MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 197
JANUARY 1992, PAGES 355–368

WITT EQUIVALENCE CLASSES OF QUARTIC NUMBER FIELDS

STANISLAV JAKUBEC AND FRANTIŠEK MARKO

ABSTRACT. It has recently been established that there are exactly seven Witt equivalence classes of quadratic number fields, and then all quadratic and cubic number fields have been classified with respect to Witt equivalence. In this paper we have classified number fields of degree four. Using this classification, we have proved the Conjecture of Szymiczek about the representability of Witt equivalence classes by quadratic extensions of quadratic fields.

1. INTRODUCTION

This article arose as a response to questions posed by Szymiczek at the 9th Czechoslovak Colloquium on Number Theory held at Račková dolina in September 1989. At this colloquium he introduced the Witt equivalence invariant of an algebraic number field which classifies number fields according to the isomorphism classes of their Witt rings of nondegenerate symmetric bilinear forms. In [7] a complete classification of cubic number fields is carried out, and the earlier classification of quadratic fields (due to Czogala and Szymiczek, and independently to Carpenter) is given a new treatment in the unifying language of the Witt equivalence invariant.

Here we solve the classification problem for number fields of degree four. The problem consists in determining the Witt equivalence invariant for an arbitrary quartic field F. To this end, we divide the quartic fields into eleven classes according to the splitting behavior of the principal ideal (2) in F, and then we compute the Witt equivalence invariant in each case. It is known from [7] that there are exactly 29 Witt equivalence classes of quartic fields.

The essential difficulty is to determine local levels at dyadic primes for fields with prescribed splitting type. The theorems in §4 determine local levels, provided uniformizing elements of the corresponding dyadic primes are available. The determination of these elements is simple if the index of the field is odd.

Szymiczek observed that there are three classes of quartic fields where the local degrees are odd, and that these three classes cannot be represented by quartic fields having quadratic subfields. He conjectured, however, that all the remaining 26 classes can be represented by quadratic extensions of some quadratic fields. He even asserted that $Q(\sqrt{2})$ and $Q(\sqrt{17})$ will do as base fields.

Using the classification of quartic fields, we have constructed representatives of the 26 classes mentioned above, and in this way we have proved the Conjec-

Received February 2, 1990; revised August 13, 1990.
1991 *Mathematics Subject Classification.* Primary 11E81, 11A07.

0025-5718/92 $1.00 + $.25 per page

ture of Szymiczek. Moreover, we do so using the minimal number of splitting types of the ideal (2).

2. Witt equivalence invariant

In [7] the notion of Witt equivalence invariant of a given number field F is introduced. We use the notation as in [7], namely

- n is the degree of the number field F over Q;
- r is the number of real embeddings of F;
- s is the level of F—it is equal to zero if F is formally real, otherwise it is the minimal number of summands in the expressions of -1 as a sum of squares in F;
- g is the number of dyadic primes $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_g$ in F, hence $\mathfrak{p}_i \mid 2$ for every $i = 1, 2, \dots, g$;
- $n_1, n_2, \dots, n_g$ are the local degrees $[F_{\mathfrak{p}_i} : Q_2]$ of dyadic completions $F_{\mathfrak{p}_1}, F_{\mathfrak{p}_2}, \dots, F_{\mathfrak{p}_g}$ of F over dyadic numbers Q_2;
- $s_1, s_2, \dots, s_g$ are the levels of dyadic completion $F_{\mathfrak{p}_1}, F_{\mathfrak{p}_2}, \dots, F_{\mathfrak{p}_g}$.

It is always required that $n_1 \le n_2 \le \cdots \le n_g$, and if $n_i = n_{i+1}$, then $s_i \le s_{i+1}$.

The ordered set of integers $S(F) = (n, r, s, g; n_1, \dots, n_g; s_1, \dots, s_g)$ is called the Witt equivalence invariant (shortly invariant) of the number field F.

Theorem (2.1) of [7] gives a necessary and sufficient condition for the ordered set of integers $S = (n, r, s, g; n_1, \dots, n_g; s_1, \dots, s_g)$ to be the invariant of some number field F:

(1) $n = n_1 + n_2 + \cdots + n_g$;

(2) $0 \le r \le n$ and $n \equiv r \pmod 2$;

(3) s_i divides s for every $i = 1, 2, \dots, g$ and $s = 4$ if and only if $s_i = 4$ for at least one i, $1 \le i \le g$;

(4) $s_i = 4$ if and only if $n_i = 1 \pmod 2$ for $i = 1, 2, \dots, g$, $s \in \{0, 1, 2, 4\}$, $s_i \in \{1, 2, 4\}$ for $i = 1, 2, \dots, g$, and $s = 0$ if and only if $r \neq 0$.

Using this result, one easily determines the 29 possible Witt equivalence invariants for quartic fields given in Table 1 of §5. Our main concern is the converse problem: given a quartic field F, compute the invariant $S(F)$. So, suppose ρ is a generator of F over Q and $f(x)$ is the monic minimal polynomial of ρ. Then n is equal to the degree of $f(x)$, and r is equal to the number of real zeros of $f(x)$. According to [1, Chapter IV, §2, Theorem 3], the numbers $g; n_1, n_2, \dots, n_g$ are the number and the degrees of irreducible polynomials in the factorization of $f(x)$ over Q_2. The numbers $g; n_1, n_2, \dots, n_g$ could be determined already from the decomposition of $f(x)$ into a maximal possible number of factors modulo some power of 2 (see [1, Chapter IV, §3, Theorem 3]).

Therefore, the main difficulty lies in the determination of the levels s and $s_1, s_2, \dots, s_g$.

3. Local levels

Every local level s_i takes on values from the set $\{1, 2, 4\}$. The case $s_i = 4$ is easily distinguished (see §2). Therefore, the determination of s_i is reduced to the question of whether $s_i = 1$ or not, that is, whether the equation $x^2 + 1 = 0$ is solvable in $F_{\mathfrak{p}_i}$.

Denote by $\mathfrak{O}$ the integral closure in F of the valuation ring associated with the prime 2 in Q. Then there are exactly g nonassociated prime elements $\pi_1, \pi_2, \ldots, \pi_g$ in $\mathfrak{O}$ which correspond to dyadic primes $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_g$ in F (see [1, Chapter III, §4, Theorem 7]).

According to [1, Chapter IV, §1, Remark 2] the above equation is solvable if and only if the congruence $x^2 + 1 \equiv 0 \pmod{\mathfrak{p}_i^{2e_i+1}}$ is solvable in $F_{\mathfrak{p}_i}$, where e_i is the ramification index of $\mathfrak{p}_i$. It is easy to see that we can search x in the form $x = b_0 + b_1\pi_i + b_2\pi_i^2 + \cdots + b_{e_i}\pi_i^{e_i}$, where $b_0, b_1, \ldots, b_{e_i}$ represent elements from the residue class field of integers from F modulo $\mathfrak{p}_i$.

In the case $e_i = 1$ we cannot have $s_i = 1$ because of the following result.

Lemma 1. *If $e_i = 1$, then $x^2 + 1 \equiv 0 \pmod{\mathfrak{p}_i^3}$ is not solvable.*

Proof. In this case already the congruence $x^2 + 1 \equiv 0 \pmod{\mathfrak{p}_i^2}$ does not have a solution. Let $x = b_0 + b_i\pi_i$ with b_0, b_1 as above. Then $b_0^2 \equiv -1 \pmod{\pi_i}$. The multiplicative group of the residue class field modulo $\mathfrak{p}_i$ has odd order, and therefore $b_0 = 1$ and $x = 1 + b_1\pi_i$. From $(1 + b_i\pi_i)^2 \equiv -1 \pmod{\pi_i^2}$ we have $2 \equiv 0 \pmod{\pi_i^2}$, hence π_i^2 divides 2, which is a contradiction with $e_i = 1$. □

In what follows we will denote by Δ the index of the generator ρ of the field F. This is the index of the order generated by $1, \rho, \rho^2, \ldots, \rho^{n-1}$ in the maximal order of F.

In the case when Δ is odd, the determination of local levels is simple. We will illustrate this in the next section when dealing with quartic fields. Here we state some preliminary material.

Case $\Delta \equiv 1 \pmod 2$. The theorem of Kummer [2, Chapter 3, Appendix] gives the splitting of the prime 2 in F and generators for prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_g$. If Δ is odd,

$$f(x) \equiv \prod_{j=1}^{g} \varphi_j(x)^{e_j} \pmod 2$$

is the decomposition into irreducible factors, and $G_j(x) \in Z[x]$ are such that $G_j(x) \equiv \varphi_j(x) \pmod 2$, then $(2) = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j}$, where $\mathfrak{p}_j = (2, G_j(\rho))$.

Now we are able to determine prime elements $\pi_1, \pi_2, \ldots, \pi_g$ of $\mathfrak{O}$ for which we have $2 = \varepsilon \cdot \pi_1^{e_1} \cdot \pi_1^{e_2} \cdots \pi_g^{e_g}$, where ε is a unit in $\mathfrak{O}$.

Lemma 2. *Suppose Δ is odd. If $e_i \neq 1$, then we can choose $\pi_j = G_j(\rho)$; if $e_i = 1$, then $\pi_j = G_j(\rho)$ or $\pi_j = G_j(\rho) + 2$.*

Proof. We use the following criterion: an element a can be chosen as π_j if and only if $a \in \mathfrak{p}_j \backslash \mathfrak{p}_j^2$ and $a \notin \mathfrak{p}_i$ for every $i \neq j$. □

Remark. We can decide whether $\pi_j = G_j(\rho)$ or $\pi_j = G(\rho) + 2$ by computing norms. The number a satisfying $v_2(N_{F/Q}(a)) = f_j = n_j/e_j = n_j$, where v_2 is the dyadic valuation in Q, can be chosen as π_j.

Using the following result, we can decide whether Δ is odd or even.

Lemma 3. *The index Δ of ρ is odd if and only if for every nontrivial divisor $h(x) \pmod 2$ of the polynomial $f(x)$ (that is, $f(x) \equiv g(x)h(x) \pmod 2$) there*

is a polynomial $h'(x)$ *such that* $h'(x) \equiv h(x) \pmod 2$, $\deg h'(x) = \deg h(x)$, *and* $N_{F/Q}(h'(\rho)) \not\equiv 0 \pmod 2$.

Proof. (1) Suppose Δ is odd. Let

$$f(x) \equiv \prod_{j=1}^{g} \varphi_j(x)^{e_j} \pmod 2$$

be a decomposition into irreducible factors. Using Lemma 2, we choose the polynomial $G_j'(x)$ such that $G_j'(x) \equiv \varphi_j(x) \pmod 2$ and $\pi_j = G_j'(\rho)$. For

$$h(x) \equiv \prod_{j=1}^{g} \varphi_j(x)^{m_j} \pmod 2$$

we choose

$$h'(x) = \prod_{j=1}^{g} G_j'(x)^{m_j}.$$

Then $v_2(N_{F/Q}(h'(\rho))) = \sum_{j=1}^{g} f_j m_j < n$ because $\deg h(x) < n$, and therefore

$$N_{F/Q}(h'(\rho)) \not\equiv 0 \pmod{2^n}.$$

(2) According to [6] an integral basis of the field F can be chosen in the form

$$\omega_k = \frac{g_{k-1}(\rho)}{d_{k-1}} \quad \text{for } k = 1, \dots, n,$$

where $g_k(x) \in Z[x]$, $d_k \in N$, $\deg g_k(x) \le k$, $g_0(x) = 1$, and $d_{k-1} \backslash d_k$.

Moreover, if $d_k = c_k d_{k-1}$, then the polynomial $g_k(x)$ is a divisor of $f(x)$ modulo c_k. If Δ is even, then some c_k is even, hence $g_k(x)$ divides $f(x)$ modulo 2 and the number $g_k(\rho)/2$ is an integer in F. According to our assumption there is some polynomial $h'(x)$, $h'(x) \equiv g_k(x) \pmod 2$, such that $N_{F/Q}(h'(\rho)) \not\equiv 0 \pmod{2^n}$. Since $g_k(\rho)/2$ is an integer in F, the number $h'(\rho)/2$ is also an integer in F, contradicting $N_{F/Q}(h'(\rho)) \not\equiv 0 \pmod{2^n}$. □

The usefulness of this lemma will become apparent in the next section.

4. Number fields of degree 4

The invariant $S(F)$ of a quartic field F will be determined depending on the splitting type of the ideal (2) in F. The following 11 splitting types are possible:

(1) $(2) = \mathfrak{p}^2$; $f = 2$; $e = 2$.
(2) $(2) = \mathfrak{p}^4$; $f = 1$; $e = 4$.
(3) $(2) = \mathfrak{p}_1\mathfrak{p}_2^2$; $f_1 = 2$; $f_2 = 1$; $e_1 = 1$; $e_2 = 2$.
(4) $(2) = \mathfrak{p}_1^2\mathfrak{p}_2^2$; $f_1 = 1$; $f_2 = 1$; $e_1 = 2$; $e_2 = 2$.
(5) $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$; $f_1 = f_2 = f_3 = 1$; $e_1 = e_2 = 1$; $e_3 = 2$.
(6) $(2) = \mathfrak{p}$; $f = 4$; $e = 1$.
(7) $(2) = \mathfrak{p}_1\mathfrak{p}_2$; $f_1 = 2$; $f_2 = 2$; $e_1 = 1$; $e_2 = 1$.
(8) $(2) = \mathfrak{p}_1\mathfrak{p}_2$; $f_1 = 1$; $f_2 = 3$; $e_1 = 1$; $e_2 = 1$.
(9) $(2) = \mathfrak{p}_1\mathfrak{p}_2^3$; $f_1 = 1$; $f_2 = 1$; $e_1 = 1$; $e_2 = 3$.
(10) $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$; $f_1 = f_2 = 1$; $f_3 = 2$; $e_1 = e_2 = e_3 = 1$.
(11) $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$; $f_1 = f_2 = f_3 = f_4 = e_1 = e_2 = e_3 = e_4 = 1$.

If a splitting type is given, then the parameters g and $n_1, n_2, \dots, n_g$ are immediately determined.

Real embeddings. If $F = Q(\rho)$ and ρ is a zero of the polynomial $f(x) = x^4 - sx^3 + px^2 - qx + n$, then r is equal to the number of real roots of $f(x)$. Denote by D the discriminant of the polynomial $f(x)$. Then

$$27D = 4(p^2 - 3sq + 12n)^3 - (2p^3 - 72pn + 27s^2n - 9spq + 27q^2)^2.$$

The number of real roots of $f(x)$ is given by the following formulae (see [3, Chapter I, §37; 4, Part 2, Chapter 1, §1]):

(a) $r = 4$ if and only if $D > 0$ and simultaneously the following condition "C" holds:

$$\text{"C"}: \begin{array}{l} p - \frac{3}{8}s^2 < 0, \\ p^2 - s^2p + \frac{3}{16}s^4 + sq - 4n > 0. \end{array}$$

(b) $r = 0$ if and only if $D > 0$ and simultaneously condition "C" does not hold.

(c) $r = 2$ if and only if $D < 0$.

Global levels. As we have already mentioned, $s \in \{0, 1, 2, 4\}$; we have $s \neq 0$ if and only if $r = 0$, that is, $f(x)$ has no real zeros; $s = 4$ if and only if some local level $s_i = 4$. Therefore, the determination of s is reduced to the question of whether the equation $x^2 = -1$ is solvable in F, that is, whether the imaginary unit i belongs to F. If so, then F is a quadratic extension of $Q(i)$, hence ρ is a zero of the polynomial $x^2 + (a + bi)x + c + di$, where $b \neq 0$ or $d \neq 0$ and $a, b, c, d \in Z$. Then ρ is a zero of the polynomial

$$x^4 + 2ax^3 + (a^2 + 2c + b^2)x^2 + 2(ac + bd)x + c^2 + d^2.$$

Conversely, if $f(x)$ can be written in the above form, then $s = 1$.

If a prime $p \equiv 3 \pmod 4$ does not divide the discriminant D of the polynomial $f(x)$, and the congruence $f(x) \equiv 0 \pmod p$ has a solution in Z, then F does not contain i (hence $s \neq 1$) because in this case the congruence $x^2 \equiv -1 \pmod{\mathfrak{p}}$, where $\mathfrak{p} \backslash p$ is a prime divisor in F, is not solvable. On the other hand, if $s \neq 1$, then according to [5, Theorem 7.12] there are infinitely many such primes p.

Local levels. According to §2 and Lemma 1, when the splitting type of (2) is any of 8, 9, 10, or 11, then necessarily all the local levels s_i are equal to 4, and when the splitting type of (2) is 6 or 7, the local levels s_i are equal to 2.

Therefore, it is necessary to investigate the remaining splitting types 1, 2, 3, 4, 5.

If the splitting type of the prime ideal (2) in the field F is 1, 2, 3, or 4, then according to [5, Theorem 4.11] there is an element $\rho \in F$ which generates F and whose index is odd. If the splitting type of (2) in F is 5, then again according to [5, Theorem 4.11] such an element ρ with odd index does not exist.

In the sequel we will show how to determine local levels s_i in the cases 1, 2, 3, 4, 5.

In cases 1–4 we will assume that a number ρ with odd index is available.

Case (1) corresponds to the decomposition

$$f(x) \equiv (x^2 + x + 1)^2 \pmod 2.$$

Theorem 1. *Suppose* $f(x) \equiv (x^2 + x + 1)^2 \pmod 2$. *If* Δ *is odd, then the congruence* $x^2 \equiv -1 \pmod{\pi^5}$ *has a solution if and only if one of the following conditions is satisfied*:

(i) $s \equiv 2,\ p \equiv 1,\ q \equiv 0,\ n \equiv 1 \pmod 4;\ p + q \equiv 1 \pmod 8$.
(ii) $s \equiv 0,\ p \equiv 1,\ q \equiv 2,\ n \equiv 1 \pmod 4;\ s + p - n \equiv 0 \pmod 8$.
(iii) $s \equiv 0,\ p \equiv 3,\ q \equiv 0,\ n \equiv 1 \pmod 4;\ -s + q + n \equiv 1 \pmod 8$.

Proof. We have

$$\pi = \rho^2 + \rho + 1, \qquad \rho^4 = s\rho^3 - p\rho^2 + q\rho - n,$$

and

$$\pi^2 = (s+2)\rho^3 + (-p+3)\rho^2 + (q+2)\rho + (-n+1).$$

Since $f(x) \equiv (x^2 + x + 1)^2 \pmod 2$, the following numbers are integers:

$$S = \frac{s+2}{2}, \quad P = \frac{-p+3}{2}, \quad Q = \frac{q+2}{2}, \quad N = \frac{-n+1}{2}.$$

Let $A = S\rho^3 + P\rho^2 + Q\rho + N$. Then $2A = \pi^2$ and

$$A = \pi[S\rho + (P - S)] + (Q - P)\rho + N - (P - S).$$

We have three possibilities for A:

(i) $A \equiv 1 \pmod \pi$.
(ii) $A \equiv \rho \pmod \pi$.
(iii) $A \equiv 1 + \rho \pmod \pi$.

First we consider case (i). In this case we have

$$(*) \qquad Q \equiv P \pmod 2, \quad N - (P - S) \equiv 1 \pmod 2,$$

and $A = 1 + \pi u_1 + 2u_2$, where

$$u_1 = S\rho + (P - S) \quad \text{and} \quad u_2 = \frac{Q - P}{2}\rho + \frac{N - (P - S) - 1}{2}.$$

Our task is to solve the congruence $(b_0 + b_1\pi + b_2\pi^2)^2 \equiv -1 \pmod{\pi^5}$, where $b_0, b_1, b_2 \in \{0, 1, \rho, \rho + 1\}$.

As in the proof of Lemma 1, we have $b_0 = 1$. From the congruence

$$(1 + b_1\pi + b_2\pi^2)^2 \equiv -1 \pmod{\pi^5}$$

we obtain

$$2 + b_1^2\pi^2 + b_2^2\pi^4 + 2b_1\pi + 2b_2\pi^2 \equiv 0 \pmod{\pi^5}.$$

If we multiply this by A we find

$$\pi^2 + Ab_1^2\pi^2 + Ab_2^2\pi^4 + b_1\pi^3 + b_2\pi^4 \equiv 0 \pmod{\pi^5},$$

$$1 + Ab_1^2 + b_1\pi + \pi^2(b_2 + Ab_2^2) \equiv 0 \pmod{\pi^3},$$

and

$$1 + b_1^2(1 + \pi u_1 + 2u_2) + b_1\pi + \pi^2(b_2 + Ab_2^2) \equiv 0 \pmod{\pi^3}.$$

Therefore, $b_1 = 1$, which means that

$$2 + 2u_2 + \pi u_1 + \pi + \pi^2(b_2 + Ab_2^2) \equiv 0 \pmod{\pi^3}.$$

Multiplication by A gives

$$\pi^2(1 + u_2) + \pi A(u_1 + 1) + \pi^2(Ab_2 + A^2b_2^2) \equiv 0 \pmod{\pi^3}$$

and

$$(**) \qquad A(1+u_1)+\pi(1+u_2)+\pi(Ab_2+A^2b_2^2)\equiv 0 \pmod{\pi^2}.$$

Therefore, $1+u_1\equiv 0 \pmod{\pi}$, and this means that $S\equiv 0 \pmod 2$, $P\equiv 1 \pmod 2$.

From $(*)$ we obtain $Q\equiv 1 \pmod 2$ and $N\equiv 0 \pmod 2$. From $(**)$ we deduce $1+u_2+b_2+b_2^2\equiv 0 \pmod{\pi}$. For $b_2\in\{0,1,\rho,\rho+1\}$ the expression $b_2+b_2^2$ takes on values 0 and 1. Therefore, $u_2\equiv 0 \pmod{\pi}$ or $u_2\equiv 1 \pmod{\pi}$, and this implies $(Q-P)/2\equiv 0 \pmod 2$.

We have proved that in case (i) the congruence $x^2\equiv -1 \pmod{\pi^5}$ has a solution only if $S\equiv 0 \pmod 2$, $P\equiv 1 \pmod 2$, $Q\equiv 1 \pmod 2$, $N\equiv 0 \pmod 2$, and $Q\equiv P \pmod 4$.

It is easy to see that the converse implication is also correct. If we substitute the expressions for S, P, Q, N, we obtain the statement of the theorem.

In cases (ii) and (iii) we proceed analogously. □

Case (2) corresponds to the decompositions

$$f(x)\equiv x^4 \pmod 2 \quad \text{and} \quad f(x)\equiv (x+1)^4 \pmod 2.$$

Theorem 2. *Suppose* $f(x)\equiv x^4 \pmod 2$. *Then* Δ *is odd if and only if* $N_{F/Q}(\rho)=n\equiv 2 \pmod 4$. *Moreover, if* Δ *is odd, then the congruence* $x^2\equiv -1 \pmod{\pi^9}$ *is solvable if and only if one of the following conditions is satisfied*:

(i) $s\equiv 0, p\equiv 2, q\equiv 0 \pmod 4$; $n\equiv 2 \pmod 8$,
(ii) $s\equiv 2, p\equiv 0, q\equiv 0 \pmod 4$; $n\equiv 2 \pmod 8$.

Proof. The first part follows from Lemmas 2 and 3.

We take

$$\pi=\rho, \quad S=\frac{s}{2}, \quad P=\frac{-p}{2}, \quad Q=\frac{q}{2}, \quad N=\frac{-n}{2},$$

$$A=S\pi^3+P\pi^2+Q\pi+N=\pi(S\pi^2+P\pi+Q)+N\equiv 1 \pmod{\pi},$$

and

$$L=S\pi^2+P\pi+Q.$$

We have to solve the congruence

$$(b_0+b_1\pi+b_2\pi^2+b_3\pi^3+b_4\pi^4)^2\equiv -1 \pmod{\pi^9},$$

where each $b_i=0$ or 1. It is easy to see that the solution has to be in one of the forms

(i) $1+\pi^2+b_4\pi^4$;
(ii) $1+\pi^2+\pi^3+b_4\pi^4$.

We first deal with case (i). Here $(1+\pi^2+b_4\pi^4)^2\equiv -1 \pmod{\pi^9}$, hence

$$2+\pi^4+b_4^2\pi^8+2\pi^2+2b_4\pi^4\equiv 0 \pmod{\pi^9}.$$

We multiply by A and obtain

$$\pi^4+A\pi^4+\pi^6+\pi^8(b_4+b_4^2A)\equiv 0 \pmod{\pi^8}.$$

Since $b_4+b_4^2A\equiv 0 \pmod{\pi}$, we have $1+N+\pi L+\pi^2\equiv 0 \pmod{\pi^5}$. If we put $N_1=(1+N)/2$ and multiply the congruence by A, we obtain

$$A(S\pi^2+P\pi+Q)+A\pi+N_1\pi^3\equiv 0 \pmod{\pi^4}.$$

Hence, $Q \equiv 0 \pmod 2$, and in this case $Q \equiv 0 \pmod{\pi^4}$, therefore

$$A(1+P) + AS\pi + N_1\pi^2 \equiv 0 \pmod{\pi^3}.$$

We must have $1+P \equiv 0 \pmod 2$ and $AS + N_1\pi \equiv 0 \pmod{\pi^2}$, and therefore $S \equiv 0 \pmod 2$ and $N_1 \equiv 0 \pmod 2$.

Finally in case (i) the original congruence has a solution if and only if $S \equiv 0$, $P \equiv 1$, $Q \equiv 0 \pmod 2$ and $N_1 \equiv 0 \pmod 2$. From this we obtain the statement of the theorem.

Case (ii) is analogous. □

Remark. If $f(x) \equiv (x+1)^4 \pmod 2$, we can change the generator ρ to $\rho - 1$ and transform the equation $f(x) = 0$, using the substitution $z = x + 1$, and then we can use Theorem 2.

Case (3) corresponds to the decompositions

$$f(x) \equiv x^2(x^2 + x + 1) \pmod 2$$

and

$$f(x) \equiv (x+1)^2(x^2 + x + 1) \pmod 2.$$

Theorem 3. *Suppose* $f(x) \equiv x^2(x^2 + x + 1) \pmod 2$. *If* Δ *is odd, then the congruence* $x^2 \equiv -1 \pmod{\pi_1^5}$ *has a solution if and only if* $q \equiv 0 \pmod 4$ *and* $n + 2p \equiv 4 \pmod 8$.

Proof. We choose $\pi = \rho$. Again,

$$\rho^4 = s\rho^3 - p\rho^2 + q\rho - n$$

and

$$\rho^2(\rho^2 + \rho + 1) = \rho^4 + \rho^3 + \rho^2 = (s+1)\rho^3 + (-p+1)\rho^2 + q\rho - n.$$

In this case we put

$$S = \frac{s+1}{2}, \quad P = \frac{-p+1}{2}, \quad Q = \frac{q}{2}, \quad N = \frac{-n}{2},$$

$$A = S\pi^3 + P\pi^2 + Q\pi + N$$

and have

$$A = \pi(S\pi^2 + P\pi + Q) + N \equiv 1 \pmod \pi.$$

That is, $A = L\pi + N$, where $L = S\pi^2 + P\pi + Q$. Moreover, $\pi^2(\pi^2 + \pi + 1) = 2A$.

We solve the congruence

$$(b_0 + b_1\pi + b_2\pi^2)^2 \equiv -1 \pmod{\pi^5}.$$

It is easy to find that $b_0 = b_1 = 1$, hence

$$(1 + \pi + b_2\pi^2)^2 \equiv -1 \pmod{\pi^5}$$

and

$$2 + \pi^2 + 2\pi + b_2^2\pi^4 + 2b_2\pi^2 \equiv 0 \pmod{\pi^5}.$$

If we multiply this congruence by A we obtain

$$(\pi^2 + \pi^3 + \pi^4 b_2)(\pi^2 + \pi + 1) + A\pi^2 + b_2^2 A\pi^4 \equiv 0 \pmod{\pi^5}.$$

From this we deduce that $1 + A \equiv 0 \pmod{\pi^3}$.

If we substitute for A we have

$$1 + N + \pi(S\pi^2 + P\pi + Q) \equiv 0 \pmod{\pi^3}.$$

We put $N_1 = (1 + N)/2$ and obtain

$$2N_1 + \pi(S\pi^2 + P\pi + Q) \equiv 0 \pmod{\pi^3},$$

$$2N_1 + P\pi^2 + Q\pi \equiv 0 \pmod{\pi^3}.$$

Multiplying by A, we obtain

$$\pi^2(\pi^2 + \pi + 1)N_1 + PA\pi^2 + QA\pi \equiv 0 \pmod{\pi^3},$$

$$QA + PA\pi + \pi N_1 \equiv 0 \pmod{\pi^2}.$$

Therefore, $Q \equiv 0 \pmod 2$, and from this $PA + N_1 \equiv 0 \pmod{\pi}$ and $P + N_1 \equiv 0 \pmod 2$.

This means that $Q \equiv 0 \pmod 2$ and $P + N_1 \equiv 0 \pmod 2$.

If we substitute back for P, Q, and N_1, we obtain the statement of the theorem. □

Remark. If $f(x) \equiv (x + 1)^2(x^2 + x + 1) \pmod 2$, then we can proceed analogously as in the preceding remark.

Case (4) is considered in the following theorem.

Theorem 4. *Suppose* $f(x) \equiv x^2(x + 1)^2 \pmod 2$. *Then* Δ *is odd if and only if* $n \equiv 2 \pmod 4$ *and* $n + s + p + q \equiv 1 \pmod 4$. *In this case the congruence* $x^2 \equiv -1 \pmod{\pi_1^5}$ *has a solution if and only if* $q \equiv 2 \pmod 4$ *and* $n + 2p \equiv 0 \pmod 8$, *and the congruence* $x^2 \equiv -1 \pmod{\pi_2^5}$ *has a solution if and only if* $s + q \equiv 0 \pmod 4$ *and* $s + p - q - n \equiv 1 \pmod 8$.

Proof. The proof of this theorem is analogous to the preceding one. □

Remark. If Δ is odd, then we could solve the question about the solvability of the equation $x^2 = -1$ in local fields $F_{\mathfrak{p}}$, where $\mathfrak{p} \mid 2$ and $\mathfrak{p}$ is ramified, analogously also in the case when the degree of the field F is greater than 4. For small n, say $n \leq 10$, the problem would not be too complicated because there are only a few irreducible polynomials modulo 2 whose degree is less than or equal to 5. The problem would be more complicated for large n, in which case there are many irreducible polynomials modulo 2 with degree less than or equal to $n/2$, and we would have to consider too many cases. If we are interested only in representatives of Witt equivalence classes, then it is possible to consider even larger n.

We now consider case (5) corresponding to the splitting $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$.

Let d be the greatest integer such that 2^d divides the discriminant D of the polynomial $f(x)$.

Theorem 5. (A) *Suppose* $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$ *is the splitting of the ideal* (2) *in* F. *Let* $f(x) = x^4 - sx^3 + px^2 - qx + n$ *be the minimal polynomial of a uniformizing element* π_3 *corresponding to the dyadic prime* $\mathfrak{p}_3$. *Then*

(1) $n \equiv 2 \pmod 4$.

(2) $f(x) \equiv x^2(x + 1)^2 \pmod 2$.

(3) *The congruence* $x_2 \equiv -1 \pmod{\pi_3^5}$ *is solvable if and only if* $q \equiv 2 \pmod 4$ *and* $n + 2p \equiv 0 \pmod 8$.

(B) *Conversely, let* $F = Q(\rho)$ *and* ρ *be a zero of the polynomial* $f(x) = x^4 - sx^3 + px^2 - qx + n \equiv x^2(x+1)^2 \pmod 2$. *Suppose further that* $n \equiv 2 \pmod 4$, $d \geq 1$ (*that is, the discriminant* D *is even*), *and there are nontrivial monic polynomials* $f_1(x)$, $f_2(x)$, $f_3(x)$ *such that* $f(x) \equiv f_1(x)f_2(x)f_3(x) \pmod{2^{d+1}}$. *Then* $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$ *is the splitting in* F *and* ρ *can be chosen as a uniformizing element of* $\mathfrak{p}_3$.

Proof. (A)(1) The inertion degree f_3 of the prime divisor $\mathfrak{p}_3$ equals 1, hence $N(\mathfrak{p}_3) = 2$, and this implies $N(\pi_3) \equiv 2 \pmod 4$.

(2) We have

$$\frac{-n}{\pi_3^2} = \frac{\pi_3^4 - s\pi_3^3 + p\pi_3^2 - q\pi_3}{\pi_3^2} = \pi_3^2 - s\pi_3 + p - \frac{q}{\pi_3}.$$

Therefore, q is even and x^2 divides the polynomial $f(x)$ modulo 2. According to [1, Chapter IV, §2, Theorem 3 and Chapter IV, §3, Theorem 3] there is a decomposition

$$f(x) \equiv f_1(x)f_2(x)f_3(x) \pmod{2^{d+1}},$$

where $\deg f_3(x) = 2$.

If x^3 divides $f(x) \pmod 2$, then at least two of the polynomials $f_1(x)$, $f_2(x)$, $f_3(x)$ are divisible by $x \pmod 2$. This is a contradiction with $n \equiv 2 \pmod 4$ and $d \geq 1$.

If $f(x) \equiv x^2(x^2 + x + 1) \pmod 2$, then $f_3(x) \equiv x^2 + x + 1 \pmod 2$ because the polynomial $x^2 + x + 1$ is irreducible modulo 2. Therefore, $f_1(x) \equiv x \pmod 2$ and $f_2(x) \equiv x \pmod 2$, contradicting $n \equiv 2 \pmod 4$ and $d \geq 1$. Hence, $f(x) \equiv x^2(x+1)^2 \pmod 2$.

(3) The proof of this part is analogous to that of Theorem 4.

(B) Since $n \equiv 2 \pmod 4$, $f(x) \equiv x^2(x+1)^2 \pmod 2$, and 4 divides 2^{d+1}, it is impossible to satisfy the congruence

$$f(x) \equiv (x + a_1)(x + a_2)(x + a_3)(x + a_4) \pmod{2^{d+1}}.$$

From the congruence $f(x) \equiv f_1(x)f_2(x)f_3(x) \pmod{2^{d+1}}$ and [1, Chapter IV, §2, Theorem 3 and Chapter IV, §3, Theorem 3] we obtain that the prime 2 is divisible by three different prime divisors of the field F.

From the congruence $N(\rho) \equiv 2 \pmod 4$ it follows that ρ is a uniformizing element of some of these prime divisors. Since

$$f(x) \equiv x^2(x + 1)^2 \pmod 2,$$

the number q is even and we infer that ρ^2 divides 2 because

$$\frac{-n}{\rho^2} = \frac{\rho_4 - s\rho^3 + p\rho^2 - q\rho}{\rho^2} = \rho^2 - s\rho + p - \frac{q}{\rho^2}.$$

Therefore, $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$ in F, and ρ is a uniformizing element of the prime divisor $\mathfrak{p}_3$. □

5. Conjecture of Szymiczek

In this section we will show that the Conjecture of Szymiczek stated in the introduction is true. We will give a list of representatives of the 26 Witt eqivalence classes, which confirms this conjecture.

We will use only the following four splitting types of the prime ideal (2):

(1) $(2) = \mathfrak{p}^2$; $f = 2$; $e = 2$.
(2) $(2) = \mathfrak{p}^4$; $f = 1$; $e = 4$.
(3) $(2) = \mathfrak{p}_1\mathfrak{p}_2^2$; $f_1 = 2$; $f_2 = 1$; $e_1 = 1$; $e_2 = 2$.
(4) $(2) = \mathfrak{p}_1^2\mathfrak{p}_2^2$; $f_1 = 1$; $f_2 = 1$; $e_1 = 2$; $e_2 = 2$.

It is clear that this is the minimal number of splitting types which are necessary to cover all Witt equivalence classes in Table 1 below except lines 8, 12, 20.

Lines 8, 12, 20 are empty in Table 1 because every field F which represents one of these lines cannot contain any quadratic subfield. This is due to the fact that local degrees are multiplicative and one of the local dyadic degrees of such a field F has to be equal to 3.

For the sake of completeness we give some representatives of these classes in Table 2 at the end of the paper.

Let ρ be a root of the equation $x^2 + (a + b\omega)x + (c + d\omega) = 0$, where $b \neq 0$ or $d \neq 0$, a, b, c, d are integers, and $\omega = \sqrt{2}$ or $\omega = (1 + \sqrt{17})/2$, respectively. Then ρ is a zero of a polynomial

$$(***) \qquad f(x) = x^4 + 2ax^3 + (a^2 + 2c - 2b^2)x^2 + (2ac - 4bd)x + (c^2 - 2d^2)$$

or

$$(****) \qquad \begin{aligned} f(x) = {} & x^4 + (2a + b)x^3 + (a^2 + ab - 4b^2 + 2c + d)x^2 \\ & + (2ac + bc + ad - 8bd)x + (c^2 + cd - 4d^2), \end{aligned}$$

respectively.

If the polynomials $(***)$, $(****)$ are irreducible in the ring $Z[x]$, then the field $F = Q(\rho)$ has degree 4 over Q and it contains the quadratic subfield $Q(\sqrt{2})$ or $Q(\sqrt{17})$, respectively.

The fields F which correspond to the polynomials given in lines 1–7 in Table 1 contain the subfield $Q(\sqrt{2})$, and the fields corresponding to the polynomials in lines 8–29 except 8, 12, 20 contain the subfield $Q(\sqrt{17})$.

The values a, b, c, d displayed in Table 1 are numbers which appear in coefficients of the polynomials $(***)$ and $(****)$.

All representatives in Table 1 except lines 27, 28, 29 were constructed using the theorems in §4.

The fields in lines 27, 28, 29 were found on the basis of [1, Chapter IV, §2, Theorem 3 and Chapter IV, §3, Theorem 3], where

$$f(x) \equiv x(x + 1)(x + 2)(x + 3) \pmod{32}.$$

The irreducibility of the polynomials in Table 1 was checked by the Eisenstein criterion, or using Berlekamp's algorithm, or taking into consideration the real quadratic subfield and the presence of complex elements in the field F.

TABLE 1

type	n	r	s	g	n_i	s_i	a	b	c	d	polynomial $f(x)$
1.	4	4	0	1	4	1	0	3	2	1	$x^4 - 14x^2 - 12x + 2$
2.	4	4	0	1	4	2	0	2	0	1	$x^4 - 8x^2 - 8x - 2$
3.	4	2	0	1	4	1	0	1	2	3	$x^4 + 2x^2 - 12x - 14$
4.	4	2	0	1	4	2	0	0	0	1	$x^4 - 2$
5.	4	0	1	1	4	1	2	1	2	1	$x^4 + 4x^3 + 6x^2 + 4x + 2$
6.	4	0	2	1	4	1	0	1	10	1	$x^4 + 18x^2 - 4x + 98$
7.	4	0	2	1	4	2	0	0	2	1	$x^4 + 4x^2 + 2$
8.	4	4	0	2	1, 3	4, 4					no quadratic subfield
9.	4	4	0	2	2, 2	1, 1	0	6	5	−7	$x^4 + 6x^3 - 141x^2 + 366x - 206$
10.	4	4	0	2	2, 2	1, 2	2	4	6	1	$x^4 + 8x^3 - 39x^2 + 18x + 38$
11.	4	4	0	2	2, 2	2, 2	0	4	1	1	$x^4 + 4x^3 - 61x^2 - 28x - 2$
12.	4	2	0	2	1, 3	4, 4					no quadratic subfield
13.	4	2	0	2	2, 2	1, 1	−8	−6	−3	−7	$x^4 - 22x^3 - 45x^2 - 214x - 166$
14.	4	2	0	2	2, 2	1, 2	0	2	1	5	$x^4 + 2x^3 - 9x^2 - 78x - 94$
15.	4	2	0	2	2, 2	2, 2	0	0	1	1	$x^4 + 3x^2 - 2$
16.	4	0	1	2	2, 2	1, 1	0	−2	5	1	$x^4 - 2x^3 - 5x^2 + 6x + 26$

TABLE 1 (*continued*)

type	n	r	s	g	n_i	s_i	a	b	c	d	polynomial $f(x)$
17.	4	0	2	2	2, 2	1, 1	−2	2	38	−1	$x^4 - 2x^3 + 59x^2 - 58x + 1402$
18.	4	0	2	2	2, 2	1, 2	−2	0	6	1	$x^4 - 4x^3 + 17x^2 - 26x + 38$
19.	4	0	2	2	2, 2	2, 2	0	0	6	3	$x^4 + 15x^2 + 18$
20.	4	0	4	2	1, 3	4, 4					no quadratic subfield
21.	4	4	0	3	1, 1, 2	4, 4, 1	82	−28	126	−117	$x^4 + 136x^3 + 1427x^2 - 18666x - 53622$
22.	4	4	0	3	1, 1, 2	4, 4, 2	10	−14	10	21	$x^4 + 6x^3 - 783x^2 + 2622x - 1454$
23.	4	2	0	3	1, 1, 2	4, 4, 1	18	−12	62	27	$x^4 + 24x^3 - 317x^2 + 4566x + 2602$
24.	4	2	0	3	1, 1, 2	4, 4, 2	10	−14	138	21	$x^4 + 6x^3 - 527x^2 + 3390x + 20178$
25.	4	0	4	3	1, 1, 2	4, 4, 1	18	−12	446	27	$x^4 + 24x^3 + 451x^2 + 13782x + 208042$
26.	4	0	4	3	1, 1, 2	4, 4, 2	10	−14	298	21	$x^4 + 6x^3 - 207x^2 + 4350x + 93298$
27.	4	4	0	4	1, 1, 1, 1	4, 4, 4, 4	10	−14	28	11	$x^4 + 6x^3 - 757x^2 + 1510x + 608$
28.	4	2	0	4	1, 1, 1, 1	4, 4, 4, 4	1	4	8	22	$x^4 + 6x^3 - 21x^2 - 634x - 1696$
29.	4	0	4	4	1, 1, 1, 1	4, 4, 4, 4	1	4	72	22	$x^4 + 6x^3 + 107x^2 - 250x + 4832$

TABLE 2

type	n	r	s	g	n_i	s_i	polynomial $f(x)$
8.	4	4	0	2	1, 3	4, 4	$x^4+5x^3+x^2-7x-2$
12.	4	2	0	2	1, 3	4, 4	$x^4-3x^3+x^2-3x+2$
20.	4	0	4	2	1, 3	4, 4	$x^4+x^3+x^2+x+2$

ACKNOWLEDGMENT

We are very grateful to the referee for valuable comments and suggestions towards improving the paper.

BIBLIOGRAPHY

1. Z. I. Borevič and I. R. Šafarevič, *Number theory*, 3rd rev. ed., Nauka, Moscow, 1985. (Russian)
2. J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Proceeding of an instructional conference organized by the London Mathematical Society, Academic Press, London and New York, 1967.
3. B. N. Delone and D. K. Faddeev, *Theory of irrationalities of the third degree*, Trudy Mat. Inst. Steklov. **11** (1940); English transl., Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R. I., 1964.
4. R. Fricke, *Lehrbuch der Algebra*, Vol. I, Vieweg, Braunschweig, 1924.
5. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN, Warszawa, 1974.
6. K. Petr, *Bases of integers in algebraic number fields*, Časopis Pěst. Mat. Fys. **5** (1935), 62–72. (Czech)
7. K. Szymiczek, *Witt equivalence of global fields*, Comm. Algebra **19** (1991), 1125–1149.

THE INSTITUTE OF MATHEMATICS, STEFANIKOVA 49, 814 73 BRATISLAVA, CZECHOSLOVAKIA