Computing with quadratic forms over number fields

Przemysław Koprowski

Faculty of Mathematics
University of Silesia
ul. Bankowa 14
PL-40-007 Katowice, Poland

Alfred Czogała

Faculty of Mathematics
University of Silesia
ul. Bankowa 14
PL-40-007 Katowice, Poland

Abstract

This paper presents fundamental algorithms for the computational theory of quadratic forms over number fields. In the first part of the paper, we present algorithms for checking if a given non-degenerate quadratic form over a fixed number field is either isotropic (respectively locally isotropic) or hyperbolic (respectively locally hyperbolic). Next we give a method of computing the dimension of an anisotropic part of a quadratic forms. The second part of the paper is devoted to algorithms computing two field invariants: the level and the Pythagoras number. Ultimately we present an algorithm verifying whether two number fields have isomorphic Witt rings (i.e. are Witt equivalent).

Key words: Algorithms, quadratic forms, number fields, level, Pythagoras number, Witt equivalence

Email addresses: pkoprowski@member.ams.org (Przemysław Koprowski), alfred.czogala@us.edu.pl (Alfred Czogała).

URLs: http://z2.math.us.edu.pl/perry/ (Przemysław Koprowski), http://www.math.us.edu.pl/czogala/ (Alfred Czogała).

1. Introduction

The algebraic theory of quadratic forms is a mature and important branch of mathematics. Yet still, the computational side of this theory is seriously under-developed. The majority of research concentrate on forms over the rationals. Consequently, while over $\mathbb{Q}$ there already a couple of algorithms for solving a highly non-trivial problem of determining isotropic vectors of a quadratic forms (see e.g. Cremona and Rusin (2003); Simon (2005); Castel (2013)), little has been done so far for forms over number fields (i.e. finite extensions of $\mathbb{Q}$). The algebraic theory of quadratic forms over number fields are very like the theory over the rationals, nevertheless the computational approach seems to be rudimentary here. The aim of this article is to partially fill this gap, as well as provoke further discussion and future research.

This paper is organized as follows: in Section 2 we present an algorithm (see Algorithm 5) checking if a given form (over a fixed number field K) is isotropic. This algorithm uses sub-procedures (Algorithms 2 and 3) deciding whether the form is isotropic at a non-archimedean prime of K (respectively odd or even). These two algorithm may be of an independent interest to the reader. Next, in Section 3 we show Algorithm 7 determining if a quadratic form is hyperbolic, again utilizing the local approach.

It is known that any non-degenerate form can be uniquely decomposed into an orthogonal sum of its anisotropic part and a hyperbolic form (one of these two parts may of course be void if the form in question is either anisotropic or hyperbolic itself). In Section 4 we shows a procedure computing the dimension of an anisotropic part of a quadratic form.

In Sections 5–7 we go a step further and develop algorithms computing invariants of the ground fields, that play important roles in the algebraic theory of quadratic forms. Algorithm 10 computes the level $s(K)$ of a number field K, which is the length of the shortest representation of -1 as a sum of squares. Another invariant of the field is the minimal number of squares needed to represent any sum of squares. This invariant is called the Pythagoras number and is computed by Algorithm 11.

Recall that the set WK of similarity classes of non-degenerate symmetric bilinear forms over a given base field K is a ring with operations induced by the orthogonal sum and the tensor product. It is called the *Witt ring* of the field K. Because a bilinear form defines an orthogonal geometry on the vector space on which it is defined, thus the Witt ring can be viewed as an algebraic structure encoding information on all possible orthogonal geometries over a given base field. Two fields are said to be *Witt equivalent*, if their Witt rings are isomorphic. The set of global field invariants that fully determine its Witt equivalence class was described in Szymiczek (1991). In Section 7 we present Algorithm 13 computing all these invariants. In particular the algorithm may be used to verify whether two number fields are Witt equivalent.

The authors implemented all the algorithms presented in this paper in a computer algebra system Sage. Using this implementation, we were able to find representatives of Witt classes of number fields of low degrees. These results are presented in Tables A.1–A.4. Moreover, using our implementation, we were able to give an affirmative answer to Conner's question for number field of degree not exceeding 6 (for details see the last section of the paper).

In these paper, $K = \mathbb{Q}(\vartheta)$ is always a number field specified by the minimal polynomial of ϑ over $\mathbb{Q}$ and $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. Two basic building blocks that we

use in subsequent algorithms are procedures that test whether a given algebraic number $a \in K$ is a square: either in its base field K or in a completion $K_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime of K. A procedure testing whether an element is a square in a number field is available as standard in computer algebra systems. On the other hand, testing whether a is a square in a completion $K_{\mathfrak{p}}$ is obviously equivalent to testing whether $x^2 - a$ is irreducible in $K_{\mathfrak{p}}[x]$. There are known algorithms for testing irreducibility of a polynomial in local fields. These include for example: Montes' algorithm (see e.g. Veres (2009) or Guàrdia et al. (2011, 2012)) or variations of Zassenhaus Round Four algorithm (see e.g. Pauli (2001, 2010)).

In the algorithms presented below, an input is a non-degenerate diagonal quadratic form with coefficients in some number field K. Since K is the field of fractions of $\mathcal{O}_K$ and for every $a, b \in \mathcal{O}_K$, both a/b and $a \cdot b$ belong to the same square-class on $\dot{K}/\dot{K}^2$, hence in Algorithms 1–9 we usually assume that the coefficients of the quadratic form come from $\mathcal{O}_K$.

2. Isotropy of a quadratic form

In this section, we present an algorithm that checks if a given form φ over a number field K is isotropic or not. The organization of this section reflects the general idea of solving the problem locally. Hence, Algorithms 2, 3 and 4 deal respectively with odd and even finite fields and real infinite primes of K. Finally, Algorithm 5 checks if the form is globally isotropic, using the above-mentioned algorithms as sub-procedures.

Below we utilize the notion of the discriminant of a quadratic form. Recall (see e.g. (Szymiczek, 1991, Definition 15.2.1)) that for a quadratic form φ, we define the discriminant of φ by the formula

$$\operatorname{disc} \varphi := (-1)^{d(d-1)/2} \det \varphi,$$

where $d = \dim \varphi$.

Algorithm 1. Let $\mathfrak{p}$ be an odd prime of K and $\varphi = \langle a_1, \ldots, a_d \rangle$ be a non-degenerate diagonal quadratic form with all its entries being $\mathfrak{p}$-adic units. This algorithm returns true if and only if the residual form $\varphi \otimes K/\mathfrak{p}$ is isotropic, otherwise it returns false.

(1) If $\dim \varphi = 1$, return false.
(2) If $\dim \varphi = 2$, return true when $\operatorname{disc} \varphi$ is a square in $K/\mathfrak{p}$, otherwise return false.
(3) If $\dim \varphi > 2$, return true.

The correctness of the above algorithm follows immediately from (Lam, 2005, Theorem I.3.2).

Algorithm 2. Let $\mathfrak{p}$ be an odd prime of a number field K. Given a non-degenerate quadratic form φ, this algorithm returns true if $\varphi \otimes K_{\mathfrak{p}}$ is isotropic and false otherwise.

(1) If $\dim \varphi = 1$, return false.
(2) If $\dim \varphi \geq 5$, return true.
(3) Let $\{a_1, \ldots, a_d\}$ be the list of coefficients of a diagonalization of φ, all $a_i \in \mathcal{O}_K$. Partition this list into two sublists depending on the parity of the $\mathfrak{p}$-adic valuation:

$$\varphi_0 := \left\{ a_i \cdot \pi^{-\operatorname{ord}_{\mathfrak{p}} a_i} \;\middle|\; \operatorname{ord}_{\mathfrak{p}} a_i \equiv 0 \pmod 2 \right\},$$
$$\varphi_1 := \left\{ a_i \cdot \pi^{-\operatorname{ord}_{\mathfrak{p}} a_i} \;\middle|\; \operatorname{ord}_{\mathfrak{p}} a_i \equiv 1 \pmod 2 \right\}.$$

Here π is a uniformizer of $\mathfrak{p}$ (see Remark 1 below).

(4) Use Algorithm 1 to verify whether any of φ_0, φ_1 is isotropic over $K/\mathfrak{p}$. Return true if Algorithm 1 returned true at least once, otherwise return false.

Remark 1. In order to find a uniformizer of a given prime in step (3) of the above algorithm, one may use for example (Cohen, 1993, Algorithm 4.8.17) or (Guàrdia et al., 2013, §3).

The correctness of the algorithm follows from (Lam, 2005, Proposition VI.1.9). Next, we consider even primes. Recall (see e.g. (Lam, 2005, Definition V.3.17)) that the Hasse invariant of a quadratic form $\varphi = \langle a_1, \ldots, a_d \rangle$ at a prime $\mathfrak{p}$ is:

$$s_{\mathfrak{p}}(\varphi) := \prod_{1 \leq i < j \leq d} (a_i, a_j)_{\mathfrak{p}}, \tag{1}$$

where $(a_i, a_j)_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic Hilbert symbol. An algorithm for computing the Hilbert symbol in a completion of a number field was recently presented in Voight (2013). We use it to verify whether a quadratic form is isotropic over a dyadic completion of K.

Algorithm 3. Let $\mathfrak{d}$ be an even prime of K and φ be a non-degenerate quadratic form over K. This algorithm returns true if and only if $\varphi \otimes K_{\mathfrak{d}}$ is isotropic, otherwise it returns false.

(1) If $\dim \varphi \leq 1$, then return false and quit.
(2) If $\dim \varphi = 2$, then check whether $\operatorname{disc} \varphi$ is a square in $K_{\mathfrak{d}}$. If so, then return true and quit, otherwise return false and quit.
(3) If $\dim \varphi = 3$, then proceed as follows:
   (a) Compute the Hilbert symbol $\big(-1, -\det(\varphi)\big)_{\mathfrak{d}}$ by applying (Voight, 2013, Algorithm 6.6).
   (b) Use Eq. (1) and (Voight, 2013, Algorithm 6.6) to compute the Hasse invariant $s_{\mathfrak{d}}(\varphi)$ of φ at $\mathfrak{d}$.
   (c) If $\big(-1, -\det(\varphi)\big)_{\mathfrak{d}} = s_{\mathfrak{d}}(\varphi)$, then return true otherwise return false
(4) If $\dim \varphi = 4$, then proceed as follows:
   (a) Check if $\det \varphi$ is a square in $K_{\mathfrak{d}}$. If not, then return true and quit.
   (b) If $\det \varphi \in (K_{\mathfrak{d}}^{\times})^2$, then use Eq. (1) and (Voight, 2013, Algorithm 6.6) to compute the Hasse invariant $s_{\mathfrak{d}}(\varphi)$ and the Hilbert symbol $(-1, -1)_{\mathfrak{d}}$. Return true if they are equal, return false if they are not.
(5) If $\dim \varphi \geq 5$, then return true.

Proof of correctness. An unary form is never isotropic and a quintic or higher-dimensional form over a dyadic field is always isotropic by the means of (Lam, 2005, Theorem VI.2.12). This justifies steps (1) and (5). Next, it is well known that a binary form is isotropic if and only if its determinant is a minus square, which proves step (2). On the other hand, if the form has dimension three, then (Lam, 2005, Proposition V.3.22) asserts that it is isotropic if and only if $\big(-1, -\det(\varphi)\big)_{\mathfrak{d}} = s_{\mathfrak{d}}(\varphi)$.

This leaves us with quaternary forms. Now, (Lam, 2005, Corollary VI.2.15) asserts that over a local field there is only one anisotropic form of dimension 4 and its determinant is a square. Thus, if $\det \varphi \notin (K_{\mathfrak{d}}^{\times})^2$, then $\varphi \otimes K_{\mathfrak{d}}$ is necessarily isotropic. On the other hand, if $\det \varphi \in (K_{\mathfrak{d}}^{\times})^2$, then (Lam, 2005, Proposition V.3.23) provides us with a needed criterion for isotropy. □

After covering the finite primes we need a tool do deal with the infinite ones, as well. Recall (see e.g. (Lam, 2005, p. 34)), that the *signature* of a non-degenerate quadratic form φ with respect to an ordering β of the coefficient field is the difference between the number of positive and negative entries of a diagonalization $\langle a_1, \ldots, a_d \rangle$ of φ:

$$\operatorname{sgn}_\beta(\varphi) := \sharp\{a_i \mid a_i >_\beta 0\} - \sharp\{a_i \mid a_i <_\beta 0\}.$$

This number is known to be independent of a choice of an actual diagonalization of φ. We now present an algorithm computing the signatures of the form with respect to all orderings of K.

Algorithm 4. Let $\mathbb{Q}(\vartheta)$ be a number field, specified by a minimal polynomial $f \in \mathbb{Q}[x]$ of its generator ϑ. Given a non-degenerate diagonal quadratic form $\varphi = \langle a_1, \ldots, a_d \rangle$ with coefficients in $\mathcal{O}_K$, this algorithm computes the list of signatures of φ with respect to all orderings of K.

(1) Use (Basu et al., 2003, Algorithm 10.64) to find a list $(\sigma_1, \ldots, \sigma_r)$ of Thom encodings of all real roots of $x_1 < \cdots < x_r$ of the generating polynomial f;
(2) For every coefficient a_i of φ proceed as follows:
   (a) Let $g_0, \ldots, g_{n-1} \in \mathbb{Q}$ be the coordinates of a_i with respect to the power basis $\{1, \vartheta, \ldots, \vartheta^{n-1}\}$ (i.e. $a_i = g(\vartheta)$ with $g = g_0 x + \cdots + g_{n-1}x^{n-1} \in \mathbb{Q}[x]$).
   (b) Use (Basu et al., 2003, Algorithm 10.67) to determine the signs:

$$s_{i1} = \operatorname{sgn} g(x_1), \ldots, s_{ir} = \operatorname{sgn} g(x_r)$$

   of the polynomial g at the roots of f.
(3) Return the list of sums $\left(\sum_{i=1}^d s_{i1}, \ldots, \sum_{i=1}^d s_{ir}\right)$.

The correctness of the algorithm follows immediately from the correctness of (Basu et al., 2003, Algorithms 10.64 and 10.67).

Remark 2. The above algorithm is used subsequently in step (3) of Algorithms 5, 7 and step (1) of Algorithm 9. As an alternative approach, one could use here an interval arithmetic and evaluate the signs of $\left(g_j(\vartheta_i)\right)$ by the means of (Mishra, 1993, §8.5, Sign evaluation).

Remark 3. In algorithms 5, 7, 9, 10 and 11 below, we need to perform factorizations of two kinds. The first one is to find all even primes of a given field K, i.e. to factor $2\mathcal{O}_K$. The other one is to find all primes dividing any of the coefficients of a given quadratic form. The factorization of an ideal in a number field corresponds to the factorization of a polynomial in a local field (see a comment at the end of the introduction). Algorithms for the factorization of ideals are known and described in computational algebraic number theory literature. One may refer for example to (Cohen, 1993, §6.2.5) and (Cohen, 2000, 2.3.22) or to a newer algorithm described in (Guàrdia et al., 2013, §2.2).

Now, we are finally ready to present the main algorithm of this section, that checks if a form is isotropic over a given number field.

Algorithm 5. Given a non-degenerate diagonal quadratic form $\varphi = \langle a_1, \ldots, a_d \rangle$ over K with $a_i \in \mathcal{O}_K$, this algorithm returns true if and only if φ is isotropic and false if it is not.

(1) If $\dim \varphi \leq 1$, then return false and quit.

(2) If $\dim \varphi = 2$, then check if $\operatorname{disc} \varphi$ is a square in K. If so, then return false; if not, return true.
(3) Use Algorithm 4 to compute the list $(s_1, \ldots, s_r)$ of the signatures of φ under all real embeddings of K. If $|s_j| = \dim \varphi$ for any $1 \leq j \leq r$, then return false and quit.
(4) Factor $2\mathcal{O}_K$ into prime ideals $2\mathcal{O}_K = \mathfrak{d}_1^{e_1} \cdots \mathfrak{d}_n^{e_n}$ in $\mathcal{O}_K$ (see Remark 3). For each $\mathfrak{d}_i$ use Algorithm 3 to check if $\varphi \otimes K_{\mathfrak{d}_i}$ is isotropic. If the algorithm returns false, for at least one $\mathfrak{d}_i$, then return false and quit.
(5) Find all odd primes $\mathfrak{p}$ of K dividing any of the coefficients a_i of φ. For each such a prime $\mathfrak{p}$ call Algorithm 2. If the procedure returns false at least once, then return false and quit.
(6) Return true.

Proof of correctness. The cases of unary and binary forms are trivial. For forms of higher dimension we use the local-global principle (Lam, 2005, Principle VI.3.1). The form is isotropic over K if and only if it is isotropic over all the completions of K. Now φ, having dimension at least three, is trivially isotropic at all odd primes that do not divide any of the coefficients. These are almost all primes of K. Thus, we are left with only finitely many cases to check: finitely many real places treated in step (3), finitely many dyadic places covered by step (4) and finitely many non-dyadic primes considered in step (5). □

3. Hyperbolicity of a quadratic form

In this section we present an algorithm checking another fundamental property of a quadratic form, namely whether it is hyperbolic (hence, a zero element in the Witt group). The general idea is similar to the one adopted in the previous section. Again, we treat the problem locally, separately for finite and real infinite primes of K.

Algorithm 6. Let $\mathfrak{p}$ be a finite prime of a number field K (either even or odd). Given a non-degenerate quadratic form φ, this algorithm returns true if the form $\varphi_{\mathfrak{p}} := \varphi \otimes K_{\mathfrak{p}}$ is hyperbolic and false otherwise.
(1) If $\dim \varphi$ is odd, then return false and quit.
(2) Compute the discriminant $\operatorname{disc} \varphi$ and check if it is a square in the completion $K_{\mathfrak{p}}$. If it is not a square, then return false and quit.
(3) Use Eq. (1) and (Voight, 2013, Algorithm 6.6) to compute the Hasse invariant $s_{\mathfrak{p}}(\varphi)$ and the power $(-1,-1)_{\mathfrak{p}}^{m(m-1)/2}$ of $\mathfrak{p}$-adic Hilbert symbol, where $2m = \dim \varphi$. Return true if they are equal, return false if they are not.

Proof of correctness. Take a form φ of an even dimension. If the discriminant $\operatorname{disc} \varphi$ is a square in $K_{\mathfrak{p}}$ and the Hasse invariant $s_{\mathfrak{p}}(\varphi)$ equals $(-1,-1)_{\mathfrak{p}}^{m(m-1)/2}$, then φ is isometric to the hyperbolic space $m\langle 1, -1\rangle$ by (Lam, 2005, Proposition V.3.25). □

Algorithm 7. Given a non-degenerate diagonal quadratic form $\varphi = \langle a_1, \ldots, a_d\rangle$ over K with $a_i \in \mathcal{O}_K$, this algorithm returns true if and only if φ is hyperbolic, otherwise it returns false.
(1) If $\dim \varphi$ is odd, then return false and quit.
(2) Compute the discriminant $\operatorname{disc} \varphi$. Check if $\operatorname{disc} \varphi$ is a square in K. If it is not, then return false.

(3) Use Algorithm 4 to compute the list $(s_1, \ldots, s_r)$ of the signatures of φ under all real embeddings of K. If $s_j \neq 0$ for any $1 \leq j \leq r$, then return false and quit.
(4) Let $\mathcal{L}$ be the set consisting of all odd primes of K dividing any of the coefficients a_i of φ and of all even primes of K.
(5) Apply Algorithm 6 to every $\mathfrak{p} \in \mathcal{L}$ to check if $\varphi \otimes K_\mathfrak{p}$ is hyperbolic. If it returns false, for at least one $\mathfrak{p}$, then return false and quit.
(6) Return true.

Proof of correctness. It is well known that the discriminant of a hyperbolic form is a square and its dimension has to be even. Moreover, by the well known Weak Hasse Principle, a quadratic form is hyperbolic over a number field if and only if it is hyperbolic over every completion (finite or real infinite) of the field. Over the reals, the form is hyperbolic, when its signature is null. This proves that the algorithm returns true for all hyperbolic forms.

Conversely, suppose that the algorithm returns true for some non-degenerate form φ. Thus, $\dim \varphi$ is even, its discriminant is a square an it has a zero signature with respect to every ordering of K.

Recall that a quadratic form over a non-dyadic local field $K_\mathfrak{p}$ decomposes into a sum $\varphi \cong \varphi_1 \perp \pi \cdot \varphi_2$, where π is a $\mathfrak{p}$-adic uniformizer and the coefficients of φ_1, φ_2 are $\mathfrak{p}$-adic units. Recall (see e.g. (Lam, 2005, § VI.1)) that a map $\varphi \mapsto \varphi_2 \otimes ({}^K\!/_\mathfrak{p})$ is a well defined homomorphism of Witt groups (i.e. additive groups of Witt rings) $WK_\mathfrak{p} \to W({}^K\!/_\mathfrak{p})$ called the *second residue homomorphism*.

If the second residual homomorphisms with respect to all odd primes of K are null, then the Witt class of φ sits in $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ by (Milnor and Husemoller, 1973, Corollary IV.4.5), where $\mathfrak{N}(W\mathcal{O}_K)$ denotes the nilradical of the Witt ring of $\mathcal{O}_K$ and IK is the fundamental ideal of the Witt ring WK. Clearly one needs to check only these primes that divide any of the coefficients of φ as we do in step (4). Since our algorithm returns true for the form φ, hence in particular $\varphi \otimes K_\mathfrak{d}$ is hyperbolic, and so $c_\mathfrak{d}(\varphi) = 1$, for every even prime $\mathfrak{d}$ of K. Here

$$c_\mathfrak{d}(\varphi) = (-1,-1)_\mathfrak{d}^{m(m-1)/2} s_\mathfrak{d}(\varphi), \qquad m = \frac{1}{2}\dim\varphi$$

is the Hasse-Witt invariant of φ (c.f. (Lam, 2005, Proposition V.3.20). Now, the map $\varphi \mapsto \big(c_{\mathfrak{d}_1}(\varphi), \ldots, c_{\mathfrak{d}_{g-1}}(\varphi)\big)$ is an isomorphism from $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ onto $\{\pm 1\}^{g-1}$, where $\mathfrak{d}_1, \ldots, \mathfrak{d}_g$ are all the dyadic primes of K, by (Czogała, 2001, Proposition 3.5). It follows that the class of φ in WK is null, hence φ is a hyperbolic form. □

4. Witt index of a quadratic form

Recall (see e.g. (Lam, 2005, Chapter i, §4)) that any non-degenerate quadratic form φ can be uniquely (up to an isometry) decomposed as $\varphi = \psi \perp H$, where ψ is an anisotropic form, called the *anisotropic part* of φ and H is hyperbolic. The number of hyperbolic planes constituting H (i.e. half of the dimension of H) is called the *Witt index* of φ and denoted $\operatorname{ind}(\varphi)$. In this section we present an algorithm that computes the dimension of the anisotropic part of φ. It can be also used to deduce the Witt index since clearly $\operatorname{ind}\varphi = {}^1\!/_2 \cdot (\dim\varphi - \dim\psi)$. Again, the problem is first solved locally (see Algorithm 8) and then the local solution is used to derive the global one in Algorithm 9.

Algorithm 8. Given a non-degenerate quadratic form φ over a number field K and a finite prime $\mathfrak{p}$, this algorithm computes the dimension of the anisotropic part of $\varphi_\mathfrak{p} := \varphi \otimes K_\mathfrak{p}$ over the completion $K_\mathfrak{p}$.

(1) If $\dim \varphi$ is even, proceed as follows:
   (a) Use Algorithm 6 to check if $\varphi_\mathfrak{p}$ is hyperbolic. If it is, then return 0 and quit.
   (b) Check if $\operatorname{disc} \varphi$ is a square in $K_\mathfrak{p}$. If so, then return 4 and quit.
   (c) Return 2.

(2) If $\dim \varphi$ is odd, proceed as follows:
   (a) Let $d := \dim \varphi$ and take $\psi := \varphi \perp \langle (-1)^{d(d+1)/2} \cdot \det \varphi \rangle$.
   (b) Use Algorithm 6 to check if $\psi \otimes K_\mathfrak{p}$ is hyperbolic. If it is, then return 1 and quit.
   (c) Return 3.

Proof of correctness. First assume that φ is an even-dimensional form, so $\varphi_\mathfrak{p} \in IK_\mathfrak{p}$. If it is not hyperbolic, then its class in the Witt ring $WK_\mathfrak{p}$ is not zero. Suppose that $\operatorname{disc} \varphi$ is a square in $K_\mathfrak{p}$. It follows that $\varphi_\mathfrak{p} \in I^2K_\mathfrak{p}$. But for a local field there is only one non-zero element of $I^2K_\mathfrak{p}$, namely the form $\eta_\mathfrak{p} = \langle 1, u, \pi, u\pi \rangle$, here u is a $\mathfrak{p}$-adic unit such that $K_\mathfrak{p}(\sqrt{u})$ is the unique unramified extension of $K_\mathfrak{p}$ (see (Lam, 2005, Corollary VI.2.15)). It follows that the anisotropic part pf $\varphi_\mathfrak{p}$ has dimension 4. Conversely, suppose that $\operatorname{disc} \varphi$ is not a square in $K_\mathfrak{p}$. Therefore $\varphi_\mathfrak{p} \in IK_\mathfrak{p} \setminus I^2K_\mathfrak{p}$ and so the anisotropic part of $\varphi_\mathfrak{p}$ has dimension 2.

Now assume that the dimension of φ is odd. Hence, the form ψ constructed in step (2a) is an even dimensional form and its discriminant is a square in $K_\mathfrak{p}$. Consequently, the Witt class of $\psi_\mathfrak{p} := \psi \otimes K_\mathfrak{p}$ sits in $I^2K_\mathfrak{p}$. If $\psi_\mathfrak{p}$ is hyperbolic then $\psi_\mathfrak{p} \cong \frac{d+1}{2}\langle 1, -1 \rangle$, hence $\varphi_\mathfrak{p} \perp \langle 1, -1 \rangle \cong \langle c \rangle \perp \frac{d+1}{2}\langle 1, -1 \rangle$ for $c = -(-1)^{d(d+1)/2} \det \varphi$. This implies that the anisotropic part of $\varphi_\mathfrak{p}$ is unary. Conversely, suppose that $\psi_\mathfrak{p}$ is not hyperbolic. As in the first part of the proof, this leads to $\psi_\mathfrak{p} = \eta_\mathfrak{p}$ in the Witt ring $WK_\mathfrak{p}$. In particular, the Witt classes of $\varphi_\mathfrak{p}$ and $\langle c, 1, u, \pi, u\pi \rangle$ are equal. But a quintic form over a local field is necessarily isotropic and so it is similar to either ternary or unary form. We claim that the unary case is impossible. Indeed, if

$$\langle c, 1, u, \pi, u\pi \rangle \cong \langle x \rangle \perp 2\langle 1, -1 \rangle,$$

then square classes of c and x are equal and the Witt cancellation theorem asserts that the forms $\langle 1, u, \pi, u\pi \rangle$ and $2\langle 1, -1 \rangle$ are isometric over $K_\mathfrak{p}$ contradicting (Lam, 2005, Corollary VI.2.15). All in all, $\langle c, 1, u, \pi, u\pi \rangle$ has a ternary anisotropic part and so has $\varphi_\mathfrak{p}$. □

Algorithm 9. Given a non-degenerate quadratic form φ over a number field K, this algorithm computes the dimension of the anisotropic part of φ.

(1) Use Algorithm 4 to compute the list $S = (s_1, \ldots, s_r)$ of the signatures of φ under all real embeddings $\rho_1, \ldots, \rho_r$ of K and take the maximum of the absolute values of these signatures
$$N := \max_{1 \le j \le r} |\operatorname{sgn} s_j|.$$
(2) If $N \ge 3$, then return N and quit.
(3) Let $\mathcal{L}$ be the set consisting of all even primes of K and all odd primes dividing any of the coefficients of φ.
(4) For every $\mathfrak{p} \in \mathcal{L}$ compute the dimension $d_\mathfrak{p}$ of the anisotropic part of $\varphi \otimes K_\mathfrak{p}$ using Algorithm 8 and let $M = \max\{ d_\mathfrak{p} \mid \mathfrak{p} \in \mathcal{L} \}$.

(5) Return $\max\{M, N\}$.

Proof of correctness. Let ψ be the anisotropic part of φ. Obviously

$$\dim \psi \equiv \dim \varphi \equiv |\operatorname{sgn} \rho_j(\varphi)| \pmod 2$$

for any real embedding ρ_j of K. Take N to be the maximum of the absolute values of the signatures of φ at all the real places. Now, ψ being anisotropic must be anisotropic at some place of K, either finite or infinite. Therefore, clearly $\dim \psi$ is the maximum of the dimensions of the anisotropic parts of the localizations of φ at all the places of K. However, if $N \geq 3$, then we do not need to consider the finite primes at all. Indeed, if $\dim \psi \geq 5$, then (Lam, 2005, Theorem VI.2.2) implies that it must be an infinite, hence real, place. Therefore in this case $\dim \psi = N \geq 5$. Similarly, if $N = 3$ or $N = 4$, then there is a real embedding ρ_j, with $\operatorname{sgn} \rho_j(\psi) = \operatorname{sgn} \rho_j(\varphi) = N$ and so $\dim \psi \geq N$. On the other hand, it cannot be strictly greater, since otherwise ψ would have to be anisotropic at some finite place contrary to the already mentioned (Lam, 2005, Theorem VI.2.2). □

5. Level of a number field

In this section we present an algorithm determining an important invariant of a number field, namely its level. Recall that a *level* of a field K, denoted $s(K)$ is the minimal number of terms needed to represent -1 as a sum of squares in K. We set $s(K) = \infty$, when -1 cannot be expressed as a sum of squares (i.e. K is formally real).

Algorithm 10. Given a number field $K = \mathbb{Q}(\vartheta)$ specified by its defining polynomial f, this algorithm computes the level $s(K)$.

(1) If the degree of f is odd, then return ∞ and quit.
(2) Check if f has any real roots (see Remark 5 below). If so, then return ∞ and quit.
(3) Check if -1 is a square in K. If so, then return 1 and quit.
(4) Find the factorization of 2 in $\mathcal{O}_K$ in the form of a list $\mathcal{L}$ consisting of triples $(\mathfrak{d}_j, e_j, f_j)$, where $\mathfrak{d}_j$ is a prime of K dominating 2 with the ramification index e_j and the inertia degree f_j.
(5) If for any j, both e_j and f_j are odd, then return 4 and quit.
(6) Return 2.

Proof of correctness. The real roots of f correspond to real embeddings of K. Hence, if f has a real root (this happens trivially, when $\deg f$ is odd), then K is formally real and consequently its level equals $s(K) = \infty$. Next, if -1 is a square in K, then $s(K) = 1$. In every other case, $s(K)$ is either 2 or 4. In order to distinguish between these two cases, (Lam, 2005, Proposition XI.2.11) comes in handy. It asserts that $s(K) = 4$ if and only if there is $1 \leq j \leq k$ such that $d_j = e_j f_j$ is odd. Otherwise, $s(K) = 2$. This is precisely what step (5) at the end of the algorithm is for. □

6. Pythagoras number

Another field invariant, important from the point of view of the algebraic theory of quadratic forms, is the Pythagoras number. It turns out that an algorithm computing it is in principle the same as the one computing the level. Recall (see e.g. (Lam, 2005,

Chapter XI)) that a Pythagoras number $P(K)$ of a field K is the smallest integer $p \in \mathbb{N}$ such that every sum of squares in K is a sum of p squares. If no such an integer exists, then $P(K) := \infty$. It is well known (see e.g. (Lam, 2005, Theorem XI.5.6)) that for any arbitrary non-real field K (not necessarily a number field), its Pythagoras number $P(K)$ and its level $s(K)$ differ by no more than 1, more precisely

$$P(K) = s(K) \quad \text{or} \quad P(K) = s(K) + 1. \tag{2}$$

There are known examples of fields for which any of these two equalities holds. Nevertheless, for number fields the situation is much simpler. We claim that for number fields the latter case is possible only when $s(K) = 4$. We expect that the following result is known to the experts in the field, but since we are not aware of any easily available reference, it easier just to prove it.

Proposition 4. *Let K be a non-real number field, then*

$$P(K) = \begin{cases} 2, & \text{if } s(K) = 1 \\ 3, & \text{if } s(K) = 2 \\ 4, & \text{if } s(K) = 4. \end{cases}$$

Proof. The quadratic closure of $\mathbb{Q}$ has infinite degree over $\mathbb{Q}$, hence it cannot be contained in any algebraic number field. It follows that $P(K) \neq 1$ for any number field K. On the other hand, $P(K) \leq s(K) + 1$ by Eq. (2). Therefore $P(K) = 2$ whenever $s(K) = 1$.

Now, assume that $s(K) = 2$, we need to show that $P(K) = 3$. Suppose otherwise, i.e. suppose that $P(K) = s(K) = 2$. This means that for every prime $\mathfrak{p}$ of K and every element $a \in \dot{K}$, the form $\langle a, 1, 1\rangle \otimes K_\mathfrak{p}$ is isotropic. Fix first an odd prime $\mathfrak{p}$ and take a to be its uniformizer. Then $\langle a, 1, 1\rangle \otimes K_\mathfrak{p}$ is isotropic if and only if $\langle 1, 1\rangle \otimes K_\mathfrak{p}$ is isotropic (by (Lam, 2005, Proposition VI.1.9)) and so -1 is a square in $K_\mathfrak{p}$. Now take an even prime $\mathfrak{d}$. By our assumption, for every $a \in \dot{K}$, the form $\varphi_\mathfrak{d} = \langle a, 1, 1\rangle \otimes K_\mathfrak{d}$ is isotropic. It follows form (Lam, 2005, Proposition V.3.22) that the Hasse invariant $s(\varphi_\mathfrak{d})$ of $\varphi_\mathfrak{d}$ equals $(-1, -\det \varphi_\mathfrak{d})_\mathfrak{d} = (-1, -1)_\mathfrak{d}$. Now the Hasse invariant of $\varphi_\mathfrak{d}$ is

$$s(\varphi_\mathfrak{d}) = (a, 1)_\mathfrak{d}(a, 1)_\mathfrak{d}(1, 1)_\mathfrak{d} = 1.$$

Thus, $(-1, -1)_\mathfrak{d} = 1$ for every $a \in \dot{K}$. By the non-degeneracy of the Hilbert symbol (see e.g. (Lam, 2005, Theorem VI.2.16)), this means that -1 is a square in $K_\mathfrak{d}$. All in all, we showed that -1 is a square in every completion of K, but then $s(K) = 1$ contrary to our assumption $s(K) = 2$. This proves the claim $P(K) = 3$.

Finally assume that $s(K) = 4$. A form $\langle a, 1, 1, 1, 1\rangle$ is isotropic over K for every $a \in \dot{K}$ by (Lam, 2005, Corollary VI.3.5). Hence, every $a \in \dot{K}$ is a sum of four squares and consequently $P(K) = 4$. □

Algorithm 11. Given a number field $K = \mathbb{Q}(\vartheta)$ specified by its defining polynomial f, this algorithm computes the Pythagoras number $P(K)$.

(1) Check if -1 is a square in K. If so, then return $P(K) = 2$ and quit.
(2) Find the factorization of 2 in $\mathcal{O}_K$ in the form of a list $\mathcal{L}$ consisting of triples $(\mathfrak{d}_j, e_j, f_j)$, where $\mathfrak{d}_j$ is a prime of K dominating 2 with the ramification index e_j and the inertia degree f_j.
(3) If for any j, both e_j and f_j are odd, then return $P(K) = 4$ and quit.

(4) Return 3.

Proof of correctness. Fix a number field K. If K is formally real, then (Lam, 2005, Example XI.5.9) asserts that $P(K) = 4$ iff there is an even prime $\mathfrak{d}_j$ such that $(K_{\mathfrak{d}_j} : \mathbb{Q}_2)$ is odd, otherwise $P(K) = 3$. Now, $(K_{\mathfrak{d}_j} : \mathbb{Q}_2) = e_j f_j$ and so the above-mentioned condition is equivalent to the test in step (3). On the other hand, if K is not real, then the correctness of the algorithm follows immediately from (Lam, 2005, Proposition XI.2.11) and Proposition 4. □

7. Witt equivalence

An important problem in the algebraic theory of quadratic forms is to find criteria for an existence of an isomorphism between the Witt rings of two fields. Such fields are then called *Witt equivalent* if the above-mentioned isomorphism exists. In this section we present an algorithm computing the complete set of Witt equivalence invariants of a given number fields. In particular, comparing the results returned by the algorithm one can check whether two number fields are Witt equivalent or not. It was proved in Szymiczek (1991) that the following invariants fully determine the Witt class of a number field K:

- $d = (K\colon \mathbb{Q})$ the degree of K over $\mathbb{Q}$;
- r the number of real embeddings of K;
- $s = s(K)$ the level of K;
- k the number of dyadic primes of K;
- for each dyadic prime $\mathfrak{d}_j$ with $1 \leq j \leq k$, the pair (d_j, s_j) consisting of a local degree $d_j = (K_{\mathfrak{d}_j}\colon \mathbb{Q}_2)$ and the local level $s_j = s(K_{\mathfrak{d}_j})$.

We claim that all these invariants are computable.

Let again $K = \mathbb{Q}(\vartheta)$ be a fixed number field specified by the minimal polynomial $f \in \mathbb{Q}[x]$ of the generator ϑ. The first two invariants d and r are trivially computable. The degree d is just the degree $\deg f$ of the defining polynomial. In order to compute r one simply counts the number of real roots of f (see Remark 5 below). In the previous section we showed how to compute the level of K. This leaves us only with the local invariants. Assume that the principal ideal $2\mathcal{O}_K$ factors into prime ideals as:

$$2\mathcal{O}_K = \mathfrak{d}_1^{e_1} \cdots \mathfrak{d}_k^{e_k}$$

and let $f_j = (\mathcal{O}_K/\mathfrak{d}_j\colon \mathbb{F}_2)$ be the inertia degree of $\mathfrak{d}_j$ $(1 \leq j \leq k)$. The local degree $d_j = (K_{\mathfrak{d}_j}\colon \mathbb{Q}_2)$ is the product $d_j = e_j f_j$. What we need is to determine the local level $s_j = s(K_{\mathfrak{d}_j})$. Fix an even prime $\mathfrak{d} = \mathfrak{d}_j$.

Algorithm 12. Let $\mathfrak{d}$ be an even prime of a number field K, e be the ramification index and f the inertia degree of $\mathfrak{d}$. This algorithm computes the level $s(K_{\mathfrak{d}})$ of the dyadic completion $K_{\mathfrak{d}}$ of K.

(1) Check if -1 is a square in K, if so then return 1 and quit.
(2) If both e and f are odd, then return 4.
(3) If e is odd but f is even, then return 2.
(4) If e is even, check whether -1 is a square in $K_{\mathfrak{d}}$, if so then return 1, if not then return 2.

Proof of correctness. It is clear that if -1 is a square already in K, then it is also a square in $K_{\mathfrak{d}}$ and so $s(K_{\mathfrak{d}}) = 1$. This justifies the first step. Suppose that e is odd. Let $\mathbb{Q}_2(\eta)$ be the (unique) maximal unramified extension of $\mathbb{Q}_2$ contained in $K_{\mathfrak{d}}$. Since the quadratic extension $\mathbb{Q}_2(i)/\mathbb{Q}_2$ is totally ramified (see e.g. (Narkiewicz, 1990, Ch. V §2)), it follows that $i \notin \mathbb{Q}_2(\eta)$. Now, $\big(\mathbb{Q}_2(\eta)\colon \mathbb{Q}_2\big) = f$ and $(K_{\mathfrak{d}}\colon \mathbb{Q}_2) = ef$. Hence the relative degree $\big(K_{\mathfrak{d}}\colon \mathbb{Q}_2(\eta)\big)$ equals e and so is odd. In particular $i \notin K_{\mathfrak{d}}$ and so $s(K_{\mathfrak{d}}) \geq 2$. Finally (Lam, 2005, Example XI.2.4) asserts that $s(K_{\mathfrak{d}}) = 4$ if and only if $(K_{\mathfrak{d}}\colon \mathbb{Q}_2)$ is odd.

Conversely, assume that e is even and so is the degree $(K_{\mathfrak{d}}\colon \mathbb{Q}_2)$. It follows from (Lam, 2005, Example XI.2.4) that $s(K_{\mathfrak{d}}) \leq 2$. It equals one if and only if -1 is a square in $K_{\mathfrak{d}}$. □

Having all the necessary ingredients ready we may now present the last algorithm of this paper that construct the complete set of Witt equivalence invariants.

Algorithm 13. If $K = \mathbb{Q}(\vartheta)$ is a number field specified (up to an isomorphism) by the minimal polynomial $f \in \mathbb{Q}[t]$ of its generator, then this algorithm computes the complete set of Witt equivalence invariants of K. In particular, two fields are Witt equivalent if and only if the outputs of the algorithm are the same for both fields.

(1) Let $d = \deg f$.
(2) Compute the number r of real roots of f.
(3) Use Algorithm 10 to compute the level $s = s(K)$.
(4) Let $\mathcal{L} = \big\{(\mathfrak{d}_j, e_j, f_j)\big\}$ be the list of all even primes of K together with their ramification indices and inertia degrees.
(5) Take an empty list $\mathcal{S}$.
(6) For each even prime $\mathfrak{d}_j \in \mathcal{L}$ let $d_j = e_j f_j$. Use Algorithm 12 to compute the local level $s_j = s(K_{\mathfrak{d}_j})$. Append the pair (d_j, s_j) to the list $\mathcal{S}$.
(7) Sort the list $\mathcal{S}$ lexicographically.
(8) Return $(d, r, s, k, \mathcal{S})$.

Remark 5. There is a number of known algorithms which can be used to count real roots of f in step (2). They vary from methods based on Sturm's and Hermite's theorems (see e.g. (Basu et al., 2003, Theorems 2.56, 4.13 and also Algorithm 9.28)) to those based on Vincent's theorem (see Akritas and Strzeboński (2005); Akritas and Vigklas (2010)). Of course, any algorithm that counts real roots can also be used to check if a polynomial has at least one real root, which is needed in step (2) of Algorithm 10. Honestly, the authors of this paper are not aware of any method answering the latter question, that would be significantly simpler than a general root counting algorithm.

8. Example applications

In order to verify the correctness of the algorithm as well as to allow experimentation, we implemented the presented algorithm in a computer algebra system Sage (see The Sage Developers (2015)). The code is available from the first author's home page at `http://z2.math.us.edu.pl/perry/papersen.html`. A formula for the number of Witt classes of number fields of a fixed degree was developed in Szymiczek (1991). Nevertheless, actual representatives for these classes were only found for quadratic and cubic fields in Szymiczek (1991) and for quartic fields in Jakubec and Marko (1992). The first test for

usability of our implementation was to find new representatives of all classes of cubic and quartic fields. Next, we found the representatives of all 36 classes of quintic fields and all 95 classes of sextic fields. These two results are completely new. The findings are gathered in tables A.1–A.4. For those classes, for which we found more than one field, the corresponding table contains a representative with the smallest absolute value of the discriminant.

The method used here was a combination of an 'aided random search' (explained bellow) and (following a suggestion of the reviewer) a search of the data base of number fields in The LMFDB Collaboration (2016). In case of quartic fields we were able to significantly improve the known results, as the largest discriminant in our case is 122 825 and the largest absolute value of a coefficient of a defining polynomial is 86 (vs. respectively 210 668 284 and 208 042 in Jakubec and Marko (1992)).

Some of Witt classes are extremely rare and virtually impossible to be found by a blind random search. These are mostly the classes of fields were 2 splits completely. In order to find the representatives of these classes one may proceed as follows. Denote by $|a|_2 := 2^{-\operatorname{ord}_2 a}$ the canonical dyadic norm and let $\|(a_0,\ldots,a_d)\|_2 := \max\{|a_0|_2,\ldots,|a_d|_d\}$ be the associated norm of the vector space $(\mathbb{Q}_2)^{d+1}$. Take a polynomial f with d distinct integral roots. Write it as a dot product $f = V \cdot X$, where V is the vector of coefficients of f and $X = (1, x, x^2, \ldots, x^d)^T$ are the powers of x. Take now some random vector W and let $\tilde{f} = (V + W) \cdot X$. If the norm $\|W\|_2$ of W is small enough, then $\tilde{f}$ still has d distinct roots in $\mathbb{Q}_2$ but there is a good chance that it is irreducible over $\mathbb{Q}$. It follows that 2 splits completely in the field $K = \mathbb{Q}[x]/\langle\tilde{f}\rangle$, as desired.

8.1. Conner's Problem

A number field K is said to satisfy Conner's Level Condition (CLC for short) if $s(K) = 2$ but $s(K_\mathfrak{d}) = 1$ for every even prime $\mathfrak{d}$ of K. Jakubec et al. (1995, 1997) proved that if a number field satisfies CLC, then its class number is even.

Since CLC is expressed in terms of Witt equivalence invariants, thus one may treat it as a property of Witt equivalence classes. In particular, if a Witt equivalence class satisfies CLC, then every field in this class has an even class number. P.E. Conner asked for an inverse of this statement (c.f. Szymiczek (2000)):

Suppose a Witt equivalence class does not satisfy CLC.
Does it contain a field with an odd class number?

An affirmative answer to Conner's question was found in Szymiczek (1991) for quadratic and cubic fields and in Jakubec et al. (1995, 1997) for quartic fields.

Observe that a field of an odd degree cannot satisfy CLC (since its level is infinite). Using The LMFDB Collaboration (2016) one checks that all fields in Tables A.1 and A.3 have trivial class groups.

As for quartic and sextic fields, there are precisely five Witt equivalence classes for which CLC holds. These are classes: 4.3, 4.6, 6.4, 6.7 and 6.12. Once we omit them, all other representatives listed in tables A.2 and A.4, except 4.21 (which has class number 2), have odd class numbers. In fact, all these fields have class numbers not only odd but actually equal one, with only two exceptions. The exceptions are the representatives of Witt equivalence classes: 6.14 and 6.18. Their class numbers equal respectively: 9 and 5. Nevertheless, it is possible to find representatives of these three "exceptional" classes with trivial class groups but with higher absolute values of discriminants (recall that the tables contain representatives with smallest discriminant we were able to find):

class	defining polynomial	LMFDB label
4.21	$x^4 - 2x^3 - 13x^2 + 14x + 32$	4.4.164441.1
6.14	$x^6 - 3x^5 - 21x^4 - x^3 + 228x^2 + 532x + 448$	6.0.827250487.1
6.18	$x^6 + 2x^4 + x^2 + 28$	6.0.12122992.1

In all cases, the class numbers where either obtained from The LMFDB Collaboration (2016) or computed in Sage using GP/Pari back-end (see The PARI Group (2015)), except for classes 6.28, 6.50–6.52, 6.54, 6.74–6.78. The class numbers of these ten fields were computed using Magma back-end (see Bosma et al. (1997)) under assumption of Generalized Riemann Hypothesis.

Summarizing the above discussion, this proves:

Theorem 6. *The Conner's question has an affirmative answer for fields of degree < 7. What is more, every Witt equivalence class of number fields of degree < 7 that do not satisfy CLC contains a field with a trivial class group.*

References

Akritas, A. G., Strzeboński, A. W., 2005. A comparative study of two real root isolation methods. Nonlinear Anal. Model. Control 10 (4), 297–304.

Akritas, A. G., Vigklas, P. S., 2010. Counting the number of real roots in an interval with Vincent's theorem. Bull. Math. Soc. Sci. Math. Roumanie (N.S.) 53(101) (3), 201–211.

Basu, S., Pollack, R., Roy, M.-F., 2003. Algorithms in real algebraic geometry. Vol. 10 of Algorithms and Computation in Mathematics. Springer-Verlag, Berlin.

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. J. Symbolic Comput. 24 (3-4), 235–265, computational algebra and number theory (London, 1993).
URL http://dx.doi.org/10.1006/jsco.1996.0125

Castel, P., 2013. Solving quadratic equations in dimension 5 or more without factoring. In: ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium. Vol. 1 of Open Book Ser. Math. Sci. Publ., Berkeley, CA, pp. 213–233.
URL http://dx.doi.org/10.2140/obs.2013.1.213

Cohen, H., 1993. A course in computational algebraic number theory. Vol. 138 of Graduate Texts in Mathematics. Springer-Verlag, Berlin.

Cohen, H., 2000. Advanced topics in computational number theory. Vol. 193 of Graduate Texts in Mathematics. Springer-Verlag, New York.
URL http://dx.doi.org/10.1007/978-1-4419-8489-0

Cremona, J. E., Rusin, D., 2003. Efficient solution of rational conics. Math. Comp. 72 (243), 1417–1441 (electronic).
URL http://dx.doi.org/10.1090/S0025-5718-02-01480-1

Czogała, A., 2001. Witt rings of Hasse domains of global fields. J. Algebra 244 (2), 604–630.
URL http://dx.doi.org/10.1006/jabr.2001.8918

Guàrdia, J., Montes, J., Nart, E., 2011. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. J. Théor. Nombres Bordeaux 23 (3), 667–696.
URL http://dx.doi.org/10.5802/jtnb.782

Guàrdia, J., Montes, J., Nart, E., 2012. Newton polygons of higher order in algebraic number theory. Trans. Amer. Math. Soc. 364 (1), 361–416.
URL http://dx.doi.org/10.1090/S0002-9947-2011-05442-5

Guàrdia, J., Montes, J., Nart, E., 2013. A new computational approach to ideal theory in number fields. Found. Comput. Math. 13 (5), 729–762.
URL http://dx.doi.org/10.1007/s10208-012-9137-5

Jakubec, S., Marko, F., 1992. Witt equivalence classes of quartic number fields. Math. Comp. 58 (197), 355–368.
URL http://dx.doi.org/10.2307/2153040

Jakubec, S., Marko, F., Szymiczek, K., 1995. Parity of class numbers and Witt equivalence of quartic fields. Math. Comp. 64 (212), 1711–1715.
URL http://dx.doi.org/10.2307/2153380

Jakubec, S., Marko, F., Szymiczek, K., 1997. Corrigendum: "Parity of class numbers and Witt equivalence of quartic fields" [Math. Comp. **64** (1995), no. 212, 1711–1715; MR1308455 (95m:11123)]. Math. Comp. 66 (218), 927.
URL http://dx.doi.org/10.1090/S0025-5718-97-00842-9

Lam, T. Y., 2005. Introduction to quadratic forms over fields. Vol. 67 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI.

Milnor, J., Husemoller, D., 1973. Symmetric Billinear Forms. Vol. 73 of Ergebnise der Matematic und ihrer Grenzgebiete. Springer Verlag, New York.

Mishra, B., 1993. Algorithmic algebra. Texts and Monographs in Computer Science. Springer-Verlag, New York.

Narkiewicz, W., 1990. Elementary and analytic theory of algebraic numbers, 2nd Edition. Springer-Verlag, Berlin.

Pauli, S., 2001. Factoring polynomials over local fields. J. Symbolic Comput. 32 (5), 533–547.
URL http://dx.doi.org/10.1006/jsco.2001.0493

Pauli, S., 2010. Factoring polynomials over local fields II. In: Algorithmic number theory. Vol. 6197 of Lecture Notes in Comput. Sci. Springer, Berlin, pp. 301–315.
URL http://dx.doi.org/10.1007/978-3-642-14518-6_24

Simon, D., 2005. Solving quadratic equations using reduced unimodular quadratic forms. Math. Comp. 74 (251), 1531–1543 (electronic).
URL http://dx.doi.org/10.1090/S0025-5718-05-01729-1

Szymiczek, K., 1991. Witt equivalence of global fields. Comm. Algebra 19 (4), 1125–1149.
URL http://dx.doi.org/10.1080/00927879108824194

Szymiczek, K., 2000. Conner's level condition. In: Algebraic number theory and Diophantine analysis (Graz, 1998). de Gruyter, Berlin, pp. 445–452.

The LMFDB Collaboration, 2016. The L-functions and modular forms database. http://www.lmfdb.org, [Online; accessed 18 January 2016].

The PARI Group, 2015. PARI/GP version 2.8.0. Bordeaux, available from http://pari.math.u-bordeaux.fr/.

The Sage Developers, 2015. Sage Mathematics Software (Version 6.9). Available from http://www.sagemath.org.

Veres, O. E., 2009. On the complexity of polynomial factorization over p-adic fields. ProQuest LLC, Ann Arbor, MI, thesis (Ph.D.)–Concordia University (Canada).

Voight, J., 2013. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. In: Quadratic and higher degree forms. Vol. 31 of Dev. Math. Springer, New York, pp. 255–298.
URL http://dx.doi.org/10.1007/978-1-4614-7488-3_10

A. Tables of representatives of Witt classes

Table A.1: Witt classes of cubic fields

No.	defining polynomial	LMFDB	r	dyadic degrees and levels
3.1.	$x^3 - x - 8$	3.1.431.1	1	$\{(1,4),(1,4),(1,4)\}$
3.2.	$x^3 + 2x - 1$	3.1.59.1	1	$\{(1,4),(2,1)\}$
3.3.	$x^3 - 3x - 4$	3.1.324.1	1	$\{(1,4),(2,2)\}$
3.4.	$x^3 - x^2 + 1$	3.1.23.1	1	$\{(3,4)\}$
3.5.	$x^3 - x^2 - 10x + 8$	3.3.961.1	3	$\{(1,4),(1,4),(1,4)\}$
3.6.	$x^3 - 4x - 1$	3.3.229.1	3	$\{(1,4),(2,1)\}$
3.7.	$x^3 - x^2 - 4x + 2$	3.3.316.1	3	$\{(1,4),(2,2)\}$
3.8.	$x^3 - x^2 - 2x + 1$	3.3.49.1	3	$\{(3,4)\}$

Table A.2: Witt classes of quartic fields

No.	defining polynomial	LMFDB	r	s	dyadic degrees and levels
4.1.	$x^4 - 2x^3 - x^2 + 2x + 2$	4.0.656.1	0	1	$\{(2,1),(2,1)\}$
4.2.	$x^4 - x^2 + 1$	4.0.144.1	0	1	$\{(4,1)\}$
4.3.	$x^4 + 3x^2 - 14x + 18$	4.0.44688.1	0	2	$\{(2,1),(2,1)\}$
4.4.	$x^4 - x^3 + x^2 + 4x + 2$	4.0.2156.1	0	2	$\{(2,1),(2,2)\}$
4.5.	$x^4 - x^3 + 2x^2 + x + 1$	4.0.225.1	0	2	$\{(2,2),(2,2)\}$
4.6.	$x^4 - 5x^2 + 25$	4.0.3600.3	0	2	$\{(4,1)\}$
4.7.	$x^4 - x^3 - x^2 + x + 1$	4.0.117.1	0	2	$\{(4,2)\}$
4.8.	$x^4 - 2x^3 - x^2 + 2x + 8$	4.0.6713.1	0	4	$\{(1,4),(1,4),(1,4),(1,4)\}$
4.9.	$x^4 - x^3 + 6x^2 - 2x + 4$	4.0.4508.1	0	4	$\{(1,4),(1,4),(2,1)\}$
4.10.	$x^4 - 2x^3 + 2x^2 - x + 2$	4.0.1421.1	0	4	$\{(1,4),(1,4),(2,2)\}$
4.11.	$x^4 + x^2 - x + 1$	4.0.257.1	0	4	$\{(1,4),(3,4)\}$
4.12.	$x^4 - 2x^3 - 5x^2 + 6x - 8$	4.2.29767.1	2	∞	$\{(1,4),(1,4),(1,4),(1,4)\}$
4.13.	$x^4 - 5x^2 - 4$	4.2.6724.1	2	∞	$\{(1,4),(1,4),(2,1)\}$
4.14.	$x^4 - 2x^2 - x - 2$	4.2.4027.1	2	∞	$\{(1,4),(1,4),(2,2)\}$

Continued on the next page

Table A.2: Witt classes of quartic fields (continued)

No.	defining polynomial	LMFDB	r	s	dyadic degrees and levels
4.15.	$x^4 - 2x^3 + x^2 - x - 1$	4.2.751.1	2	∞	$\{(1,4),(3,4)\}$
4.16.	$x^4 - 2x^3 - 5x^2 - 2x + 2$	4.2.27632.1	2	∞	$\{(2,1),(2,1)\}$
4.17.	$x^4 - x^3 - 3x^2 + 2$	4.2.1588.1	2	∞	$\{(2,1),(2,2)\}$
4.18.	$x^4 - x^3 - 3x - 1$	4.2.775.1	2	∞	$\{(2,2),(2,2)\}$
4.19.	$x^4 + x^2 - 6x + 1$	4.2.3312.2	2	∞	$\{(4,1)\}$
4.20.	$x^4 - x^3 + 2x - 1$	4.2.275.1	2	∞	$\{(4,2)\}$
4.21.	$x^4 - x^3 - 23x^2 + x + 86$	4.4.122825.1	4	∞	$\{(1,4),(1,4),(1,4),(1,4)\}$
4.22.	$x^4 - x^3 - 15x^2 + 31x - 8$	4.4.54332.1	4	∞	$\{(1,4),(1,4),(2,1)\}$
4.23.	$x^4 - 2x^3 - 4x^2 + 5x + 2$	4.4.15317.1	4	∞	$\{(1,4),(1,4),(2,2)\}$
4.24.	$x^4 - x^3 - 4x^2 + x + 2$	4.4.2777.1	4	∞	$\{(1,4),(3,4)\}$
4.25.	$x^4 - 2x^3 - 5x^2 + 6x + 2$	4.4.44688.2	4	∞	$\{(2,1),(2,1)\}$
4.26.	$x^4 - 5x^2 + 2$	4.4.9248.1	4	∞	$\{(2,1),(2,2)\}$
4.27.	$x^4 - x^3 - 5x^2 + 2x + 4$	4.4.2225.1	4	∞	$\{(2,2),(2,2)\}$
4.28.	$x^4 - 2x^3 - 7x^2 + 8x + 1$	4.4.3600.1	4	∞	$\{(4,1)\}$
4.29.	$x^4 - x^3 - 3x^2 + x + 1$	4.4.725.1	4	∞	$\{(4,2)\}$

Table A.3: Witt classes of quintic fields

No.	defining polynomial	LMFDB label	r	dyadic degrees and levels
5.1.	$x^5 - x^3 - 4\,x^2 + 20\,x + 16$	5.1.1659001.1	1	$\{(1,4),(1,4),(1,4),(1,4),(1,4)\}$
5.2.	$x^5 - 2\,x^4 + 8\,x^3 - 8\,x^2 + 15\,x + 2$	5.1.224956.1	1	$\{(1,4),(1,4),(1,4),(2,1)\}$
5.3.	$x^5 - 3\,x^2 + 8\,x - 4$	5.1.119701.2	1	$\{(1,4),(1,4),(1,4),(2,2)\}$
5.4.	$x^5 - 2\,x^4 + 3\,x^3 - 5\,x^2 + 3\,x - 2$	5.1.19633.1	1	$\{(1,4),(1,4),(3,4)\}$
5.5.	$x^5 - x^3 - 4\,x^2 + 6\,x - 4$	5.1.408976.1	1	$\{(1,4),(2,1),(2,1)\}$
5.6.	$x^5 + 2\,x^3 - x^2 + 2\,x - 2$	5.1.28684.1	1	$\{(1,4),(2,1),(2,2)\}$
5.7.	$x^5 - x^4 + 2\,x^3 - x^2 + x + 2$	5.1.17161.1	1	$\{(1,4),(2,2),(2,2)\}$
5.8.	$x^5 - 2\,x^4 + x^3 + 4\,x^2 - 7\,x + 4$	5.1.42256.1	1	$\{(1,4),(4,1)\}$
5.9.	$x^5 - 2\,x^2 - 2\,x - 1$	5.1.4261.1	1	$\{(1,4),(4,2)\}$
5.10.	$x^5 - x^4 + 2\,x^3 - 3\,x^2 + 2\,x - 2$	5.1.10492.1	1	$\{(2,1),(3,4)\}$
5.11.	$x^5 - x - 1$	5.1.2869.1	1	$\{(2,2),(3,4)\}$
5.12.	$x^5 - x^3 - x^2 + x + 1$	5.1.1609.1	1	$\{(5,4)\}$
5.13.	$x^5 - x^4 - 3\,x^3 + 17\,x^2 - 38\,x + 8$	5.3.6556247.1	3	$\{(1,4),(1,4),(1,4),(1,4),(1,4)\}$
5.14.	$x^5 - 8\,x^3 + 7\,x - 16$	5.3.1078244.1	3	$\{(1,4),(1,4),(1,4),(2,1)\}$
5.15.	$x^5 - 2\,x^4 + 9\,x^2 - 4$	5.3.443291.1	3	$\{(1,4),(1,4),(1,4),(2,2)\}$
5.16.	$x^5 - 2\,x^4 + x^3 + x^2 - 7\,x + 4$	5.373607.1	3	$\{(1,4),(1,4),(3,4)\}$
5.17.	$x^5 - x^3 - 4\,x^2 - 2\,x + 4$	5.3.409328.1	3	$\{(1,4),(2,1),(2,1)\}$
5.18.	$x^5 - x^4 - 4\,x^3 + x^2 + 3\,x + 2$	5.3.113684.1	3	$\{(1,4),(2,1),(2,2)\}$
5.19.	$x^5 - 4\,x^3 - x^2 + 2\,x + 4$	5.3.67943.1	3	$\{(1,4),(2,2),(2,2)\}$
5.20.	$x^5 - 2\,x^3 - 2\,x^2 - 3\,x + 2$	5.3.41456.1	3	$\{(1,4),(4,1)\}$
5.21.	$x^5 - x^4 - x^3 - x^2 - 3\,x + 1$	5.3.13523.1	3	$\{(1,4),(4,2)\}$

Continued on the next page

Table A.3: Witt classes of quintic fields (continued)

No.	defining polynomial	LMFDB label	r	dyadic degrees and levels
5.22.	$x^5 - x^4 - 2\,x^3 - x^2 + 2\,x + 2$	5.3.17348.1	3	$\{(2,1),(3,4)\}$
5.23.	$x^5 - x^4 - 2\,x + 1$	5.3.11243.1	3	$\{(2,2),(3,4)\}$
5.24.	$x^5 - x^3 - 2\,x^2 + 1$	5.3.4511.1	3	$\{(5,4)\}$
5.25.	$x^5 - x^4 - 19\,x^3 + 17\,x^2 + 58\,x - 40$	5.5.46919377.1	5	$\{(1,4),(1,4),(1,4),(1,4),(1,4)\}$
5.26.	$x^5 - x^4 - 14\,x^3 - 2\,x^2 + 28\,x + 16$	5.5.8048764.1	5	$\{(1,4),(1,4),(1,4),(2,1)\}$
5.27.	$x^5 - 13\,x^3 - 4\,x^2 + 24\,x + 8$	5.5.3609877.1	5	$\{(1,4),(1,4),(1,4),(2,2)\}$
5.28.	$x^5 - 7\,x^3 - x^2 + 11\,x + 4$	5.5.372289.1	5	$\{(1,4),(1,4),(3,4)\}$
5.29.	$x^5 - 2\,x^4 - 10\,x^3 + 14\,x^2 + 21\,x - 16$	5.5.46919377.1	5	$\{(1,4),(2,1),(2,1)\}$
5.30.	$x^5 - x^4 - 7\,x^3 + 6\,x^2 + 6\,x - 4$	5.5.600268.1	5	$\{(1,4),(2,1),(2,2)\}$
5.31.	$x^5 - x^4 - 6\,x^3 + 5\,x^2 + 7\,x - 4$	5.5.406264.1	5	$\{(1,4),(2,2),(2,2)\}$
5.32.	$x^5 - 8\,x^3 - 2\,x^2 + 5\,x + 2$	5.5.380224.1	5	$\{(1,4),(4,1)\}$
5.33.	$x^5 - x^4 - 5\,x^3 + 3\,x^2 + 5\,x - 2$	5.5.81509.1	5	$\{(1,4),(4,2)\}$
5.34.	$x^5 - 2\,x^4 - 4\,x^3 + 5\,x^2 + 3\,x - 1$	5.5.218524.1	5	$\{(2,1),(3,4)\}$
5.35.	$x^5 - x^4 - 5\,x^3 + 4\,x^2 + 4\,x - 1$	5.5.117688.1	5	$\{(2,2),(3,4)\}$
5.36.	$x^5 - x^4 - 4\,x^3 + 3\,x^2 + 3\,x - 1$	5.1.14641.1	5	$\{(5,4)\}$

Table A.4: Witt classes of sextic fields

No.	defining polynomial	LMFDB label	r	s	dyadic degrees and levels
6.1.	$x^6 - 2\,x^5 + 3\,x^4 - 6\,x^3 + 6\,x^2 - 8\,x + 8$	6.0.399424.1	0	1	$\{(2,1),(2,1),(2,1)\}$
6.2.	$x^6 - 2\,x^3 + x^2 + 2\,x + 2$	6.0.53824.1	0	1	$\{(2,1),(4,1)\}$
6.3.	$x^6 - x^4 - 2\,x^3 + 2\,x + 1$	6.0.10816.1	0	1	$\{(6,1)\}$
6.4.	$x^6 - 2\,x^5 - x^4 + 10\,x^3 + 82\,x^2 - 8\,x + 16$	6.0.45118016.1	0	2	$\{(2,1),(2,1),(2,1)\}$
6.5.	$x^6 - x^5 + 3\,x^4 - 2\,x^3 + 13\,x^2 - 17\,x + 11$	6.0.2787888.1	0	2	$\{(2,1),(2,1),(2,2)\}$
6.6.	$x^6 - 3\,x^5 + 4\,x^4 - 3\,x^3 + 3\,x^2 + 2$	6.0.236708.2	0	2	$\{(2,1),(2,2),(2,2)\}$
6.7.	$x^6 + 4\,x^4 - 8\,x^3 + 4\,x^2 + 1$	6.0.11999296.1	0	2	$\{(2,1),(4,1)\}$
6.8.	$x^6 + 2\,x^4 - x^3 + 3\,x^2 + 2$	6.0.122708.1	0	2	$\{(2,1),(4,2)\}$
6.9.	$x^6 - 2\,x^4 - 2\,x^3 + 4\,x^2 + 2\,x + 1$	6.0.93987.1	0	2	$\{(2,2),(2,2),(2,2)\}$
6.10.	$x^6 - 3\,x^4 - 2\,x^3 + 9\,x^2 + 12\,x + 4$	6.0.314928.2	0	2	$\{(2,2),(4,1)\}$
6.11.	$x^6 - x^5 - x^4 + 3\,x^3 - 2\,x + 1$	6.0.16551.1	0	2	$\{(2,2),(4,2)\}$
6.12.	$x^6 - 2\,x^5 + 12\,x^4 - 30\,x^3 + 74\,x^2 - 88\,x + 82$	6.0.9199872.1	0	2	$\{(6,1)\}$
6.13.	$x^6 - x^5 + x^4 - 2\,x^3 + 4\,x^2 - 3\,x + 1$	6.0.9747.1	0	2	$\{(6,2)\}$
6.14.	$x^6 - x^5 + 3\,x^4 - 11\,x^3 + 44\,x^2 - 36\,x + 32$	6.0.28629151.1	0	4	$\{(1,4),(1,4),(1,4),(1,4),(1,4),(1,4)\}$
6.15.	$x^6 - x^2 + 16$	6.0.11930116.1	0	4	$\{(1,4),(1,4),(1,4),(1,4),(2,1)\}$
6.16.	$x^6 - 3\,x^5 + 2\,x^4 + x^3 + x^2 - 2\,x + 8$	6.0.4807171.1	0	4	$\{(1,4),(1,4),(1,4),(1,4),(2,2)\}$
6.17.	$x^6 - x^5 + 3\,x^4 + 2\,x^3 + 6\,x^2 + 3\,x + 2$	6.0.469567.1	0	4	$\{(1,4),(1,4),(1,4),(3,4)\}$
6.18.	$x^6 - x^5 + 6\,x^4 + 4\,x^3 + 11\,x^2 + 21\,x + 22$	6.0.7888624.1	0	4	$\{(1,4),(1,4),(2,1),(2,1)\}$
6.19.	$x^6 - 13\,x^2 + 20$	6.0.5060180.2	0	4	$\{(1,4),(1,4),(2,1),(2,2)\}$
6.20.	$x^6 - 3\,x^5 + x^4 + 3\,x^3 + x^2 - 3\,x + 2$	6.0.489119.1	0	4	$\{(1,4),(1,4),(2,2),(2,2)\}$
6.21.	$x^6 - x^5 - x^4 - 3\,x^3 + x^2 + 7\,x + 4$	6.0.887152.1	0	4	$\{(1,4),(1,4),(4,1)\}$

Continued on the next page

Table A.4: Witt classes of sextic fields (continued)

No.	defining polynomial	LMFDB label	r	s	dyadic degrees and levels
6.22.	$x^6 - 2\,x^5 + 2\,x^4 - x + 2$	6.0.134363.1	0	4	$\{(1,4),(1,4),(4,2)\}$
6.23.	$x^6 - 2\,x^5 + x^4 - x^3 + x^2 + 2$	6.0.1085252.1	0	4	$\{(1,4),(2,1),(3,4)\}$
6.24.	$x^6 + x^4 - x + 1$	6.0.89363.1	0	4	$\{(1,4),(2,2),(3,4)\}$
6.25.	$x^6 - x^5 + x^4 - x^3 + 2\,x^2 - x + 1$	6.0.31223.1	0	4	$\{(1,4),(5,4)\}$
6.26.	$x^6 - 3\,x^5 + 5\,x^4 - 5\,x^3 + 5\,x^2 - 3\,x + 1$	6.0.12167.1	0	4	$\{(3,4),(3,4)\}$
6.27.	$x^6 - 53\,x^4 - 16\,x^3 + 868\,x^2 - 800\,x - 4288$	—	2	∞	$\{(1,4),(1,4),(1,4),(1,4),(1,4),(1,4)\}$
6.28.	$x^6 - 232\,x^5 - 479\,x^4 - 440\,x^3 - 502\,x^2 + 348\,x - 64$	—	2	∞	$\{(1,4),(1,4),(1,4),(1,4),(2,1)\}$
6.29.	$x^6 - 3\,x^5 - 4\,x^4 + 13\,x^3 - x^2 - 6\,x - 8$	6.2.26919373.1	2	∞	$\{(1,4),(1,4),(1,4),(1,4),(2,2)\}$
6.30.	$x^6 - x^5 - x^4 - 7\,x^2 - 2\,x + 8$	6.2.4721393.4	2	∞	$\{(1,4),(1,4),(1,4),(3,4)\}$
6.31.	$x^6 - 2\,x^5 + x^4 - 18\,x^3 + 18\,x^2 - 8$	6.2.11279504.1	2	∞	$\{(1,4),(1,4),(2,1),(2,1)\}$
6.32.	$x^6 - x^4 + 6\,x^2 - 8$	6.2.5944352.3	2	∞	$\{(1,4),(1,4),(2,1),(2,2)\}$
6.33.	$x^6 - 3\,x^5 + 5\,x^4 - 5\,x^3 - 3\,x^2 + 5\,x - 2$	6.2.2150081.1	2	∞	$\{(1,4),(1,4),(2,2),(2,2)\}$
6.34.	$x^6 - x^5 - 5\,x^4 + 5\,x^3 + x^2 + 5\,x - 4$	6.2.946832.1	2	∞	$\{(1,4),(1,4),(4,1)\}$
6.35.	$x^6 - 2\,x^5 - x^4 + 2\,x^3 - x^2 - 3\,x + 2$	6.2.365117.1	2	∞	$\{(1,4),(1,4),(4,2)\}$
6.36.	$x^6 + 2\,x^5 - x^4 - x^3 - x^2 - 2$	—	2	∞	$\{(1,4),(2,1),(3,4)\}$
6.37.	$x^6 - x^4 - 2\,x^2 - x - 1$	6.2.255917.1	2	∞	$\{(1,4),(2,2),(3,4)\}$
6.38.	$x^6 - 2\,x^5 + 3\,x^4 - x^3 + 2\,x - 1$	6.2.89737.1	2	∞	$\{(1,4),(5,4)\}$
6.39.	$x^6 - 2\,x^5 - 5\,x^4 + 18\,x^3 - 10\,x^2 - 8\,x + 8$	6.2.48491968.1	2	∞	$\{(2,1),(2,1),(2,1)\}$
6.40.	$x^6 - 2\,x^5 - x^4 + 4\,x^3 + 2\,x^2 - 4\,x - 8$	6.2.2895824.1	2	∞	$\{(2,1),(2,1),(2,2)\}$
6.41.	$x^6 - 2\,x^5 + 5\,x^4 - 4\,x^3 - 3\,x^2 + 6\,x - 2$	6.2.633788.1	2	∞	$\{(2,1),(2,2),(2,2)\}$

Continued on the next page

Table A.4: Witt classes of sextic fields (continued)

No.	defining polynomial	LMFDB label	r	s	dyadic degrees and levels
6.42.	$x^6 - 4\,x^4 - 8\,x^3 - 4\,x^2 + 1$	6.2.3548608.1	2	∞	$\{(2,1),(4,1)\}$
6.43.	$x^6 - x^4 - 2\,x^3 + x^2 + 2\,x - 2$	6.2.95852.1	2	∞	$\{(2,1),(4,2)\}$
6.44.	$x^6 - 2\,x^5 + 2\,x^3 - 2\,x^2 + 4\,x + 1$	6.2.332021.1	2	∞	$\{(2,2),(2,2),(2,2)\}$
6.45.	$x^6 - 2\,x^5 + 2\,x^4 - 4\,x^3 + 2\,x^2 - 4\,x + 1$	6.2.242000.2	2	∞	$\{(2,2),(4,1)\}$
6.46.	$x^6 - x^4 - x^3 - x^2 + 1$	6.2.52441.1	2	∞	$\{(2,2),(4,2)\}$
6.47.	$x^6 - x^5 - 3\,x^4 + 3\,x^3 + 3\,x^2 - x - 1$	6.2.47081.1	2	∞	$\{(3,4),(3,4)\}$
6.48.	$x^6 + 2\,x^4 + x^2 - 23$	6.2.778688.2	2	∞	$\{(6,1)\}$
6.49.	$x^6 - 2\,x^5 + 3\,x^3 - 2\,x - 1$	6.2.28037.1	2	∞	$\{(6,2)\}$
6.50.	$x^6 + 8152\,x^5 + 131685\,x^4 + 3664\,x^3 + 49395\,x^2 + 496600\,x + 23207$	—	4	∞	$\{(1,4),(1,4),(1,4),(1,4),(1,4),(1,4)\}$
6.51.	$x^6 + 474\,x^5 - 72\,x^4 - 424\,x^3 + 415\,x^2 - 434\,x - 280$	—	4	∞	$\{(1,4),(1,4),(1,4),(1,4),(2,1)\}$
6.52.	$x^6 + 120\,x^5 + 2\,x^4 - 169\,x^3 - 170\,x^2 + 176\,x + 32$	—	4	∞	$\{(1,4),(1,4),(1,4),(1,4),(2,2)\}$
6.53.	$x^6 + x^5 + x^4 - 21\,x^2 + 4$	—	4	∞	$\{(1,4),(1,4),(1,4),(3,4)\}$
6.54.	$x^6 - 484\,x^5 - 696\,x^4 + 346\,x^3 - 671\,x^2 - 538\,x + 114$	—	4	∞	$\{(1,4),(1,4),(2,1),(2,1)\}$
6.55.	$x^6 - 15\,x^5 + 11\,x^4 + 25\,x^3 + 32\,x^2 + 34\,x + 8$	—	4	∞	$\{(1,4),(1,4),(2,1),(2,2)\}$
6.56.	$x^6 - 4\,x^4 - 9\,x^2 + 4$	6.4.13675204.1	4	∞	$\{(1,4),(1,4),(2,2),(2,2)\}$
6.57.	$x^6 - x^5 - 7\,x^4 + 9\,x^3 + 11\,x^2 - 17\,x + 2$	6.4.3095536.1	4	∞	$\{(1,4),(1,4),(4,1)\}$
6.58.	$x^6 - 5\,x^4 - 2\,x^3 + 7\,x^2 + 5\,x - 2$	6.4.1415907.1	4	∞	$\{(1,4),(1,4),(4,2)\}$
6.59.	$x^6 + x^5 - 3\,x^4 - 2\,x^3 - 2\,x^2 + x + 6$	—	4	∞	$\{(1,4),(2,1),(3,4)\}$

Continued on the next page

Table A.4: Witt classes of sextic fields (continued)

No.	defining polynomial	LMFDB label	r	s	dyadic degrees and levels
6.60.	$x^6 - 3\,x^5 - 6\,x^4 + 12\,x^3 + 15\,x^2 + 3$	6.4.32019867.1	4	∞	$\{(1,4),(2,2),(3,4)\}$
6.61.	$x^6 - 2\,x^5 + x^4 - 4\,x^2 + x + 2$	6.4.321527.1	4	∞	$\{(1,4),(5,4)\}$
6.62.	$x^6 - 2\,x^5 - 10\,x^4 - 2\,x^3 - 11\,x^2 - 16\,x + 16$	—	4	∞	$\{(2,1),(2,1),(2,1)\}$
6.63.	$x^6 - 3\,x^5 - 2\,x^4 + 9\,x^3 - x^2 - 4\,x + 2$	6.4.4293808.3	4	∞	$\{(2,1),(2,1),(2,2)\}$
6.64.	$x^6 + 2\,x^4 - 6\,x^2 + 1$	6.4.2149156.1	4	∞	$\{(2,1),(2,2),(2,2)\}$
6.65.	$x^6 - 2\,x^5 - 5\,x^4 + 12\,x^3 - x^2 - 6\,x + 2$	6.4.3182656.1	4	∞	$\{(2,1),(4,1)\}$
6.66.	$x^6 - x^5 - 3\,x^4 + 5\,x^3 + 3\,x^2 - 4\,x - 2$	6.4.733588.1	4	∞	$\{(2,1),(4,2)\}$
6.67.	$x^6 - 5\,x^4 + 3\,x^2 + 2$	6.4.1759688.1	4	∞	$\{(2,2),(2,2),(2,2)\}$
6.68.	$x^6 - 3\,x^5 + x^4 + 2\,x^3 - 3\,x^2 + 5\,x + 1$	6.4.478000.1	4	∞	$\{(2,2),(4,1)\}$
6.69.	$x^6 - 2\,x^5 - 2\,x^4 + 5\,x^3 - x^2 - 3\,x + 1$	6.4.202375.1	4	∞	$\{(2,2),(4,2)\}$
6.70.	$x^6 - 3\,x^5 + x^4 + 3\,x^3 - 3\,x^2 + x + 1$	6.4.170471.1	4	∞	$\{(3,4),(3,4)\}$
6.71.	$x^6 - 3\,x^4 - 4\,x^3 + 2\,x^2 + 4\,x + 1$	6.4.526912.1	4	∞	$\{(6,1)\}$
6.72.	$x^6 - x^5 - 2\,x^4 + 3\,x^3 - x^2 - 2\,x + 1$	6.4.92779.1	4	∞	$\{(6,2)\}$
6.73.	$x^6 - 85\,x^4 - 16\,x^3 + 1156\,x^2 - 544\,x + 64$	—	6	∞	$\{(1,4),(1,4),(1,4),(1,4),(1,4),(1,4)\}$
6.74.	$x^6 + 1028\,x^5 + 131059\,x^4 + 4194272\,x^3 + 8388639\,x^2 + 4194268\,x + 131117$	—	6	∞	$\{(1,4),(1,4),(1,4),(1,4),(2,1)\}$
6.75.	$x^6 + 496\,x^5 + 65611\,x^4 + 2097152\,x^3 + 2096311\,x^2 + 6032\,x - 643$	—	6	∞	$\{(1,4),(1,4),(1,4),(1,4),(2,2)\}$
6.76.	$x^6 + 8\,x^5 - 105\,x^4 + 8\,x^3 + 912\,x^2 + 16\,x - 768$	—	6	∞	$\{(1,4),(1,4),(1,4),(3,4)\}$
6.77.	$x^6 + 2\,x^5 - 77\,x^4 + 4\,x^3 + 910\,x^2 + 4\,x - 768$	—	6	∞	$\{(1,4),(1,4),(2,1),(2,1)\}$
6.78.	$x^6 + 4\,x^5 - 105\,x^4 + 4\,x^3 + 910\,x^2 + 4\,x - 768$	—	6	∞	$\{(1,4),(1,4),(2,1),(2,2)\}$

Continued on the next page

Table A.4: Witt classes of sextic fields (continued)

No.	defining polynomial	LMFDB label	r	s	dyadic degrees and levels
6.79.	$x^6 - 3\,x^5 - 9\,x^4 + 23\,x^3 + 20\,x^2 - 32\,x - 8$	6.6.56269193.1	6	∞	$\{(1,4),(1,4),(2,2),(2,2)\}$
6.80.	$x^6 - 9\,x^4 + 13\,x^2 - 4$	6.6.24167056.1	6	∞	$\{(1,4),(1,4),(4,1)\}$
6.81.	$x^6 - 2\,x^5 - 7\,x^4 + 14\,x^3 + 5\,x^2 - 13\,x + 4$	6.6.10330877.1	6	∞	$\{(1,4),(1,4),(4,2)\}$
6.82.	$x^6 - 2\,x^5 - 6\,x^4 + 11\,x^3 + 7\,x^2 - 11\,x - 2$	6.6.20413244.1	6	∞	$\{(1,4),(2,1),(3,4)\}$
6.83.	$x^6 - x^5 - 7\,x^4 + 4\,x^3 + 13\,x^2 - 2\,x - 4$	6.6.7432373.1	6	∞	$\{(1,4),(2,2),(3,4)\}$
6.84.	$x^6 - 6\,x^4 - x^3 + 8\,x^2 + x - 2$	6.6.1868969.1	6	∞	$\{(1,4),(5,4)\}$
6.85.	$x^6 - 2\,x^5 - 17\,x^4 + 54\,x^3 - 34\,x^2 - 8\,x + 8$	6.6.31554496.1	6	∞	$\{(2,1),(2,1),(2,1)\}$
6.86.	$x^6 - 14\,x^4 - 2\,x^3 + 15\,x^2 - 2\,x - 2$	6.6.34350464.1	6	∞	$\{(2,1),(2,1),(2,2)\}$
6.87.	$x^6 - 3\,x^5 - 6\,x^4 + 13\,x^3 + 9\,x^2 - 12\,x - 4$	6.6.35478972.1	6	∞	$\{(2,1),(2,2),(2,2)\}$
6.88.	$x^6 - 9\,x^4 - 6\,x^3 + 15\,x^2 + 14\,x + 2$	6.6.9186752.1	6	∞	$\{(2,1),(4,1)\}$
6.89.	$x^6 - x^5 - 6\,x^4 + 4\,x^3 + 7\,x^2 - 2\,x - 2$	6.6.3072812.1	6	∞	$\{(2,1),(4,2)\}$
6.90.	$x^6 - 12\,x^4 - 4\,x^3 + 16\,x^2 + 4\,x - 1$	6.6.6555125.1	6	∞	$\{(2,2),(2,2),(2,2)\}$
6.91.	$x^6 - 7\,x^4 + 12\,x^2 - 2$	6.6.3195392.1	6	∞	$\{(2,2),(4,1)\}$
6.92.	$x^6 - x^5 - 7\,x^4 + 7\,x^3 + 12\,x^2 - 12\,x - 1$	6.6.1312625.1	6	∞	$\{(2,2),(4,2)\}$
6.93.	$x^6 - x^5 - 7\,x^4 + 9\,x^3 + 7\,x^2 - 9\,x - 1$	6.6.905177.1	6	∞	$\{(3,4),(3,4)\}$
6.94.	$x^6 - 7\,x^4 + 14\,x^2 - 7$	6.6.1075648.1	6	∞	$\{(6,1)\}$
6.95.	$x^6 - x^5 - 7\,x^4 + 2\,x^3 + 7\,x^2 - 2\,x - 1$	6.6.300125.1	6	∞	$\{(6,2)\}$