$

(2) We say that $\{u_n\}_{n\geq 0}$ is a *Schinzel sequence* if,

$$\text{for } i \neq j,\ N(u_i - u_j) \leq \max(i, j).$$

In fact, we restrict our attention to quadratic extensions. In a first part we shall investigate the maximal length for a Newton or Schinzel sequence in the ring of integers of a quadratic number field $K = \mathbb{Q}(\sqrt{d})$. Some computations were performed by computer on the cluster Gaia of Paris 13 with the software of formal calculus Pari/GP [12]. In the second and last part, we investigate the case of quadratic function fields.

In all cases, as noted in [6, 8], if $\{u_n\}_{n\geq 0}$ is either a Newton or a Schinzel sequence of a domain D, then so is the sequence $\{au_n + b\}$, for each unit a and each $b \in D$. We shall thus always assume that $u_0 = 0$ and $u_1 = 1$. And in many cases, we shall see that the longest Schinzel or Newton sequence is but the sequence $\{0, 1\}$!

2. Maximal lengths of sequences in quadratic number fields

In this section we consider a quadratic number field $K = \mathbb{Q}(\sqrt{d})$, assuming as usual that d is a square-free integer and denote by $\mathcal{O}_K$ its ring of integers. Recall that for $x = \alpha + \beta\sqrt{d}$ in K, the *relative norm* of x is $N_{K/\mathbb{Q}}(x) = \alpha^2 - d\beta^2$ and that, for $x \in \mathcal{O}_K$, $|N_{K/\mathbb{Q}}(x)| = N(x)$, the *absolute norm* of x, is the cardinality of $\mathcal{O}_K/x\mathcal{O}_K$. We denote respectively by $m(d)$ and $n(d)$ the maximal length of a Schinzel and a Newton sequence in $\mathcal{O}_K$.

2.1. Schinzel sequences.

Here is our main result.

Theorem 4. *Let $K = \mathbb{Q}(\sqrt{d})$. Then, $m(d) = 1$, except for seven cases, with the following values:*

d	**-7**	**-3**	**-1**	**2**	**3**	**5**	**17**
$m(d)$	**2**	**11**	**3**	**5**	**5**	**17**	**3**

The fact that $m(d) = 1$, but for 7 cases, is essentially due to B. Wantula [14], yet he wrote in Polish and we thought it might be useful to translate (and rewrite) the proof in English. Moreover, his list of exceptions, in his introduction, contains $d = -5$ instead of $d = 5$, and although it is clear from the body of the paper that this is a typo, the wrong list is to be found in the review by Witold Wieslaw [MR0369314]. We sketch the proof that there are only 7 exceptional cases.

Proof. As we assume that $u_0 = 0$ and $u_1 = 1$, a sequence of length $L > 1$ is of the form $\{0, 1, \alpha, \ldots\}$. We then derive easily from Definition 3 that $N(\alpha) \leq 2$ and $N(\alpha - 1) \leq 2$ in particular, $\alpha \notin \mathbb{Z}$. Write $\alpha = \frac{a+b\sqrt{d}}{2}$, with $a, b \in \mathbb{Z}, b \neq 0$.

- In the imaginary case (that is, $d < 0$), it is enough to use the first condition to derive the diophantine inequality
$$a^2 + |d|b^2 \leq 8.$$
Thus $|d| \leq 8$, in fact $|d| \leq 7$, as d is square-free.
- In the real case (that is, $d > 0$), using both conditions, we have
$$-8 \leq a^2 - db^2 \leq 8 \text{ and } -8 \leq (a-2)^2 - db^2 \leq 8.$$
By substraction, we obtain $-3 \leq a \leq 5$ which in turn implies
$$d \leq db^2 \leq 8 + \inf\{a^2, (a-2)^2\} = 17.$$

A little more work allows to narrow to 7 exceptional cases. □

To compute the maximal length of a Schinzel sequence, we can also use the following, due to Sophie Frisch [6, Corollary 1.12].

Proposition 5. *Let D be a domain. If there exists a Schinzel sequence of length L in D then every ideal I of D with norm $N(I) \leq L$ is principal.*

In particular, a Schinzel domain is principal (in fact, Sophie Frisch showed that a Schinzel domain with finite residue rings is Euclidean for the norm).

For $d = -7, -3, -1$, a case by case argumentation allows to conclude. In the real case, as the units provide infinitely many element with norm 1, we had to use a computer. The computations were performed on the cluster Gaia of Paris 13, using the software of formal calculus Pari/GP [12].

2.2. Newton sequences.

We can link Newton sequences to Schinzel sequences with the following from [6, Corollary 4.12].

Proposition 6. *Let D be a Dedekind domain and n an integer. If there is at most one prime ideal $\mathfrak{P}$ of D with norm $N(\mathfrak{P}) \leq n$, then every Newton sequence of length $L \leq n$ in D is also a Schinzel sequence.*

In particular, if $d \not\equiv 1 \pmod 8$, then 2 is non split in $K = \mathbb{Q}(\sqrt{d})$ and it follows that a Newton sequence of length 2 in the ring of integers $\mathcal{O}_K$ is also a Schinzel sequence. Thus $n(d) = 1$, except in the five cases (among seven), given in Theorem 4, where $d \not\equiv 1 \pmod 8$.

For the case $d \equiv 1 \pmod 8$, recall that $\{0, 1, \ldots, m_K - 1\}$ is always a Newton sequence of $\mathcal{O}_K$ contained in $\mathbb{Z}$, where m_K denotes the least non splitting prime in K, and there are no longer Newton sequences contained in $\mathbb{Z}$ [16, Proposition 4.3]. M. Wood could prove that, in the imaginary case, there are no longer Newton sequences of $\mathcal{O}_K$, wether contained in $\mathbb{Z}$ or not [16, Theorem 5.2]. In the paper we are presenting here, we proved the same in the real case, for d large enough. We can summarize our results as follows.

Theorem 7. *Let $K = \mathbb{Q}(\sqrt{d})$.*

(1) *For $d \not\equiv 1 \pmod 8$, then $n(d) = 1$, except for five case with the following values*

d	**-3**	**-1**	**2**	**3**	**5**
$n(d)$	**4**	**3**	**4**	**5**	**6**

(2) *For $d \equiv 1 \pmod 8$, denoting by m_K the least non splitting prime in K, then $n(d) \geq m_K - 1$. Moreover $n(d) = m_K - 1$ in the imaginary case and for d larger than a constant $D > 0$ in the real case.*

The principle of the proof for the real case is similar to M. Wood argument in the imaginary case. We first show that, for d large enough and some function $f(d)$ of d, every Newton sequence (beginning with 0 and 1) of length $L \leq f(d)$ is contained in $\mathbb{Z}$. We then derive a bound for m_K from a result by Granville et al. [10]:

Lemma 8. *Let $K = \mathbb{Q}(\sqrt{d})$. For each $\lambda > \frac{1}{4\sqrt{e}}$, there exists a constant $C_\lambda > 0$ such that for $d > C_\lambda$, $m_K < d^\lambda$.*

We then show that, for d large enough again, $m_K \leq f(d)$. A Newton sequence of length m_K would thus be contained in $\mathbb{Z}$, contradicting [16, Proposition 4.3].

Remarks. 1) For $d \not\equiv 1 \pmod 8$, 2 is either ramified or inert, thus $m_K = 2$ and we could also say that $n(d) = m_K - 1$, as for $d \not\equiv 1 \pmod 8$.
2) In [10] the authors note that the constant $C_\lambda > 0$ is probably enormous, well beyond the range of computation.
3) Contrarily to $m(d)$, we see that $n(d)$ can be arbitrarily large, since this is the case for the least non splitting prime m_K.
4) -7 and 17 are special cases for Schinzel sequences, not for Newton sequences. The case $d = 17$ could be among the real exceptions such that $n(d) > m_K - 1$ (if any) but the computation shows that $n(17) = 4 = m_K - 1$ ($m_K = 5$, as 2 and 3 are decomposed, but 5 is inert).

3. Function fields

We consider a quadratic extension K of a function field $\mathbb{F}_q(T)$. We always suppose the extension to be *geometric*, that is, $\mathbb{F}_q$ is algebraically closed in K. We denote by $\mathcal{O}_K$ the ring of integers of K, that is, the integral closure of $\mathbb{F}_q[T]$ in K.

Recall that a *place* of $\mathbb{F}_q(T)$ is a (rank one discrete) valuation of $\mathbb{F}_q(T)$, either the $(1/T)$-adic valuation, called the *infinite place*, or the P-adic valuation for some monic irreducible polynomial P of $\mathbb{F}_q[T]$. The *degree* of a place is the degree of the corresponding polynomial, the infinite place being of degree one. Places of degree n thus correspond to the valuations with residue field of cardinal q^n. Recall also that a quadratic extension K of $\mathbb{F}_q(T)$ is said to be *real* if the infinite place is split in K, and *imaginary* otherwise, that is, $\left(\frac{1}{T}\right)$ is inert or ramified in K.

An extension is said to be *rational* if it is of the form $K = \mathbb{F}_q(U)$ for some $U \in K$. In this case, we have the following:

Proposition 9. *Let K be a rational quadratic real extension of $\mathbb{F}_q(T)$. Then the ring of integers $\mathcal{O}_K$ is both a Schinzel and a Newtonian domain.*

3.1. **Newton sequences in real quadratic function fields.** In [1], we proved that if K is an imaginary quadratic extension of $\mathbb{F}_q(T)$, then K is never a Newtonian field unless $\mathcal{O}_K$ is $\mathbb{F}_q$-isomorphic to $\mathbb{F}_q[T]$. In the real case, if the extension is geometric as assumed throughout this paper, $\mathcal{O}_K$ is never isomorphic to $\mathbb{F}_q[T]$, as it admits infinitely many units, and we could show it is not Newtonian but for finitely many cases, similarly to Theorem 7 for real quadratic number fields. Here we denote by m_K the least degree of a place that is non split in K.

Theorem 10. *Assume q odd. There exists a constant $\mathcal{C} > 0$ such that, for any real quadratic geometric extension $K := \mathbb{F}_q(T)[\sqrt{U}]$ of $\mathbb{F}_q(T)$, with $U \in \mathbb{F}_q[T]$ and $\deg U > \mathcal{C}$, the longest length of a Newton sequence in K is $n_K = q^{m_K} - 1$.*

The pattern of the proof is similar to the case of a real number field, using a bound for m_K, similar to Lemma 8, thanks to results kindly communicated to us by M. Car. It follows there exist at most finitely many separable real quadratic Newtonian extensions of $\mathbb{F}_q(T)$, among which the rational real quadratic extensions of $\mathbb{F}_q(T)$ for which $d \leq 2$.

Similar results are obtained in the case of characteristic 2.

3.2. **Schinzel sequences in quadratic function fields.** Clearly, the elements of $\mathbb{F}_q$ form always both a Schinzel and Newton sequence. But we could prove, in the real case, that the longest length of Schinzel sequence is $q-1$ except for the "trivial" case where K is a Schinzel field. We also have the following link with Newton sequences.

Proposition 11. *Let K be a separable and geometric quadratic extension of $\mathbb{F}_q(T)$. If K is a Schinzel field then K is Newtonian.*

The converse holds in the imaginary case. We then end with two results, the first one is for the real case.

Proposition 12. *Let K be a separable and geometric real quadratic extension of $\mathbb{F}_q(T)$. The followings are equivalent.*

(1) *K is a Schinzel field.*
(2) *K is a rational extension of $\mathbb{F}_q(T)$.*

Moreover, if K is not a Schinzel field, the longest length of a Schinzel sequence in $\mathcal{O}_K$ is $q-1$.

The second and last result is for the imaginary case.

Proposition 13. *Let K be a separable geometric imaginary quadratic extension of $\mathbb{F}_q(T)$. The followings are equivalent.*

(1) *K is a Schinzel field,*
(2) *K is Newtonian,*
(3) *$\mathcal{O}_K$ is $\mathbb{F}_q$-isomorphic to $\mathbb{F}_q[T]$.*
(4) *K is a rational extension of $\mathbb{F}_q(T)$ and the place above $\left(\frac{1}{T}\right)$ is of degree 1.*

References

[1] D. Adam, Simultaneous orderings in function fields, *J. Number Theory* **112** (2005), 287–297.
[2] ———, Pólya and Newtonian function fields, *Manuscripta Math.* **126** (2008), no. 2, 231–246.
[3] Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964), 117–180.
[4] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.* **490** (1997), 101–127.
[5] ———, The factorial function and generalizations, *Amer. Math. Monthly* **107** (2000), 783–799.
[6] P.J. Cahen, Newtonian and Schinzel sequences in a domain, *J. of Pure and Appl. Algebra* **213** (2009), 2117–2133.
[7] P.J. Cahen, J.L. Chabert, Integer valued polynomials, *Mathematical Survey and Monographs*,vol **48**, American Mathematical Society, Providence, (1997)
[8] ———, Old Problems and New Questions around Integer-Valued Polynomials and Factorial Sequences, *Multiplicative ideal theory in commutative algebra*, Springer, New York, (2006), 89–108.
[9] M. Car, Répartition modulo 1 dans un corps de séries formelles sur un corps fini, *Acta Arith.* **69.3** (1995), 229–242.
[10] A. Granville, R.A. Mollin, H.C. Williams, An upper bound on the least inert prime in a real quadratic field, *Canad. J. Math.* **52.2** (2000), 369–380.
[11] J. Latham, On sequences of algebraic integers, *J. London Math. Soc.* **6.2** (1973), 555–560.
[12] PARI/GP, version `2.3.4`, Bordeaux, 2008, `http://pari.math.u-bordeaux.fr`.

[13] W. Narkiewicz, Some unsolved problems, *Colloque de Théorie des Nombres* (Univ. Bordeaux, Bordeaux, 1969), *Bull. Soc. Math. France, Mem.* **25** (1971), 12–02.

[14] B. Wantula, Browkin's problem for quadratic fields. (Polish) *Zeszyty Nauk. Politech. Ślpolhk ask. Mat.-Fiz.* **24** (1974), 173–178.

[15] R. Wasen, On sequences of algebraic integers in pure extensions of prime degree, *Colloq. Math.* **30** (1974), 89–104.

[16] M. Wood, P-orderings: a metric viewpoint and the non-existence of simultaneous orderings, *J. Number Theory* **99** (2003), 36–56.

[17] J. Yéramian, Anneaux de Bhargava, *Comm. Algebra* **32.8**, (2004), 3043–3069.

GAATI, Université de Polynésie Française, BP 6570, 98702 Faa'a, Tahiti, Polynésie Française •
david.adam@upf.pf

LATP, CNRS UMR 6632, Faculté des Sciences et Techniques, Université d'Aix-Marseille III, 13397 Marseille Cedex 20, France • paul-jean.cahen@univ-cezanne.fr